PRIVACY POLICY

Effective Date: June 22, 2025 (updated)

Introduction

Welcome to Yacht Crew Center LLC ("YCC," "we," or "us"). This Privacy Policy explains how we collect, use, disclose, and protect personal information when you interact with our website, mobile app, and any related services, events, or communications (collectively, the "Site"). We are committed to protecting your privacy and complying with applicable global data protection laws, including the EU and UK General Data Protection Regulations (GDPR/UK GDPR), the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Brazil's Lei Geral de Proteção de Dados (LGPD), Singapore's Personal Data Protection Act (PDPA), Australia's Privacy Act 1988, and other relevant laws. Please read this Policy carefully. By using our Site, you acknowledge that you have read and agree to this Privacy Policy. If you do not agree, please discontinue use of the Site. We may update this Privacy Policy from time to time (see "Updates to this Policy" below).

Scope: This Policy covers personal information we collect through our Site (including any content, features, and services offered) and offline interactions (such as in-person events or customer service calls). It does not cover third-party websites or services that we do not control. We only process personal information as described in this Policy, unless otherwise disclosed to you at the time of collection.

Below is a summary of the sections in this Privacy Policy for easy reference:

- Data Retention – How long we keep personal data.
- Your Rights and Choices – Your privacy rights under GDPR, CCPA/CPRA, LGPD, PDPA, and other laws, and how to exercise them.
- Children's Privacy – Our policy regarding minors.
- California Privacy Rights – Additional disclosures and rights for California residents.
- Updates to this Policy – How we notify you of changes.
- Contact Information – How to reach us or our Data Protection Officer with questions or requests.

Information We Collect

Personal Information: For purposes of this Policy, "personal information" (also known as *personal data*) means any information that identifies, relates to, describes, or can reasonably be linked to an individual. It includes obvious identifiers (like your name or email address), as well as information that can indirectly identify you when combined with other data. We collect both personal information you provide directly and information collected automatically or from third parties. We may also collect non-identifiable information (data that cannot reasonably identify you), and we either do not associate it with an identifiable person or we anonymize/pseudonymize it in accordance with applicable law.

Categories of Information We Collect: We collect (and have collected in the past 12 months) the following types of personal information:

- Identifiers and Contact Details: Name, username, password, email address, telephone number, postal address, and similar identifiers. If you create an account, we may also collect a profile photo or avatar you choose to upload.
- Demographic Information: For example, your age or date of birth, gender, and other demographic attributes you may provide (some of which may be considered protected classifications under law, such as race or ethnicity, which we only collect if you voluntarily provide it in a survey or profile).
- Professional and Education Information: Employment history, qualifications, licenses or certifications, and education history if you submit a résumé or professional profile on our platform.
- Commercial and Transaction Information: Records of products or services purchased, obtained, or considered, and purchasing or consuming histories or tendencies (e.g. if you buy merchandise or services through the Site, we collect billing address, shipping address,

and payment information). Payment card information is processed by our payment processor and is not stored by us, except for basic billing details.

- Content and Submissions: Information you post or upload on our Site, such as comments, reviews, photos or videos, forum posts, survey responses, contest entries, or any feedback. Please note: Any content you choose to make public on the Site (for example, in community forums or reviews) is visible to others at your own risk. We encourage you to be mindful of what you share publicly, as we cannot control third-party access to public postings.
- Geolocation Data: We may collect your general geographic location automatically based on your IP address or device GPS (with your permission). For example, our mobile app may access precise location information if you allow location services, to offer location-based features. We will follow applicable law for obtaining consent to precise location data where required. You may disable location sharing at any time in your device settings.
- Internet or Electronic Network Activity: This includes technical information and usage data automatically collected when you use our Site, such as your IP address, device identifiers, cookie ID, browser type, device type, operating system, access times, pages viewed, links clicked, and the webpage you visited before navigating to our Site. We also collect information about your interactions with our emails and online ads (e.g. if you open or click a newsletter email).
- Analytics and Preference Information: We use cookies and third-party analytics (like Google Analytics) to gather data about your use of the Site, such as the pages or content you view, the features you use, your preferences (language, time zone, etc.), and how you navigate or interact with our Site. Over time, we may combine this usage data with other information we have collected to create a profile of your interests or usage patterns for analytics or personalization purposes. (See "Cookies and Tracking" below for more details on profiling and how you can opt out).
- Communications: Records of our correspondence with you, such as customer support inquiries, and your preferences for receiving communications (e.g. your opt-in to newsletters or marketing).
- Sensitive Personal Data: In limited cases, we may collect information that is considered *sensitive* under certain laws. This might include government-issued identification numbers (like a passport or driver's license number) if you undergo identity verification; health or medical information (for example, if you inform us of a medical condition or disability in connection with attending an event or using our services); biometric identifiers or data (such as a facial image on a photo ID, which could be used for identity verification); precise geolocation; or demographic details like racial or ethnic origin if you volunteer such information. We do not collect sensitive personal data about you unless it is necessary to

provide you a service or required by law, and we will obtain your explicit consent where required. For instance, if we ever implement facial recognition for account security or collect health information for event accommodations, we will do so in compliance with GDPR Article 9 and similar laws, meaning we will have an additional lawful basis (such as your explicit consent or a substantial public interest justification) and apply appropriate safeguards. We will not use or disclose sensitive personal information for purposes other than those permitted by law – for example, under the CPRA (California) we will not use sensitive data (like precise geolocation or racial origin) to infer characteristics about you without your knowledge or beyond what is necessary for providing our services.

Non-Personal and Aggregated Data: We may also collect data that is not personally identifying, such as aggregated statistics or de-identified information. For example, we might track overall usage trends to understand how many users access a certain feature. This information cannot be linked to any individual and is not considered personal data under law. If we ever combine non-personal data with personal information in a way that could identify you, we will treat the combined data as personal information and protect it accordingly.

How We Collect Your Information

We collect personal information from and about you through several methods:

- Directly from You: You provide information to us when you use our Site or communicate with us. For example, when you create an account, fill out forms, enter information on our platform, or contact us for support, you are directly giving us personal data. This includes when you: register for our services (we'll ask for details like name and email), update your profile, submit a job application or résumé, post content or messages on the Site, respond to surveys or contests, or email us with inquiries. Any time you voluntarily provide information to us (whether online or offline), we will collect it and it will be apparent what data you are providing from the context. We will also collect any preferences you communicate to us (such as your marketing email preferences or language selection).

- Automatically Through Technology: Like most websites and apps, we use automated data collection technologies to gather certain information about your device and usage of our Site without you actively submitting it. When you visit or interact with the Site, we (and authorized third parties) set cookies and other tracking technologies (such as web beacons/pixel tags, embedded scripts, and mobile SDKs) on your browser or device that collect technical and behavioral information. This includes device identifiers, IP address, browser type, operating system, referring URLs, clickstream data, and details about how you navigate pages and engage with content. (See "Cookies and Tracking" below for more on how these technologies work and your choices regarding them.) We also log certain information when you access the Site, such as the time and date of access, and error logs if

a page fails to load. This automatic collection is done for purposes like maintaining security, measuring performance, and personalizing your experience.

- From Third Parties and Partners: We may receive information about you from third-party sources. For example: if you register or login via a social network (such as using "Sign in with Facebook/Google"), the third-party platform may share with us certain profile information like your name or friends list, based on their disclosure to you at login and your privacy settings. We might obtain marketing or lead information from business partners or referrals (e.g. if a partner event organizer provides us a list of attendees that includes your info, with the appropriate permissions). We also collect or generate information through service providers we work with – for instance, our analytics providers (like Google Analytics) or advertising partners may provide us aggregated audience insights or reports that include information on your interactions with our Site or ads. If we integrate a third-party service, such as a payment processor or a scheduling tool, they may send us data needed to complete transactions or fulfill services (like confirming a payment was successful). Additionally, if someone refers you to our platform (for example, via a referral program), we may receive your contact info from the referrer. We treat any information we receive from third parties according to the rules of this Privacy Policy, plus any additional restrictions imposed by the source.

We will not collect more information than is necessary for the purposes for which it will be processed. Where required by law or applicable guidelines, we will also inform you at the point of collection whether certain information is mandatory and the consequences of failing to provide it (for example, we might need certain contact information to create an account – without it, we cannot register you).

Device Permissions: Most mobile devices and browsers allow you to control or disable certain data collection. For example, you can disable location services or refuse cookies. Please note that if you choose not to provide or permit certain information (such as by disabling cookies or not providing mandatory fields), some features of our Site may not function properly or may be unavailable. We will respect "Do Not Track" (DNT) signals or equivalent preferences as required by law, though currently there is no universal standard for DNT; you can also manage cookie preferences as described below (see "Cookies and Tracking").

How We Use Your Information

We use personal information for the following business purposes and legitimate interests, all in accordance with applicable law:

- To Provide and Maintain Our Services: We process your information to operate the Site's core functionalities. This includes creating and managing user accounts; authenticating you when you log in; enabling you to search and view content; facilitating transactions or orders

you request; providing the features and services you select; and maintaining the overall operation and security of our platform. For example, we use your login credentials to allow access to your account, and use information about your device to maintain session security. Processing your data for these purposes is generally necessary to perform our contract with you (i.e. our Terms of Service) or to take steps at your request prior to entering into a contract.

- To Present Content and Personalize User Experience: We use data to tailor the content you see and personalize your experience on the Site. For instance, we may use your past browsing activity or profile information to recommend relevant articles, job opportunities, or other content that might interest you. We might remember your language and region to display the Site in the appropriate language and show local events or news. Personalizing your experience is typically based on our legitimate interests in providing a relevant and user-friendly service, and in some cases based on consent (for example, cookie-based personalization in jurisdictions where consent is required).

- To Communicate with You: We use contact information (like your email or phone number) to send you account-related or transactional communications. This includes confirming your registration, sending verification codes, responding to your inquiries or support requests, sending updates about services you've requested, and notifying you of important changes such as changes to our terms or privacy policy. These communications are necessary for customer service and contractual obligations. We may also send you promotional communications about new features, special offers, newsletters, or events that we believe may be of interest to you – you will receive such communications only in accordance with applicable law (e.g. with your consent or opt-in where required). You have the right to opt out of marketing messages at any time (see "Your Rights and Choices" below). If you opt out of marketing emails, we may still send you non-promotional emails, such as those about your account or transactions.

- To Fulfill Requests and Provide Customer Support: If you contact us for assistance or to exercise your rights, we will use your information to verify your identity (if needed) and respond to your request. We may also use information about any problems you report to fix issues (e.g. bug reports). Customer support data and feedback you provide help us improve our services.

- For Analytics, Improvement, and Product Development: We analyze usage information, feedback, and other metrics to understand how our Site is used and how we can make it better. This helps us troubleshoot issues, perform data analysis, test new features, conduct research, and develop new products or services. For example, we might use usage logs to identify slow page load times and optimize site performance, or analyze aggregated trends to decide what new content or features users are most interested in. Where feasible, we use aggregated or de-identified data for these purposes, but some analytics may involve

personal data. These activities are in our legitimate interests to innovate and improve our offerings, and they generally do not outweigh your personal data rights because we use minimal identifying information or statistical aggregation.

- To Show Advertising and Marketing (Including Targeted Advertising): We may use information (such as cookies and inferred interests) to serve you targeted advertisements on our Site or on third-party platforms. For example, if you browse certain content on our Site, we or our advertising partners might show you ads for related services. These ads may be based on your activities on our Site or across other sites over time (this is sometimes called cross-context behavioral advertising or interest-based advertising). We also use analytics to measure the effectiveness of our marketing campaigns – for instance, to learn whether a newsletter resulted in more visits to our Site. We will only engage in targeted advertising in compliance with applicable law – in some regions, this means we will first obtain your consent to certain tracking cookies or deliver only non-personalized ads if you opt out. You can control cookies and advertising preferences as described in the "Cookies and Tracking" section. California residents: see "California Privacy Rights" for how we honor "Do Not Sell or Share" requests for advertising cookies. EU/UK residents: we rely on legitimate interests to process personal data for direct marketing and advertising, but where required, we will seek your consent (e.g., for setting non-essential cookies). You have the right to object to direct marketing at any time (see "Your Rights" section).

- To Ensure Security and Prevent Fraud: We are dedicated to keeping our Site safe and secure. We process personal data as needed to detect, investigate, and prevent fraud, spam, abuse, security incidents, and other harmful or illegal activities. For example, we may use your IP address to determine if an account login attempt is suspicious (e.g. coming from an unusual location), or we might use cookies to impose security measures like CAPTCHA challenges. We may also screen user content for malicious code or scan downloads for viruses. These processing activities are based on our legal obligations to protect data and our legitimate interest in preserving the integrity of our services. In certain cases, we may process sensitive data for this purpose (e.g. using biometric verification to authenticate identity) – if so, we will ensure an appropriate lawful basis such as explicit consent or a substantial public interest in fraud prevention. Ensuring security and compliance with our legal obligations (like record-keeping, sanctions compliance, responding to lawful requests from authorities) are essential purposes for processing your data.

- To Comply with Legal Requirements: We will use or disclose your information if required to do so by law or in the good-faith belief that such use is necessary to comply with applicable laws, regulations, legal processes, or enforceable governmental requests. This includes fulfilling our tax, audit, reporting, and licensing obligations, as well as responding to lawful subpoenas or court orders. For example, if a law enforcement agency lawfully requests user data in connection with an investigation, we may be obliged to provide it. We

also may process your data to exercise or defend legal claims, protect our rights (or the rights of our users or others), or as evidence in litigation. Such processing is grounded in legal obligation or our legitimate interest in legal protection.

- With Your Consent, for Other Purposes: We may use your personal information for any other purpose that you have consented to at the time of collection or processing. If we want to process your data for a purpose that is unrelated to those listed above, we will explain the purpose and, if required by law, obtain your consent. For instance, if we ever wish to use your testimonial or success story on our marketing materials, we would ask for your permission to do so.

We will not use your personal information in a way that is incompatible with the purposes for which it was collected, unless required or allowed by law. If we need to use your information for a new purpose, we will notify you and, if necessary, seek your consent.

Legal Bases for Processing (GDPR/UK GDPR): If you are located in the European Economic Area (EEA) or the UK, we are required to inform you of the lawful bases on which we process your personal data under the GDPR/UK GDPR. We generally rely on the following bases:

- Performance of a Contract: When processing is necessary to perform our contract with you or to take steps at your request before entering into a contract. For example, when we provide services you requested, manage your account, or process payments, we do so on the basis of contractual necessity. Without this data, we cannot provide the requested service.

- Consent: Where you have given us clear consent to process your personal data for a specific purpose. We rely on consent, for instance, to send you promotional emails (when required by law), or to place certain cookies on your device, or if we ever process sensitive personal data that isn't otherwise justified by another legal basis. When we rely on consent, you have the right to withdraw that consent at any time, as easily as it was given. Withdrawal of consent will not affect the lawfulness of processing already carried out.

- Legitimate Interests: We process some data for our legitimate business interests, in a manner that does not outweigh your privacy rights. Our legitimate interests include: improving and securing our services; preventing fraud; customizing user experiences; and marketing our services to consenting individuals. When we rely on this basis, we have balanced our interests against your rights and are confident they do not override your interests or fundamental rights and freedoms. You have the right to object to processing based on legitimate interests (see "Your Rights" below).

- Legal Obligation: When processing is necessary for us to comply with a legal obligation that we are subject to. For example, retaining transaction records for tax and accounting laws, or providing information to authorities if required by law.

- Vital Interests: In rare cases, we may need to process data to protect someone's life or physical safety. (For instance, if you have a medical emergency at one of our events, we might share your known health information with medical responders to protect your vital interests.)

- Public Interest: Typically not applicable to our private business operations, but if ever necessary, we could process data for a task in the public interest or in the exercise of official authority (this is more relevant to public bodies; YCC is a private company and does not perform public tasks).

Where we process special categories of personal data (sensitive data), we ensure an additional condition under GDPR Article 9 is met – usually this will be your explicit consent or that the processing is necessary for compliance with a law or exercise of legal claims. We will make these conditions clear to you whenever we collect sensitive data.

If you have questions about the legal bases or want more detail, you can always contact us (see "Contact Information" below).

How We Share Your Information

We understand the importance of your personal information and share it only as necessary, with appropriate safeguards, and for the purposes described. We do not sell your personal information for money, and we do not share it with third parties for their own independent marketing or advertising without your consent. However, we do disclose personal information to the following categories of recipients, as needed to run our business or comply with law:

- Service Providers ("Processors"): We share personal data with third-party companies that provide services to us under contract, solely for our business purposes. These providers include, for example: cloud hosting providers (for data storage and infrastructure); payment processors (to process transactions); email service providers (to send communications on our behalf); analytics and software tools (to analyze data or perform functionality); customer support software; advertising networks and tech partners (to serve ads and measure ad performance); and security service providers (to help us identify bugs or secure our platform). These service providers act on our instructions and are bound by contractual obligations to keep personal information confidential and use it only for the services they provide to us. We require all our processors to implement adequate data protection measures. For instance, if our Site is hosted on a third-party cloud platform, that provider will process personal data on our behalf to store and retrieve it as you use the Site.

- Business Partners and Integrations: If we offer services or promotions in partnership with other organizations (for example, co-sponsored events, integration with a training provider, or a referral partnership), we might share certain information with those partners with your knowledge. For instance, if you sign up for a webinar co-hosted by YCC and a partner, the

information you provide to register may be shared with that partner for the purposes of hosting the webinar and any follow-up. We will disclose such arrangements at the time of data collection. Any third-party partner will be expected to protect your information consistent with this Policy or provide you with their own privacy notice.

- Social Networks or Other Users (at Your Direction): The Site may allow you to share information or connect with social media services. If you link your account with a third-party platform (like signing in through LinkedIn or sharing content to Facebook), you authorize us to share certain data with that platform, and vice versa, as per their authentication process. Also, any information you post in public-facing areas of our Site (such as a forum post or comment) will obviously be visible to others on the Site. If the Site includes features like user profiles or a directory visible to other members, the personal details you choose to include (e.g. your name, photo, biography) will be accessible to those users. We provide controls in your account settings to limit what information is visible to others, so please adjust these settings according to your preferences.

- Legal and Compliance Disclosures: We may disclose personal information when we believe, in good faith, that such disclosure is necessary to: comply with a legal obligation or request (such as a subpoena, court order, or investigative demand) ; enforce our terms of service or other agreements; respond to claims or protect the rights, property, or safety of YCC, our users, our employees, or the public. This includes exchanging information with law enforcement or regulators (subject to verification and appropriate process) or with other companies and organizations for fraud prevention, spam/malware protection, or other security issues. If we receive requests for user data from government authorities, we will review them carefully and only comply if required by applicable law. Where permitted, we may notify affected users of such requests.

- Corporate Transactions: If we are involved in a merger, acquisition, sale of assets, reorganization, bankruptcy, or other transaction, your personal information may be transferred to a successor or affiliate as part of that deal. We will ensure that any such entity is bound to respect your personal data in a manner consistent with this Privacy Policy. If a change in ownership occurs and results in a new materially different use of your personal information, we will notify you (for example, by email or by posting a prominent notice on our Site) and may also outline choices you have regarding the data (such as deletion, if applicable).

- With Your Consent: We will share your personal information with other third parties only if you have given us consent to do so. For example, if you specifically authorize us to share your contact details with a third-party career coach or training provider so they can offer you services, we will do so with your direction. You have the right to withdraw consent at any time, and we will stop such data sharing going forward.

No Selling of Personal Data: YCC does not sell personal information to third parties for monetary consideration. We also do not disclose personal data to third parties for their independent direct marketing purposes unless you explicitly opt in. In the context of U.S. state privacy laws (like California's CPRA), "selling" or "sharing" can include certain uses of advertising cookies or tracking that allow third parties to collect information from our Site to serve personalized ads to you. We treat such activity as described in the "Cookies and Tracking" section below, and you have options to opt out. Other than that context, we do not exchange your data for compensation. If this ever changes, we will update this Policy and provide required opt-out mechanisms.

Categories of Third Parties with Whom We Disclose Data: In the past 12 months, we have disclosed the above-listed categories of personal information to the following types of entities for our business purposes: service-provider partners (including IT hosting, payment, analytics, marketing and advertising service providers); device or software platforms (such as mobile app stores or social login providers when you connect through them); social media networks (if you intentionally share data via social plug-ins or posts); government or regulatory bodies (when required by law); and affiliated businesses or successors (in corporate transactions). The purposes of such disclosures are consistent with those outlined in this Policy (for example, all categories of personal information are shared with service providers to help us operate and fulfill our obligations, and select categories like Identifiers, Device/Network data, and Commercial data are shared with analytics and advertising partners to optimize our services and marketing). We do not disclose sensitive personal information except to service providers or as required for legal compliance or security purposes, and never for profiling or behavioral advertising without permission.

If you have questions about specific third parties with whom your information may be shared, you can contact us for more information. We aim to be transparent about our data practices.

Cookies and Tracking Technologies

Cookies and Similar Technologies: We use cookies, beacons, and related tracking technologies on our Site to provide and improve our services. Cookies are small text files stored on your browser or device by websites, applications, or advertisements that you interact with. They serve a variety of functions, such as enabling certain features, remembering your preferences, and helping us understand how users interact with our Site. Other technologies we use include pixel tags or web beacons (tiny images embedded in pages or emails that track if you've viewed them) and device identifiers in apps.

We and our third-party partners (like analytics and advertising providers) may use these technologies for the following purposes:

- Technical / Necessary: To enable core site functionality and secure the site. For example, we use cookies to keep you logged in as you navigate between pages, or to load balance and maintain the stability of our servers. These are typically *first-party cookies* set by YCC, and the site cannot function properly without them.
- Preferences: To remember your settings and preferences, such as language, font size, or region, so you don't have to set them every time.
- Analytics: To collect usage information and measure how users engage with our Site. For instance, Google Analytics may set cookies to track pageviews and user actions. This helps us analyze traffic patterns and improve content (e.g., see which pages are popular, how users navigate, what features are used, etc.). We configure these tools to anonymize IP addresses where possible.
- Advertising & Marketing: To support and measure our marketing efforts. Cookies and pixels may be used to deliver relevant ads, limit the number of times you see an ad, and measure the effectiveness of ad campaigns. For example, if you visit our Site, a cookie may remember that you showed interest in our content, and we could later show you a YCC advertisement on another website (this is known as retargeting). Our advertising partners may use their own cookies or similar identifiers to facilitate this. They may also combine information from cookies with other data they have collected about you (for instance, your activity on other sites) to infer your interests and serve you tailored ads – this is profiling for marketing purposes, which, under GDPR, we do on the basis of legitimate interest or consent, as applicable.

Your Choices for Cookies: When you first visit our Site, you may see a cookies notice or banner. In applicable jurisdictions, we will obtain your consent for non-essential cookies. You can always manage cookie preferences through our Cookie Consent Manager (if available on the Site) or by adjusting your browser settings. Most web browsers let you refuse or delete cookies. Please note that if you block all cookies, some parts of our Site may not function optimally. For example, you might not be able to log in or use certain interactive features.

For more information on controlling cookies:

- In your browser settings, you can typically find options under "Privacy" or "Security" to clear or reject cookies.
- To opt out of Google Analytics, Google provides an opt-out browser add-on: tools.google.com/dlpage/gaoptout.
- For interest-based advertising, you can visit industry opt-out sites like the NAI Opt-Out Page or DAA WebChoices Tool (for U.S. users), or Your Online Choices (for EU users). These allow you to opt out of many participating ad networks' tracking cookies. Keep in

mind, opting out does not mean you will stop seeing ads; it means the ads you do see may be less personalized to you.

Do Not Track Signals: “Do Not Track” (DNT) is a setting available in some web browsers that requests that a web application disable its tracking of an individual user. There is currently no consensus on how websites should interpret DNT signals. However, we treat Global Privacy Control (GPC) or similar signals (which can indicate a user’s choice to opt out of certain data sales/sharing under laws like the CPRA) as a valid opt-out request for cookie-based sharing in California. Outside of California, if your browser sends a DNT/GPC signal, our site will still load and trackers will function as described unless you opt out via other means, because there is not yet an industry standard. We encourage you to use the cookie management tools described above to control tracking.

Profiling and Automated Decision-Making: We may analyze user information (e.g. Site activity, preferences, demographics) to segment users or create profiles that help us make decisions – for example, deciding to show certain content or advertisements to a particular segment of users. However, any such profiling is not used to produce legal or similarly significant effects for you without human intervention. In other words, we do not make any decisions about you that are solely based on automated processing (including profiling) which have a legal effect or similarly significant impact on you, as defined under GDPR Article 22. Examples of automated decisions that would fall under this rule include credit approvals, hiring decisions, or insurance eligibility determined by algorithms without human oversight. YCC does not engage in that type of processing.

If in the future we introduce automated decision-making that could significantly affect you (for instance, an automated system that decides whether to approve you for a service, or one that uses AI to filter job candidates without human review), we will only do so as permitted by law. This means we would ensure we have a lawful basis (such as it being necessary for a contract *and* we take steps to safeguard your rights, or obtaining your explicit consent). We would also carry out a Data Protection Impact Assessment (DPIA) in advance to evaluate and mitigate any risks to your rights. Importantly, you would have the right to not be subject to such a decision in most cases, and the right to request human intervention, to express your point of view, and to contest the decision. We will inform you clearly and in advance if any such automated decision-making is being used and ensure your rights are protected.

In summary, while we do utilize technology to tailor user experiences and marketing (which involves some automated processing of personal data), no purely automated decisions with legal or significant effects are made about individuals in our current processes. Should that change, we will update this Policy and provide any required notices/consents.

International Data Transfers

YCC is headquartered in the United States, and our Site is primarily operated from the U.S. If you are located outside the U.S., be aware that your personal information will likely be transferred to and processed in the United States and possibly other countries. These countries may not have the same level of data protection laws as those in your home jurisdiction. However, we take steps to ensure that your personal information receives an adequate level of protection in the jurisdictions where we process it, in compliance with applicable law.

Transfers from the European Economic Area (EEA), UK, or Switzerland: When we transfer personal data from these regions to the U.S. or any country that the European Commission (or relevant authority) has not deemed to have "adequate" data protection, we rely on appropriate transfer mechanisms as required by GDPR/UK GDPR. Our primary safeguard is the use of Standard Contractual Clauses (SCCs) – these are contractual commitments approved by the European Commission (and adopted by the UK) that legally bind the recipient of the data to protect it to EU privacy standards. We have SCCs in place between YCC and our service providers or partners as needed. In some cases, we may also rely on your explicit consent for the transfer (for example, if you initiate a connection to a non-EEA service), or other exceptions permitted by Article 49 GDPR (such as when a transfer is necessary to perform a contract at your request, e.g. when you are an international user requesting our U.S.-based service).

Additional Safeguards: In line with the guidance of regulators and the requirements from the Schrems II decision, we have evaluated our data transfers and implemented supplementary measures where needed. This may include encryption of data in transit and at rest, access controls, and reviewing importer practices. We also assess whether government authorities in the destination country could access your data and ensure, through contractual and technical measures, that the risk to individuals is minimized.

Other International Frameworks: We monitor developments in international data transfer mechanisms. For example, if there is an EU–US or UK–US Data Privacy Framework or other adequacy decision in the future that covers our transfers, we may rely on that as appropriate. At the time of this Policy's update, data exports to the U.S. are handled via SCCs and related measures as described.

Transfers to Other Countries: For transfers to other countries outside the EEA/UK (for instance, to Canada, Brazil, Singapore, or Australia if we engage providers or partners there), we ensure compliance with local transfer requirements. Canada has been deemed adequate by the EU for private-sector data under PIPEDA (so transfers from the EEA to Canada may not require additional safeguards). For Brazil (LGPD), Singapore (PDPA), and others, we contractually require recipients to protect data, and where those laws require consent for cross-border transfer, we will obtain it or rely on an exception (e.g. performance of a contract).

Onward Transfers: If we transfer your data onward from one country to another (for example, from our U.S. headquarters to a service provider in another country), we remain responsible for protecting that data. We will only disclose the data further to third parties (like our service providers) under conditions that ensure continued protection. Any third-party processing personal data from the EU/UK/Switzerland must, by contract, provide the same level of protection as required by our commitments. If we become aware that a third-party is using or disclosing personal data in a way contrary to our instructions or that violates the law, we will take prompt action to stop and remediate that.

Your Rights with Respect to International Transfers: If you are in the EU/UK, you have the right to request details about the safeguards we have in place for transfers of your personal data outside your region. Subject to confidentiality and legal limitations, we will provide you with relevant information (e.g. the categories of data transferred, the mechanism like SCCs, etc.). If you want to exercise this right, please contact us.

By using our Site or providing us information, you consent to the transfer of your personal data to the United States or any other country in which we or our service providers maintain facilities, and to the processing of your information in those jurisdictions. We will always handle your personal data in accordance with this Policy and applicable law, wherever it is processed.

Data Security

We employ a variety of technical and organizational security measures to protect your personal information from unauthorized access, use, alteration, and destruction. These measures are designed to provide a level of security appropriate to the risk of processing your personal data. Our safeguards include:

- Encryption: We use encryption protocols (such as TLS/SSL) to secure data in transit between your browser or device and our servers. Sensitive information (like payment details) is encrypted when transmitted to our third-party payment processors. We also encrypt certain data at rest in our databases or secure environments, especially any sensitive personal data, to add an extra layer of protection.
- Access Controls: We limit access to personal information strictly to our employees, contractors, and service providers who need to know that information to perform their job duties or provide services. They are subject to confidentiality obligations. We maintain role-based access controls and review access privileges regularly. Administrative access to systems storing personal data is logged and monitored.
- Network & System Security: Our servers are protected by firewalls, intrusion detection systems, and other monitoring tools to guard against external attacks. We keep our software, website platform, and applications updated to address security vulnerabilities (and subscribe to threat intelligence to stay aware of emerging risks). We may employ

techniques like anonymization or pseudonymization where suitable – for instance, replacing identifying fields with codes – so that data becomes less identifiable if a breach occurs. Backup and recovery procedures are in place to maintain data integrity and availability.

- Testing and Training: We conduct regular security assessments, penetration testing, and audits (internally or via third parties) to evaluate the effectiveness of our security controls. We also train our staff on privacy and security best practices, including how to identify phishing attempts or social engineering that could compromise data. Our internal policies and incident response plans help ensure we react quickly if an issue arises.
- Vendor Due Diligence: When we engage service providers who will handle personal data, we vet their security practices and require them to have appropriate security controls. We include data protection provisions in contracts, and where needed, we conduct periodic reviews or request security certifications (like SOC 2, ISO 27001) or audits from those vendors to ensure ongoing compliance.
- Physical Security: For any physical facilities or servers we use, we implement controls such as restricted access, surveillance, and secure disposal of hardware that stores personal data. If we use cloud infrastructure, we rely on reputable providers with robust physical security and redundancy.

Despite our efforts, please be aware that no security measures are perfect or impenetrable. The transmission of information via the internet is not completely secure, and we cannot guarantee absolute security of your data. You are also responsible for maintaining the confidentiality of your account credentials and for any activity under your account. Please use a unique, strong password and do not share it. If you believe your account or interaction with us is no longer secure (for example, if you feel your password has been compromised), please notify us immediately so we can take appropriate action.

In the event of a data breach involving your personal information, we will act promptly to identify, contain, and investigate the issue. We will notify affected individuals and relevant authorities as required by law (for instance, we will follow the GDPR/UK GDPR requirement to report certain personal data breaches to supervisory authorities within 72 hours and to individuals without undue delay, where the breach is likely to result in a high risk to rights and freedoms). Similarly, we will comply with any applicable breach notification laws in other jurisdictions (such as PIPEDA in Canada or state laws in the U.S.).

Data Retention

We will retain your personal information only for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting

requirements. The precise duration we keep data can vary depending on the type of information and the context in which it was collected:

- Account Information: If you have an account with us, we retain your account data while your account is active and for a reasonable period afterward in case you decide to reactivate or there are issues to resolve. If you choose to delete your account (or if we close it due to inactivity or as per our Terms), we will delete or anonymize the personal information in your account within a specified timeframe, except for data we are required or permitted to keep longer (e.g. for legal compliance or legitimate business interests).
- Transaction Data: We keep records of purchases, payments, and financial transactions for at least the duration required by tax and financial regulations (which can be 7 years or more in some jurisdictions).
- Communications: Emails or communications you send us may be retained for a period to assist with ongoing matters or our records. Support tickets and customer service chat logs are usually kept for a set time (e.g. 2 years) in case of follow-up needs.
- Marketing Data: Information used for marketing (such as your email for newsletters) is kept until you opt out or withdraw consent, or the information becomes outdated. After you unsubscribe from marketing communications, we may keep your contact details on a suppression list to ensure we respect your opt-out.
- Usage Data: Analytics data is often collected in aggregate form and not tied to you after initial analysis. Raw logs may be kept for a short period (e.g. a few months) then either deleted or anonymized. Some high-level aggregated analytics may be kept longer for trend analysis, but without personal identifiers.
- Legal Holds: We might need to retain data beyond our standard retention periods if it's subject to a legal hold or relevant to a dispute, investigation, or litigation. In such cases, we preserve the data until the hold is lifted or the matter resolved, then securely delete it.
- Backups: Even after data is deleted from our active systems, it may persist in backups for a short period. We have processes to eventually purge or overwrite backups containing personal data in line with our retention schedule, except where archives must be retained longer for legal reasons.

When the retention period for a given piece of data expires, or if you request deletion and we have no lawful basis to keep it, we will either securely erase your personal information or anonymize it (so it can no longer be associated with you). For example, rather than simply deleting a record, we might strip out personal identifiers and keep a statistical record (which is no longer personal data).

If you have any specific questions about our data retention practices (for example, if you want to know how long we keep a particular type of data), you can contact us for further information.

Your Rights and Choices

You have several rights regarding your personal information and how we handle it. We are committed to respecting these rights and have processes to enable you to exercise them. Your principal rights (which may apply depending on your location and the applicable law) are:

- Right to Be Informed: You have the right to be informed about the collection and use of your personal data. This Privacy Policy is one of the ways we fulfill this right by providing transparent details about our data practices. If you have questions not answered in this Policy, you can contact us for more information.
- Right of Access: You have the right to request access to the personal information we hold about you. This is sometimes called a "Data Subject Access Request." Upon verification of your identity, we will provide you with a copy of your personal data along with details on how we use it, who we share it with, and how long we intend to keep it, as required by law. For example, under GDPR, you can request: the purposes of processing, categories of data, recipients of the data, and the source of data if not collected directly from you. We will provide this information free of charge, within the timeframe required by law (typically within one month for GDPR, extendable if the request is complex).
- Right to Rectification: We want to ensure that your information is accurate and up-to-date. You have the right to request that we correct or update any personal information that you believe is incorrect or incomplete. For instance, if you find that your contact details or preferences are wrong in our records, you can ask us to correct them (and in many cases, you can directly update them by logging into your account). We will make the corrections as soon as possible.
- Right to Erasure: Also known as the "right to be forgotten," this right allows you to request the deletion of your personal data in certain circumstances. For example, if the data is no longer necessary for the purposes it was collected, or if you withdraw consent and we have no other legal basis, or if you object to processing and we have no overriding legitimate interest, or if we unlawfully processed your data, you can ask us to delete it. We will assess your request and, if warranted, erase the data. Note: This right is not absolute – sometimes we may retain certain information if allowed by law (e.g., we might refuse deletion of a transaction record we need for legal compliance). If that occurs, we will explain our reasoning.
- Right to Restrict Processing: You have the right to request that we limit the processing of your personal data in certain scenarios. For instance, if you contest the accuracy of your data, you can request restriction while we verify the data's accuracy; or if you object to our processing based on legitimate interests, you may request restriction pending verification of whose interests prevail. When processing is restricted, we will still store your data but

not use it until the restriction is lifted (unless for legal claims or with your consent). We will inform you before lifting any restriction.

- Right to Data Portability: For data you have provided to us and that we process by automated means on the basis of consent or contract, you have the right to receive that data in a structured, commonly used, and machine-readable format and to have it transmitted to another controller where technically feasible. In other words, you can ask for an electronic copy of your data (for example, your profile information and content you provided) and, if possible, have us send it directly to another company's system at your request. This is to facilitate your ability to reuse your data across different services.

- Right to Object: You have the right to object to our processing of your personal data in certain cases. You can always object to processing for direct marketing purposes – if you object, we will stop using your data for marketing (and related profiling) immediately. You can also object when we are processing your data based on legitimate interests or public interest, and you have particular grounds to object due to your situation. We will then cease processing unless we have compelling legitimate grounds that override your rights or if we need to continue for legal claims. For example, you might object to analytics processing of your data – we would consider your request and either stop the processing or justify why our interests should override (taking into account any impact on you).

- Right to Withdraw Consent: If we are processing your personal data based on your consent, you have the right to withdraw that consent at any time. This will not affect the lawfulness of any processing done before withdrawal. For instance, if you consented to receive newsletters, you can opt out (withdraw consent) via the "unsubscribe" link in our emails or by contacting us, and we will cease sending you newsletters. If you consented to cookies, you can withdraw by updating your cookie preferences. There may be cases where withdrawing consent for one service (e.g., location services) doesn't mean we delete data already collected under consent – but we will stop any further processing of that data and, if required, delete or anonymize it.

- Rights Related to Automated Decisions: As noted, we do not engage in solely automated decision-making with legal effects. However, if you believe you have been subject to an automated decision by us in error, you have the right to request human review of that decision, to express your viewpoint, and to contest the decision. We will provide a meaningful explanation of the logic involved and honor your rights in this regard.

- Right to Complain: If you have concerns about our data practices, we would appreciate the chance to address them directly. However, you also have the right to lodge a complaint with a supervisory authority or regulator. For EU residents, you can contact your country's Data Protection Authority (DPA) or the lead DPA of our EU operations (if applicable). For UK residents, you can complain to the UK Information Commissioner's Office (ICO). For

Canada, you can reach out to the Office of the Privacy Commissioner of Canada (OPC). For Australia, the Office of the Australian Information Commissioner (OAIC). For Singapore, the Personal Data Protection Commission (PDPC). We would ask that you kindly attempt to resolve any issue with us first, but you have the right to go directly to the regulator.

Exercising Your Rights: Most of the above rights can be exercised by contacting us via the contact details provided in the "Contact Information" section. To protect your privacy, we will need to verify your identity before fulfilling a rights request (for example, by asking you to confirm certain information that we have on file, or to log into your account or respond to a confirmation email). Verification steps will depend on the sensitivity of the data and the nature of the request. If an authorized agent is making the request on your behalf (as allowed by certain laws like the CPRA), we will require proof of authorization and still take steps to verify *you* (to prevent fraud).

We will respond to your request within the timeframe required by law. Under GDPR, that's generally within one month (which can be extended by two further months for complex requests with notification to you). Under CCPA/CPRA, we aim to respond within 45 days (with the possibility of a 45-day extension). If we need an extension or cannot comply with your request (due to a legal exception), we will inform you of the reason.

No Fee Usually Required: You will not have to pay a fee to exercise these rights. However, if a request is manifestly unfounded or excessive (for instance, repetitive requests), we may charge a reasonable fee or refuse to act on it – but we will explain our reasoning in such cases.

Additional Rights for Specific Jurisdictions: We have described the core rights above, many of which are granted by GDPR and mirrored in other laws. Depending on where you live, you might have some additional or slightly different rights:

- *Brazil (LGPD):* In addition to the rights above, Brazilian users have the right to confirmation of the existence of processing and to anonymization, blocking, or elimination of unnecessary or excessive data or data processed in non-compliance with LGPD. You also have the right to request information about entities with which we have shared your data and the right to object to processing in cases of non-compliance. We will respond to LGPD requests in accordance with the timelines and procedures of the law. If you withdraw consent or refuse to provide it, we will inform you about the consequences of such denial (e.g., certain services may not be deliverable), but we will not refuse services to you unless the data in question is strictly necessary. YCC has appointed a Data Protection Officer for LGPD purposes (see Contact Information) whom you may contact in Portuguese or English.
- *Canada (PIPEDA):* Canadian individuals have rights to access their personal information and request correction of any inaccuracies. You also have recourse if you feel we violate

PIPEDA – you can complain to the federal Privacy Commissioner. We will always provide the name or title of the person accountable for our privacy compliance when you inquire. We will assist you in understanding our data practices (principle of openness) and provide copies of records in understandable format. Some information may be exempt from access under PIPEDA (e.g., if it involves someone else's personal data or proprietary info), but we will explain any refusal.

- *Australia (Privacy Act):* Australian users can request access to their personal information and correction of it under Australian Privacy Principle (APP) 12 and 13. We will generally provide access unless an exception applies (e.g., if it unreasonably impacts others' privacy or is frivolous/vexatious). We also handle complaints under the Privacy Act – if you have a privacy complaint, please contact us. We will acknowledge it promptly and respond, and if you are not satisfied, you can contact the OAIC. We also note that under APP 1, you can request to remain anonymous or use a pseudonym where practicable – for many aspects of our Site, you can choose what information to include in your profile or communications, though some core details (like an email for login) are needed to provide service.

- *Singapore (PDPA):* Individuals in Singapore have the right to request access to personal data and to be informed about how it has been used or disclosed in the past year. You also can request corrections if data is inaccurate. We will respond to access requests as soon as reasonably possible (within 30 days if possible). We may charge you a reasonable cost for handling an access request, as allowed by PDPA, and will provide you a written estimate upon request. You also have the right to withdraw consent at any time with reasonable notice. Please note that we may refuse access or correction in circumstances allowed by PDPA (such as if it would threaten someone's safety or reveal third-party data, or if an exemption applies). If we refuse, we will provide you with the reason to the extent permitted by law. Our Data Protection Officer (contact below) is responsible for handling PDPA inquiries and requests.

- *Other U.S. States:* If you are a resident of certain U.S. states (such as Virginia, Colorado, Connecticut, or Utah from 2023 onwards), you may have similar rights under those states' privacy laws: the right to access, correct, delete, obtain a copy of personal data, and opt out of targeted advertising, sale of personal data, or certain profiling. YCC will honor valid requests from residents of these states in accordance with their laws. For example, if you're a Virginia resident, you can appeal a refusal of your privacy request by contacting us and indicating you are appealing a prior decision (we will respond within 60 days with an explanation). These state laws also prohibit discrimination against you for exercising your rights. We do not engage in profiling that produces legal or similarly significant effects without human involvement as described earlier. We do not sell personal data as defined by these laws. If we engage in targeted advertising, you can opt out as described in Cookies/Tracking or by contacting us.

Managing Communication Preferences: In addition to formal rights, you have control over certain uses of your information:

- Marketing Emails: You can unsubscribe from our marketing emails at any time by clicking the "unsubscribe" link in any promotional email, or by adjusting your account preferences if logged in, or by contacting us. Please note it may take a few days to process and for all our systems to reflect the change, and you may still receive service-related (non-marketing) communications.
- Push Notifications: If our mobile app sends push notifications, we will seek your consent to do so. You can disable push notifications at any time in your device settings.
- Cookies/Ad Choices: As discussed, use our cookie manager or browser settings to refuse cookies, and opt-out tools for ads if you want to reduce targeted advertising.

We strive to make exercising your rights as straightforward as possible. If you need assistance or have questions about your privacy rights, you can always reach out to us at the contact details below. We will not retaliate or deny you goods or services for exercising your rights in good faith.

Children's Privacy

Our Site and services are not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13 years old. In fact, children under 13 are prohibited from accessing or using the Site. If you are under 13, please do not use our Site or send us any personal information

If we learn that we have inadvertently collected personal information from a child under 13 (or under the applicable minimum age in other jurisdictions, which may be 16 under GDPR without parental consent), we will take prompt steps to delete such information from our records. Parents or legal guardians who believe their child may have provided us personal data without their consent can contact us, and we will work to delete it.

For users between 13 and 18: Our Site may be used by minors 13 or older (for example, perhaps young individuals interested in yacht careers) but only with appropriate consent and supervision of a parent or guardian where required by law. If you are in the European Union, note that the GDPR requires parental consent for processing personal data of children under 16 for online services (unless Member State law sets a younger age, not below 13). We do not knowingly offer services to or process data of children under 16 in the EU without such consent. If you are a minor over 13, we advise you to use our Site only with parental guidance and to not share any sensitive personal information.

We urge all users under the age of majority to use caution on the internet and not share personal details without parental permission. YCC will never knowingly request personal data from children for any promotional or marketing purposes.

If you have questions about our practices regarding children's personal information, or if you believe we have mistakenly collected such information, please contact us so we can investigate and promptly address the issue.

California Privacy Rights

If you are a California resident, you have specific privacy rights under California law, including the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). This section applies solely to individuals who reside in California and is intended to comply with CCPA/CPRA requirements. It describes the categories of personal information we have collected, the sources of that information, the business or commercial purposes for collection, the categories of third parties to whom we disclose personal information, and your California-specific rights. This section should be read together with the rest of our Privacy Policy.

Categories of Personal Information: In the preceding 12 months, we have collected the following categories of personal information (as defined by CCPA) about California consumers:

1. Identifiers: e.g., real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, or other similar identifiers.
2. Customer Records (Cal. Civ. Code §1798.80(e)): e.g., telephone number, billing address, credit card or debit card number (through our payment processor), or other financial information (note: we do not store full payment card details ourselves, but our service providers might process them).
3. Protected Classification Characteristics (under California or federal law): e.g., age (over 40), sex, race, ethnicity, nationality, disability, or other protected traits if you voluntarily provide them (for instance, in a survey or profile). We do not require this information, but it could be collected if shared by the user (such as indicating ethnicity on a profile).
4. Commercial Information: e.g., records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies on our Site.
5. Internet or Other Electronic Network Activity: e.g., browsing history, search history, information on your interaction with our website, app, or advertisement (this includes analytics and cookie data such as device identifiers, pages viewed, and clicks).
6. Geolocation Data: e.g., general location or precise geolocation if you have enabled location services (e.g., location of your device or IP-based location).
7. Professional or Employment-Related Information: e.g., your job title, work history, qualifications, or other professional information if you provide it in a profile or resume on our platform.

8. Education Information: e.g., information about your educational background, degrees, or certifications if you provide it to us (noting that "education information" as defined in CCPA refers to information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act).

9. Inferences: We may draw inferences from the information in the above categories to create a profile reflecting a consumer's preferences, characteristics, behavior, or attitudes. For example, from your browsing or purchasing behavior, we might infer your interests or likelihood of being interested in certain offers.

Categories of Sensitive Personal Information (SPI): In the last 12 months, we may have collected information that CPRA deems "sensitive personal information," such as: account login with password (for your account on our Site), precise geolocation, racial or ethnic origin (if you provided it), or health information (if you disclosed a health condition). We do not use or disclose sensitive personal information for purposes other than those which are necessary to provide the services or as otherwise permitted by CPRA regulations. For instance, if we have your account login credentials (username/password) and financial info, we use those only to provide you access and process transactions (not to infer characteristics or for secondary purposes). If we ever were to use SPI beyond the permitted "service" purposes, we would provide a "Limit the Use of My Sensitive Personal Information" option as required by law. As of the effective date of this Policy, we only use SPI for essential business purposes (such as performing the services or ensuring security) and do not use or disclose it in a way that triggers the right to limit under CPRA.

Sources of Personal Information: We collect personal information from the sources described in the "How We Collect Information" section of this Policy. These include: directly from you (e.g., when you provide information or content); automatically from your devices (through cookies and similar tech); and from third-party sources (partners, analytics providers, etc.). See that section for more details on each source type.

Purposes for Collecting Personal Information: We collect and use personal information for the business or commercial purposes described in the "How We Use Your Information" section. In summary, those purposes include: to provide and manage our services; to communicate with you; to improve and develop our offerings; for personalization; for marketing and advertising; for security and fraud prevention; and to comply with legal obligations. We do not use personal information for purposes materially different from those disclosed. If we do, we will obtain consent if required. We may also use the information for any other purpose with your consent.

Each category of personal information listed above is used for one or more of the purposes identified. For example:

- Identifiers are used to create your account, facilitate communication, process orders, and for marketing (with consent or as allowed).

- Internet activity information is used for analytics, site functionality, personalization, and advertising.
- Professional or Education info might be used to match you with relevant job opportunities or content on our platform.
- Geolocation is used to tailor content to your area or for security (detect unusual logins).
- Protected classifications (if provided) might be used in aggregate for diversity insights or to ensure content relevance, but we do not use sensitive traits to discriminate in service delivery.

Disclosure of Personal Information: In the last 12 months, we have disclosed the above categories of personal information to third parties for various business purposes (as described in "How We Share Your Information"). The categories of third parties to whom we disclose personal information include:

- Service providers (processors) that work on our behalf, such as cloud hosting services, payment processors, analytics providers, email delivery services, advertising networks (for limited use in showing ads), etc. (Applicable to all categories of personal info as needed for them to perform their functions).
- Business partners or affiliates, in cases of joint offerings or within our corporate family (if any). (Mostly identifiers and commercial info, if applicable).
- Advertising and analytics partners (we may allow them to collect internet activity via cookies on our Site for analytics and ad personalization purposes – these partners could be considered third parties to whom we "share" data under CPRA's definition of cross-context behavioral advertising).
- Government or legal entities as required by law (could involve any category necessary for compliance – e.g., identifiers for a subpoena response).
- Others at your direction, such as other users or third parties when you intentionally interact or direct us to share information (e.g., sharing your profile with an employer, or posting content viewable by others).

We have not sold personal information for monetary value. We have "shared" personal information (specifically identifiers and internet/electronic activity via tracking technologies) with third-party advertising networks for the purpose of cross-context behavioral advertising in the past 12 months, in the sense that those third parties may have collected information about users on our Site to show ads elsewhere. Under CPRA, "sharing" is defined as disclosing information to a third party for targeted advertising. We treat such activity as sharing and honor opt-outs accordingly (see below).

Your California Privacy Rights: As a California resident, you have the following rights with respect to your personal information (some of which are similar to those described in the global "Your Rights" section, and some which CPRA specifically provides):

1. Right to Know: You have the right to request that we disclose what personal information we have collected, used, disclosed, and (if applicable) sold/shared about you in the past 12 months. This includes the specific pieces of personal information we collected about you; the categories of personal information; the categories of sources; the business or commercial purposes for collecting or selling/sharing; and the categories of third parties to whom we disclosed that information. Much of this information is provided in this Privacy Policy. Upon verifying your request, we will provide: the categories of personal info collected; categories of sources; categories of personal info we disclosed for a business purpose or shared; categories of third parties to whom info was disclosed/shared; and the specific pieces of personal info we collected about you (data portability request). You may request this information up to twice in a 12-month period and it will cover the preceding 12 months (or you can request information beyond 12 months if the law permits and if it's available).

2. Right to Delete: You have the right to request deletion of personal information we have collected from you and retained, subject to certain exceptions. Once we receive and confirm a verifiable deletion request, we will delete (and instruct our service providers/contractors to delete) your personal information from our records, unless an exception applies. We may deny deletion if retaining the information is necessary for us or our service provider to, for example: complete a transaction or service you requested; detect security incidents or protect against illegal activity; exercise free speech or ensure another consumer's right to free speech; comply with a legal obligation; or for certain internal uses that are lawful (these are CCPA exceptions). If we deny the request in part, we will do so only to the extent permitted by law and will delete any other information not subject to the exception.

3. Right to Correct: You have the right to request that we correct any inaccurate personal information we maintain about you. Upon verifying your identity and the accuracy issue, we will use commercially reasonable efforts to correct the information (taking into account the nature of the personal information and purposes of processing). In some cases, we may delete the information as an alternative to correcting it, if that would not negatively impact you and if permissible.

4. Right to Opt Out of Sale or Sharing: You have the right to opt out of the "sale" of your personal information or the "sharing" of your personal information for cross-context behavioral advertising. While YCC does not sell personal data for money, we do engage in online advertising practices that may be considered "sharing" under CPRA (i.e., allowing third-party ad trackers to collect data for showing you ads). If you wish to opt out

of such sharing, you can use the "Do Not Sell or Share My Personal Information" link on our website (typically found in the footer or via our Cookie Consent tool). You can also broadcast an opt-out preference via the Global Privacy Control (GPC) signal on supported browsers; we treat GPC as a valid opt-out of sharing for that browser/device/profile. Once you opt out, we will stop sharing your data for advertising. Additionally, we do not knowingly sell/share personal info of consumers under 16 without affirmative authorization.

5. Right to Limit Use of Sensitive Personal Information: If we use or disclose sensitive personal information beyond what is necessary to provide our services or other exempt purposes, California residents have the right to direct us to limit the use and disclosure of SPI to those allowable purposes (essentially, to stop using SPI for secondary purposes like profiling or advertising). As noted, we currently do not use SPI for such purposes that would trigger this right. If in future we do, we will provide a "Limit Use of My Sensitive Personal Information" control on our site.

6. Right of No Retaliation/Non-Discrimination: We will not discriminate against you for exercising any of your CCPA rights. This means we won't deny you goods or services, charge you different prices, or provide a different level or quality of service just because you exercised your rights (as per CCPA's non-discrimination clause). If you have a loyalty program or financial incentive tied to your data, we will explain that separately and obtain opt-in consent; currently, we do not offer such programs.

Submitting Requests: To exercise your access, deletion, or correction rights described above, please submit a verifiable consumer request to us by either: (a) emailing us at privacy@yachtcrewcenter.com; or (b) mailing your request to us (see Contact Information below). Please include "California Privacy Rights Request" in the subject line of an email or on the envelope of a mailed request, and specify which right you seek to exercise (access, deletion, correction, opt-out, etc.). Provide sufficient information that allows us to verify you (such as your name, email, and details of your interactions with us), and describe your request with enough detail that we can understand and respond to it.

If you have an account with us, we may also provide self-service tools for certain requests (e.g., you can download your data or delete your account from the account settings when logged in). We may ask you to log in to your account to verify identity for certain requests, which is a secure method. For deletion or access, we might require additional confirmation via email or other means to ensure the request is from you.

Only you, or someone legally authorized to act on your behalf, may make a verifiable consumer request related to your personal information. Authorized agents must provide proof of authorization (such as a written permission signed by you). We will also generally require the

consumer to verify their identity directly with us (or confirm to us that they provided the agent permission), as allowed by law, especially for sensitive requests like access or deletion.

We aim to respond to verifiable requests within 45 days of receipt. If we need more time (up to an additional 45 days, for 90 days total), we will inform you of the reason and extension in writing. If you have a password-protected account with us, we will deliver our written response to that account (e.g., via secure message or notification). Otherwise, we will deliver via mail or email, depending on what you prefer. Any disclosures will cover the 12-month period preceding our receipt of the request, unless you request a longer timeframe and we are allowed to provide it. For data portability requests (specific pieces of data), we will select a format to provide your information that is readily usable and should allow you to transmit it to another entity (like a CSV or JSON file).

If we cannot comply with a request, we will explain the reasons in our response. Common reasons might include inability to verify identity, conflicts with legal requirements, or the request falling under an exemption. For example, we will decline overly broad requests or those that would adversely affect the rights of others (like deleting data we need to complete a transaction or that contains someone else's personal info).

For opt-out of sale/sharing requests, we will comply as soon as feasibly possible, and at most within 15 business days of receiving the request. You do not need to create an account to exercise opt-out. We will honor opt-out preferences going forward and, per CPRA, we will wait at least 12 months before asking you to re-authorize selling or sharing if you've opted out.

Shine the Light: Separately from CCPA, California's "Shine the Light" law (Civil Code § 1798.83) allows customers to request certain information about our disclosure of personal information to third parties for their direct marketing purposes in the preceding calendar year. We do not disclose personal information to third parties for their own direct marketing without consent. Thus, a Shine the Light request should yield that we have not shared data for such purposes. Nevertheless, California residents may submit a Shine the Light inquiry to our contact address for completeness.

We hope this California section has clarified our practices and your rights. If you have any questions or concerns about your California privacy rights or how to exercise them, please contact us at the details provided below. We are committed to complying with these laws and to ensuring you can exercise your rights.

Updates to this Policy

We may update or revise this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or for other operational reasons. When we make changes, we will post the updated Policy with a new "Effective Date" at the top. If the changes are significant, we will provide a more prominent notice or seek your consent where required by law. For example,

we might display a notice on our website or send you an email notification if we have your contact information.

Please review this Policy periodically to stay informed about how we protect your information. Your continued use of our Site after any changes to this Privacy Policy constitutes your acceptance of the revised terms (to the extent permitted by law). If you do not agree with the changes, you should discontinue use of the Site and services.

For material changes that affect previously collected personal data, we will obtain consent or give a clear opportunity to opt out, if required by applicable laws (e.g., if we were to materially broaden our use of your data in a way that the law deems requires consent). We will also keep prior versions of this Privacy Policy available for review (for example, by maintaining an archive or noting the changes in an update log) so you can see what changed.

Contact Information

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us. We are here to help and will respond as promptly as possible.

- Email: contact@yachtcrewcenter.com
- Postal Address: *Privacy Officer / Data Protection Officer*

Yacht Crew Center LLC (YCC)
1211 Golden Lake Loop
St. Augustine, FL 32084
United States
Attn: Privacy Officer/Data Protection Officer

For GDPR/UK GDPR inquiries or requests, you may contact our Data Protection Officer at the above email or address. Our DPO is responsible for overseeing questions about this Policy and our compliance. You also have the right to lodge a complaint with the relevant supervisory authority as noted in "Your Rights."

For LGPD (Brazil): You may contact our Data Protection Officer ("Encarregado") at the above contact details. We will respond in Portuguese or English as needed.

For Singapore PDPA: You may contact our Data Protection Officer at the above email/address. Please indicate that your inquiry is related to PDPA.

For Australia: You may contact our Privacy Officer at the contact information above.

We value your privacy and trust. Thank you for taking the time to read our Privacy Policy. If anything remains unclear, or if you need further clarification, do not hesitate to reach out. We appreciate the opportunity to address your questions and to continue to improve our practices in protecting your personal information.