Last updated: August 1, 2023

California Privacy Notice

Taoglas USA, Inc. and its affiliates (collectively, "**Taoglas**," "**we**," "**our**," and "**us**") respects your privacy and is committed to protecting your personal data. This Privacy Notice will inform you as to how we look after your personal data. We are a "B2B" company, meaning our customers are businesses and not consumers. When we use the word "you", we are referring both to people who interact with us as individuals or representatives of our customers.

You can download a pdf version of the notice here.

1. Important Information and Who We Are

1.1 Purpose of this Privacy Notice

This Privacy Notice ("Notice") aims to give you information on how Taoglas collects and processes your personal data through your use of our websites (including Taoglas.com, locate.taoglas.com, connect.taoglas.com, crowdinsights.taoglas.com)("**Sites**"), when you sign up to our newsletter, use our products and services, speak to our staff, apply for a job with us or when you otherwise interact with us or provide us with personal information on you or individuals connected with you. Where necessary, we will provide additional information in relation to specific products and services.

It is important that you read this Notice, and any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This Notice supplements the other notices and is not intended to override them.

By using our Sites or otherwise using our services, you consent to this Notice and agree to our Terms and **Conditions** ("**Terms**").

1.2 Children

Our Sites are not intended for children under the age of 18 and we do not knowingly collect data relating to children. We encourage parents and legal guardians to monitor their children's Internet usage and to help enforce this Notice by instructing their children never to provide personal information through our Sites. If you have reason to believe that a child has provided personal information to us through our Sites, please contact us at privacy@taoglas.com, and we will use commercially reasonable efforts to delete that information.

1.3 Controller

This Notice is issued on behalf of Taoglas USA, Inc. and its affiliates (collectively in this Notice, "**Taoglas**", "**we**", "**us**" or "**our**"). Unless otherwise specified (for example, in relation to specific products or services or if you apply for a job with a member of our group), Taoglas is the controller of your personal data.

We have appointed a data privacy manager who is responsible for overseeing questions in relation to this Notice. If you have any questions about this Notice, including any requests to exercise your rights, please contact the data privacy manager using the details set out below.

If you have any questions about this Notice or information we hold about you, including any requests to exercise your legal rights, please contact us at privacy@taoglas.com or write to us at Taoglas, Unit 5 Kilcannon Business Park, Old Dublin Road, Enniscorthy, Co Wexford, Y21XW56, Ireland.

1.4 Changes to this Privacy Notice

We keep our Privacy Notice under regular review and we will place any updates on this web page. We advise you to review this page regularly to stay informed and to make sure that you are happy with any changes. If we make material changes to this Notice we will notify our registered users by email or through posting a notification when you log into our products or services.

1.5 Your Personal Data

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us. If you are a representative of one of our customers and have account access credentials, you can always access the account and review the information you have provided, including name, address, email address, phone number, payment information and other relevant account information. You can update this information directly or contact us for assistance. If you delete some or all of this information, then you may be prevented from accessing your account or using any services. Data relating to device activity and to actions that have been authorized by an account representative regarding those devices that is intended for viewing by customers may be accessed at our customer portal.

1.6 Third-Party Links

Our Sites, products and services may contain links to websites operated by third parties that we believe may be of interest or that are relevant to one of our services. If you use these links, you will leave our Sites, and you should note that we do not have any control over that other websites and cannot be responsible for the protection and privacy of any information that you provide while visiting such sites. Providing a link to third party websites does not mean that we endorse or warrant the products or services provided by any third parties and this Notice does not govern such sites. These third parties and the social media providers described earlier will have their own privacy policies that will govern the data

they collect.

1.7 Taoglas as Processor

While providing services to customers, we collect information that we believe is not personal data including device IDs, time stamps, authentication records, location information, carrier service used, signal strength, the origin, destination, type and quantity of traffic passed and other operational data. For example, as part of analytic services provided to our customers, Taoglas identifies the following information based on mobile devices; MAC address of device, time device seen, estimated location of device and sometimes RSSI. Once identified, this device MAC address is immediately converted into a unique 'CROWD Insights ID' using a non-reversible hash. The CROWD Insights ID is stored and the device MAC address discarded. We require this information to present aggregated information of the venue or city to our customers. This in turn enables them to deliver better, more secure services. If we reasonably determine that any device data could reveal information about an identifiable natural person, such as their location, we will protect it as we would any other personal data. Where we are engaged as a processor on behalf of our customers (such as customers using our analytic services CROWD Insights), you should refer to our customer's privacy notice.

2. The Data We Collect About You

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity Data** including first name, maiden name, last name, username or similar identifier, job title/position, date of birth and gender.
- **Contact Data** including employer, work address, email address and telephone numbers.
- **Financial Data** including transaction amount, payment method and cardholder details.
- **Technical Data** including internet protocol (IP) address, device identifier, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our Sites, products and services.
- **Usage Data** including information about how you use our websites, products and services such as your geographical location, your Internet service provider and your IP address. We also record information about the software you are using to browse our Sites, such as the type of computer or device and the screen resolution.
- **Marketing and Communications Data** including your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law where you are directly or indirectly identified or identifiable. For example, we may aggregate your usage Data to calculate the percentage of users accessing a specific service feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Notice.

Unless required by law, we will not, without your explicit consent, collect **Special Categories of Personal**

Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data) or information about criminal convictions and offences. If you believe any of our Sites or Taoglas employee has asked you for this information, please contact us at privacy@taoglas.com.

If you fail to provide personal data. Where we need to collect personal data by law, or under the terms of a contract we have with you or your employer and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you or your employer.

For information about the personal data we collect about our job applicants, employees and independent contractors, please see the Taoglas Employee Privacy Notice.

3. How Is Your Personal Data Collected?

We use different methods to collect personal data from and about you including through:

Direct interactions. You may give us your Identity and Contact Data filling in forms or by corresponding with us by post, phone, email, or otherwise. This includes personal data you provide when you:

- subscribe to our services, newsletters or mailing lists;
- attend our webinars;
- request information to be sent to you including viewing demos;
- enter a survey;
- apply for a job in our "Careers" section;
- give us some feedback; or
- submit a query.

Tracking technologies or interactions. As you interact with our Sites, products and services, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our Cookie Notice for further details.

Third parties or publicly available sources. We may receive personal data about you from various third parties, including Identity and Contact Data from your employer and/or publicly available sources like the Companies Registration Office in Ireland and Technical Data from analytics providers/advertising networks and search information providers such as Google.

4. How We Use Your Personal Data

We will only use your personal data when the law allows us to. We have set out below a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us at privacy@taoglas.com if you need details about the specific legal basis we are relying on to process your personal data where more than one basis has been set out.

Consent. Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications to you via email or text

message. Where we rely on your consent to process your personal data, you have the right to withdraw your consent at any time, although in certain cases we may not be able to continue to provide services to you (or your employer) if we cannot use the personal data. You can withdraw consent at any time by contacting us at privacy@taoglas.com.

Legitimate Interests. Where we rely on legitimate interests as our lawful basis, we make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us at privacy@taoglas.com.

4.1. Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at privacy@taoglas.com.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. Disclosures of Your Personal Data

Access by Taoglas Personnel. We allow access to personal data only to those of our employees, and consultants who have a need to access the information for a lawful purpose. We train our employees how to appropriately handle personal data and require that consultants do likewise.

Access by other third parties. We may store your personal data with or allow access to your personal data to third parties who provide us with certain services, including websites maintenance, database and cloud, customer support, customer analytics, payment processing, payroll and benefits management or other services. Our contracts with these third party providers only allow use of your personal data to provide these services and require that they not disclose it unless required in certain situations, like those described in the following paragraph. We review the security policies and practices of our third party service providers as appropriate as part of our own efforts to maintain the security of your personal data.

Law Enforcement, Court Orders and Protection of Our Rights. We may disclose any of your personal data to government officials as necessary to comply with applicable laws and orders. If we receive a request to disclose any such data, we may do so if we believe in our reasonable discretion that such request is lawful and that disclosure is reasonably necessary to comply. We may also disclose your personal data to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. In the event that we are legally compelled to disclose your personal data to a third party, we will attempt to notify you unless doing so would violate the law, court order or government instruction.

Other Disclosures. We may also disclose your information if we believe it is necessary in order to protect our property rights or rights of a third party, to protect the safety of any person or of the public or to prevent any activity that we believe is harmful, illegal or unethical. For example, we may need to use personal data in order to enforce our terms of service with customers and our workplace rules, or to

engage in other business or corporate transactions. We will put in place appropriate security measures, such as non-disclosure agreements, whenever possible.

6. International Transfers

We choose a location storage depending on the type of data:

Website and Account Information. Our Sites are hosted in the EU. If you are located outside the EU, such as in the US, and interact with our Sites, including when you manage any account, you are effectively "visiting" an EU website, and the personal data that you provide is stored in the EU.

Marketing Information. If you share your personal data with a Taoglas sales or marketing representative, your data is generally kept in the region where you are located or where the contact (such as a tradeshow or event) took place (e.g., US, EU, APAC). We use a CRM service to help us manage our marketing and financial activities, and some of your personal data may be kept on systems in the US. In addition, our staff do share limited information, which may include your contact information, to coordinate marketing activities and to make sure that you are interacting with the correct Taoglas entity and business function, such as finance, legal, support or engineering.

Data Relevant to Employment If you apply for a position with any Taoglas company, generally, your information will stay in the country where you apply, although some data may be shared with other Taoglas companies especially for global positions. For information about the personal data we collect about our job applicants, employees and independent contractors, please see the Taoglas Employee Privacy Notice linked below

Taoglas has entered into formal agreements based on "standard contractual clauses" that commit us to following the principles in the first part of this Notice when one Taoglas company transfers personal data to another. Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the European Economic Area.

7. Your Choices About the Information We Collect

Communications Preferences

We prefer to keep your personal data accurate and up to date. If you would like to change your contact information, please contact us . We will make good faith efforts to make requested changes in our then active databases as soon as reasonably practicable (but we may retain prior information as business records).

You can opt out of receiving marketing emails or text messages from us at any time. You will still receive transactional messages from us. To manage your email preferences with us, please click on the Unsubscribe link in any email you receive from us or contact us using the information in the Contact Us section below. Your choice will not affect our ability to share information in the other ways described in this Notice.

Do Not Track

Do Not Track ("**DNT**") is a web browser setting that requests that a web application disable its tracking of an individual user. When you choose to turn on the DNT setting in your browser, your browser sends a special signal to websites, analytics companies, ad networks, plug in providers, and other web services you encounter while browsing to stop tracking your activity. Various third parties are developing or have developed signals or other mechanisms for the expression of consumer choice regarding the collection of information about an individual consumer's online activities over time and across third-party websites

or online services (*e.g.*, browser do not track signals), but there is no universally agreed upon standard for what an organization should do when it detects a DNT signal. Currently, we do not monitor or take any action with respect to these signals or other mechanisms. You can learn more about Do Not Track here.

8. Data Security

Security: Data is at the heart of an IoT business, whether it is personal data or non-personal data. We use industry-standard measures to safeguard all data and have a continuous process in place to test the effectiveness of these measures and to review the threat landscape and new tools available. You have a role to play in security as well, and we ask that you use prudent measures to protect against unauthorized access to your account information, including logging out of your account when finished, not sharing your login information and taking other customary security precautions appropriate for the situation. The type of organizational or technical measures we use to secure our systems and data may differ depending on the sensitivity of the data and our assessment of how accidental or unauthorized disclosure or use of the data could threaten the rights and freedoms of natural persons. If we become aware that the security of any of the personal information that we store or that is stored by our third party service providers has been compromised, we will comply with all applicable laws, including promptly notifying you if required by law.

Contents of Cellular Transmissions. The contents of any SMS, data or voice transmissions made by customer devices over cellular networks are not accessed, viewed or stored by Taoglas. These transmissions are made using standards-based security processes applicable to all cellular operators

Data in Transit. Any traffic sent by or to a device using cellular networks is protected in accordance with cellular security standards, including in most cases encryption. Any data sent over the Internet is not necessarily secure unless it has been encrypted during transit or is sent over a secure channel, such as a VPN. A Taoglas representative will be pleased to discuss when and whether a VPN is appropriate.

Phishing. We are aware that there are people who may pose as legitimate businesses and try to trick you into disclosing personal information that can be used to steal your identity. We will not request your account login or password, your credit card information or any sensitive data that could be used to steal your identity, such as national identifying numbers, in an unsolicited or non-secure email or telephone call. If you believe that someone representing themselves as being associated with Taoglas has requested this information in a contact that you did not request or initiate, please contact us immediately at phishing@taoglas.com so that we may verify the identity of the person contacting you and the validity of the request.

Special Laws. If you pay us by credit card, we and our payment processors protect your payment information in accordance with local laws establishing standards for payment card information. Unless we agree otherwise, however, the data security measures we take are not designed to comply with other laws applicable to specific types of businesses, such as the Health Insurance Portability and Accountability Act (HIPAA). Please contact us if you need more information about this.

9. Data Retention

We and our third party processors will keep personal data in our active operating systems only for as long as necessary to fulfil the purposes we collected it for, including for the purposes of providing services to you or a customer, satisfying any legal, accounting, or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We keep basic information about our customers (including Contact and Identity Data of our customers' representatives) for six years after our relationship with them ceases for tax and other legal purposes. If you send us information in connection with a job application, we may keep it for up to three years in case we decide to contact you at a later date. Thereafter, we and our duly authorised delegates will refrain from collecting any further personal data on you and shall take appropriate steps to dispose of any records containing your personal data, to the extent this is operationally feasible and proportionate. We reserve the right to delete and destroy all of the information collected about you in accordance with our retention policies unless otherwise required by law.

10. Your Legal Rights

Under certain circumstances, you have the following rights under data protection laws in relation to your personal data:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Opting out: You can ask us or third parties to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at marketing-optout@taoglas.com any time. Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase, warranty registration, product/service experience or other transactions.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

- If you want us to establish the data's accuracy.

- Where our use of the data is unlawful but you do not want us to erase it.
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.
- You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Contact Us If you would like to exercise any of the above rights, please contact us at privacy@taoglas.com with your request. We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response. We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

11. Your California Privacy Rights

This section of the Notice applies solely to California residents. We adopt this Section to comply with the California Consumer Privacy Act of 2018 ("**CCPA**") as amended by the California Privacy Rights Act ("**CPRA**"). Any terms defined in the CCPA or CPRA have the same meaning when used in this Section.

California residents have the following rights:

- To know the categories of personal information being collected about you, the purposes for which the categories of information are collected or used, and whether that information is sold or shared;
- To know the length of time we intend to retain each category of personal information;
- To know whether your personal information is sold or disclosed and to whom;
- To access your personal information;
- To delete the information you have provided to us, with certain exceptions;
- To correct your personal information;
- To opt out of the sale of personal information;
- To know if Sensitive Personal Information ("**SPI**") is being collected about you, the categories of SPI being collected, the purposes for which the categories of SPI are collected or used, and whether the SPI is sold or shared;
- To limit the use of your SPI if it is used for cross-contextual behavioral advertising or for the purposes of inferring characteristics about you; and
- Not to be discriminated against, even if you exercise your privacy rights.

The sections above describe in detail what categories of information we collect and the purposes for which we use that information.

11.1. Request for Information, Correction, or Deletion

California consumers have the right to request, under certain circumstances, that a business that collects personal information about the consumer disclose to the consumer the information listed below for the preceding 12 months:

- The categories of personal information collected about you;
- The categories of sources from which the personal information is collected;
- The business or commercial purpose for collecting, selling or sharing personal information;
- The categories of third parties to whom the business discloses personal information; and
- The specific pieces of personal information collected about you.

Please note that if we collected information about you for a single one-time transaction and do not keep that information in the ordinary course of business, that information will not be retained for purposes of a request under this section. In addition, if we have de-identified or anonymized data about you, we are not required to re-identify or otherwise link your identity to that data if it is not otherwise maintained that way in our records.

You can also request that we correct or delete your personal information. There may be certain exceptions to our obligation to correct or delete your information such as if you have an existing account or transaction with us or if we have a legitimate business reason to keep your information.

11.2. Personal Information Collected

We have collected the following categories of Personal Information from consumers within the last twelve (12) months:

Category of Personal Information	Examples of this Category	Sources of Personal Information	Business Purpose for Collection
Identifiers	Real name, alias, postal address, unique personal identifier, online identifier, Internal Protocol address, email address, account name, social security number, driver's license number, passport number or other similar identifiers.	You Automatically Third Parties	To provide our products and Services To provide information you requested To improve our products and Services To identify potential customers To market our products and Services To verify identity To prevent fraud To process payments To comply with law To offer employment, to provide insurance and benefits, for background checks
Personal information described in California Civ. Code § 1798.80(e)	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,	You Automatically Third Parties	To provide our products and Services To provide information you requested To improve our products and Services To identify potential customers To market our products and

Category of Personal Information	Examples of this Category	Sources of Personal Information	Business Purpose for Collection
	debit card number, or any other financial information, medical information, or health insurance information.		Services To verify identity To prevent fraud To process payments To comply with law To manage payroll and provide and administer employee benefits
Characteristics of protected classifications under California or federal law	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or credit, marital status, medical condition (AIDS/HIV status, cancer), 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), political activities or affiliations, familial status, source of income status, status as a victim of domestic violence, assault, or stalking.	N/A	To provide our products and Services to customers To improve our products and Services To offer employment, to provide insurance and benefits, for background checks To comply with law
Commercial information	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	You Automatically	To provide our products and Services To market our products and Services To improve our products and Services To provide information you

Category of Personal Information	Examples of this Category	Sources of Personal Information	Business Purpose for Collection
			requested To comply with law
Biometric information	An individual's genetic, physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA) or activity patterns that can be used to establish individual identity, including images of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health or exercise data that contain identifying information.	N/A	N/A
Internet or other electronic network activity information	Browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.	Automatically	To provide our products and services To market our products and services To improve our products and services (e.g., usage pattern data) To track employee actions for internal reports and information security purposes
Geolocation data	Physical location and/or movements.	You	To market our products and services

Category of Personal Information	Examples of this Category	Sources of Personal Information	Business Purpose for Collection
		Automatically Third Parties	To detect security incidents and protect our Sites
Sensory data	Audio, electronic, visual, thermal, olfactory, or similar information.	N/A	To provide our products and services
Professional or employment related information	Current or past job history or performance evaluations	You	To provide our products and Services To offer employment, to provide insurance and benefits, for background checks
Non-public education information (per the Family Educational Rights and Privacy Act – 20 U.S.C. § 1232g, 34 CFR 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.	You Third Parties	N/A
Inferences drawn from other Personal Information	Information used to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	You Automatically Third Parties	To provide our products and services To market our products and services To improve our products and services To detect security incidents and protect our Site

Category of Personal Information	Examples of this Category	Sources of Personal Information	Business Purpose for Collection
L. Sensitive Personal Information	Social security number, driver's license number, account log-in, debit, or credit card number in combination with password or PIN, precise geolocation (less than 1850 sf radius), racial/ethnic origins, religious or philosophical beliefs, union membership, contents of e-mails or texts to others, genetic/biometric data, health information, sex life/sexual orientation data	You	N/A

Information related to how long we retain Personal Information is included in the Retention of Personal Information section above.

11.3. Personal Information Sold or Shared

We have sold or shared (as those terms are defined in the CCPA) to third parties the following Categories of Personal Information in the last twelve (12) months:

Category of Personal Information	Recipient Categories	Purpose for Sale/Sharing
Identifiers	Advertising, marketing, and analytics providers	Marketing
Commercial information	Advertising, marketing, and analytics providers	Marketing
Internet or other electronic network activity information	Advertising, marketing, and analytics providers	Marketing and analytics
Inferences drawn from other Personal Information	Advertising, marketing, and analytics providers	Marketing

11.4. Personal Information Disclosed for Business Purposes

We have disclosed the following categories of Personal Information for business purposes in the last twelve (12) months:

Category of Personal Information	Recipient Categories	Business Purpose for Disclosure
Identifiers	Internet service providers Data analytics providers Social networks Payment processors Third party business partners	Auditing related to ad impressions Helping to ensure the security and integrity of Personal Information Performing services on behalf of the business Activities to verify or maintain the quality of, improve, upgrade, and/or enhance of our services
Commercial information		Auditing related to ad impressions Helping to ensure the security and integrity of Personal Information Performing services on behalf of the business Activities to verify or maintain the quality of, improve, upgrade, and/or enhance of our services
Internet or other electronic network activity information		Auditing related to ad impressions Helping to ensure the security and integrity of Personal Information Performing services on behalf of the business Activities to verify or maintain the quality of, improve, upgrade, and/or enhance of our services
Inferences drawn from other Personal Information		Auditing related to ad impressions Helping to ensure the security and integrity of Personal Information Performing services on behalf of the business Activities to verify or maintain the quality of, improve, upgrade, and/or enhance of our services

11.5. Do Not Sell My Personal Information

As a California resident, you also have the right, at any time, to tell us not to sell personal information – this is called the "right to opt-out" of the sale of personal information. We do not sell Personal Information, but we recognize that some privacy laws define "personal information" in such a way that making available identifiers linked to you for a benefit may be considered a "sale." To opt-out of this, please click on this link.

Right to Limit Use of Sensitive Personal Information

California consumers have the right to limit the use of each type of Sensitive Personal Information for each purpose with each type of third-party partner. Consumers can revoke this permission at any time. **Currently, we do not provide your Sensitive Personal Information to any third parties other than those service providers that are necessary for us to provide our Services to you.**

11.6. Right Not to Be Discriminated Against

We will not discriminate against you for exercising any of your rights under the CCPA. Unless permitted by California law, 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.

However, as permitted by California law, we may offer you certain financial incentives that can result in different prices, rates, or quality levels. Any permitted financial incentive we offer will reasonably relate to the value of your Personal Information, for instance, if you sign up for a newsletter with us, we may provide you with discounts for future Services. Participation in a financial incentive program requires your prior opt in consent, which you may revoke at any time.

11.7. Third Party Marketing

California Civil Code Section 1798.83 permits our users who are California residents to request and obtain from us a list of what personal information (if any) we disclosed to third parties for their own direct marketing purposes in the preceding calendar year and the names and addresses of those third parties. We do not currently disclose personal information protected under this section to third parties for their own direct marketing purposes.

11.8. Exercising Your California Privacy Rights

You or your authorized agent may make a request to access, correct, delete, opt-out of the sale of your Personal Information, or limit the use of your Sensitive Personal Information by contacting us as follows:

- **Email**: privacy@taoglas.com
- **Address**: Attention Legal Department

4851 Paramount Drive, San Diego, CA 92123

If you use an authorized agent to submit your request, we may require proof of the written authorization you have given. We also may require you to confirm your identity and your residency to obtain the information, and you are only entitled to make this request twice in a 12-month period. For emails, please include “California Privacy Rights” as the subject line. You must include your full name, email address, and attest to the fact that you are a California resident. We will acknowledge your request within 10 days and respond to your request within 45 days or let you know if we need additional time. If you make this request by telephone, we may also ask you to provide the request in writing so that we may verify your identity. If we are unable to honor your request for any reason, we will notify you of the reason within the request time period.

12. Your Privacy Rights under Other US State Laws

If you are a resident of Colorado, Connecticut or Virginia, you have the right, upon a verified request, to:

- To confirm whether a controller is processing your personal data and to access such personal data;
- To correct inaccuracies in your personal data;
- To delete your personal data;
- To obtain a copy of your personal data that you previously provided to us in a portable, and if technically feasible, readily usable format, if processing is carried out by automated means;
- To opt out of the processing of your personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

To exercise these rights, you or your authorized agent may make a request to confirm, access, correct, delete, obtain a copy, or opt-out of the processing of your personal data for targeting advertising, sale, or profiling by using this link or contacting us using the information in the Contact Us section below.

If you use an authorized agent to submit your request, we may require proof of the written authorization you have given. We also may require you to confirm your identity and your residency in order to obtain the information. For emails, please include “Privacy Rights” as the subject line. You must include your full name, email address, and attest to the fact that you are a resident of Colorado, Connecticut or Virginia. We will process your request within 45 days or let you know if we need additional time or cannot process your request. If you make this request by telephone, we may also ask you to provide the request in writing so that we may verify your identity. If we are unable to honor your request for any reason, we will notify you of the reason within the request time period.

12.1. Right to Opt Out Under Applicable State Laws

Residents of Colorado, Connecticut, Nevada and Virginia have the right to opt out of the sale of their Personal Information and targeted advertising. To exercise your right, please click on “Your Privacy Choices” link on the bottom of the webpage where your information is being collected.

California residents may have additional rights, as shown in the Your California Privacy Rights section above.

12.2. Opt-Out Preference Signals

Some browsers and browser extensions support opt-out preference signals such as the Global Privacy

Control ("**GPC**") that can send a signal to the websites you visit indicating your choice to opt-out from certain types of data processing, including data sales. GPC is a web browser-level setting, maintained by either a browser or a browser extension, that a user or privacy-focused technology can set. In certain regions, when we detect such a signal, we will make reasonable efforts to respect your choices as required by applicable law.

12.3. Appeals of Our Decisions

In some states, you may appeal to us if we refuse to take action on your exercise of certain choices described above. To appeal such a refusal, please contact us using the information in the Contact Us section below with the subject line "Appeal of Refusal to Take Action on Privacy Request" and provide the relevant information in the email. If your appeal is denied, residents of certain states can contact their attorney general as follows:

- Virginia Attorney General
- Colorado Attorney General
- Connecticut Attorney General