Table of Contents

Privacy Policy

Last Updated: September 28, 2023

1 Introduction

At Prime Electric, Inc. ("Prime Electric," "we," "us," or "our"), we [and our subsidiaries and affiliates] respect the privacy of our users. This general privacy policy ("Privacy Policy" or "Policy") outlines our data handling practices and explains how we collect, use, and disclose personal information. We encourage you to read this Policy carefully to understand these practices.

1.1 Purpose of the Privacy Policy

The purpose of this Privacy Policy is to transparently communicate how Prime Electric handles your personal information. This includes the types of information we collect, how it is used, and the rights and choices you have concerning its use. This Policy aims to provide you with all the information you need to make informed decisions about your interactions with us.

By using our Services, you acknowledge that you have read, understood, and agree to the practices described in this Privacy Policy. If you do not agree with our policies and practices, your choice is to discontinue use of our Services.

1.2 Scope and Applicability

This Privacy Policy describes our practices and outlines the various contexts, platforms, and services ("Services") in which we may collect, use, maintain, protect, disclose, and process your personal information. These Services include:

- **Digital Interactions**: This encompasses your online engagements with us, which may occur through:
  - Our Websites: Any that link to this Privacy Policy, including https://www.primee.com/.
  - Social Media and Affiliates: Interactions on our social media pages and engagements with our affiliates.
  - Other Digital Platforms: Includes interactions such as clicking on our ads on third-party sites and to our electronic communications.
- **Transactional Activities**: Such as making a purchase or engaging in any other form of transaction with us.
- **Customer Service**: Including communications with our service representatives or features via chat functions, email, text, or phone.

- **Physical Locations**: Such as visiting our offices or jobsites, where we may collect information related to your visit, including video and audio security footage or your use of our Wi-Fi network.
- **Third-Party Information**: This policy also extends to information we may collect about you from third parties, even in the absence of direct interactions with us.

Our privacy practices are designed to adhere to all applicable laws and regulations. Certain provisions may or may not apply to you based on your jurisdiction, as detailed in specific sections throughout this Privacy Policy.

1.3 What is Personal Information

Personal Information (or Personal Data) refers to any information that is directly or indirectly linked to you or your household. Not just your name or email, Personal Information can be anything that identifies, relates to, or could reasonably be connected with you, whether something simple like your age or more complex data like your online activity.

2 Data Protection Principles

This section outlines the fundamental principles that govern our data protection practices. These principles are designed to ensure the responsible and transparent handling of your personal information.

2.1 Lawfulness, Fairness, and Transparency

We are committed to handling your personal information with lawfulness, fairness, and transparency. Our data practices comply with applicable laws, and we aim to be clear about how your information is used. This ensures you can make informed decisions about your interactions with us.

2.2 Purpose Limitation

We only collect and process your personal information for specified, explicit, and legitimate purposes. We do not further process your data in ways incompatible with those purposes.

2.3 Data Minimization

We limit our collection and processing of personal information to data that is relevant and not excessive in relation to the purposes for which it is processed. We take measures to delete or anonymize data when no longer needed.

2.4 Accuracy

We take reasonable steps to keep your personal information accurate, complete, and up to date as necessary for the purposes outlined in this Policy.

2.5 Integrity and Confidentiality

We are committed to ensuring the integrity, confidentiality, and security of your personal information. This involves taking appropriate technical and organizational measures to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to data. For a more detailed discussion on the specific security measures we have in place, please refer to Security.

3 How We Obtain Information

We obtain the information we collect about you through various means and sources, including:

3.1 Direct Interactions

We collect information directly from you when you submit forms, make purchases, register for services, participate in surveys or contests, communicate with us via phone, email, online chat, or otherwise, or use other features of our services. This information may include contact details, financial information, and other personal information depending on the nature of your interactions.

3.2 Automated Technologies

We may use various automated tools, including cookies, to collect certain information. These tools can help us improve site performance, understand how our services are being accessed and used, and provide customized content and advertising.

3.2.1 Cookies

Cookies are small text files that websites send to your computer or device to uniquely identify your browser or mobile device or to store information in your browser setting. We use cookies for a variety of reasons, including to offer and provide our services, understand usage, and customize advertising. You can disable cookies through your browser settings, but some features of our services may not work properly without cookies enabled.

3.2.2 Web Beacons

Web beacons are tiny pixel images that allow us to collect information about site traffic and effectiveness. We may use web beacons to deliver cookies, count visits, understand usage, and customize advertising.

3.2.3 Log Files

Log file information is automatically reported by your browser or mobile device each time you access our services. When you use our services, our servers automatically record information including your device IP address, access times, pages viewed, and

referring website addresses. We may use log file information to ensure quality of service and customize site content.

3.3 Third-Party Sources

We may receive personal and non-personal information about you from third-party sources, including marketing partners, social media platforms, and data brokers. This information may be combined with other information we collect about you.

3.4 Offline Methods

We may also collect information through offline means such as paper forms, in-person interactions, point of sale systems, and audio and video security camera footage. This information collected online may be entered into our systems and combined with other information we collect about you. Any data collected in this manner will be treated with the same level of care as data collected online.

4 Information Collected and How We Use It

Note: This section also serves as our Notice of Collection for purposes of the California Consumer Privacy Act.

This section provides an overview of the types of personal information we may collect about you and the general purposes for which they are used. Please note that the actual information collected and its use may vary depending on your interactions with us and the Services you use.

4.1 Categories of Data

To align with applicable data protection laws, we have organized personal information into specific categories, which are listed below. These categories serve as a framework for understanding the various types of data that could be involved in our services. However, it's important to note that we may not collect or use information from every category listed here. The specifics of what we do collect and how we use it are detailed in the Data Use and Sharing Table.

- **Identifiers**: Such as name, postal address, email address, account name, or Social Security number.
- **Personal Information Categories Listed in the California Customer Records Statute**: Such as name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
  Note: This category overlaps with other categories listed.

- **Protected Classification Characteristics Under State or Federal Law**: Such as age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex, sexual orientation, veteran or military status, genetic information.
- **Commercial Information**: Such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- **Biometric Information**: Such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.
- **Internet or Other Similar Network Activity**: Such as browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.
- **Geolocation Data**: Such as physical location or movements.
- **Sensory Data**: Such as audio, electronic, visual, thermal, olfactory, or similar information.
- **Professional or Employment-Related Information**: Such as current or past job history or performance evaluations.
- **Non-Public Education Information**: Such as education records directly related to a student maintained by an educational institution or party acting on its behalf.
- **Inferences Drawn from Other Personal Information**: Such as profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

4.1.1 Categories of Sensitive Data

Certain data protection laws apply heightened standards to specific categories of data deemed to be sensitive or special. The definition of sensitive personal information may vary depending on applicable laws, but generally the following types of information are included: Social Security numbers, driver's license numbers, state identification card numbers, financial account information, medical information, health insurance information, biometric data, precise geolocation, racial or ethnic origin, religious or philosophical beliefs, and union membership. Our practices regarding sensitive personal information are described below.

4.2 Data Uses and Purposes

In accordance with data protection laws, each category of personal information we collect serves one or more specific business or commercial purposes. Below, we outline these purposes, which essentially dictate how we use the data we collect. Additional details regarding the purposes for each data type are contained in the Data Use and Sharing Table.

4.2.1 Common Uses

We commonly use or disclose the personal information we collect for the following purposes:

- **Service Fulfillment**: To perform a variety of services essential to your customer experience or our business. This includes, but is not limited to:
    - Account setup, maintenance, and support
    - Order processing and fulfillment
    - Billing and payment processing
    - Shipping and delivery
    - Customer service across multiple channels
    - Any other services described at the time of data collection
- **Business Operations**: To perform business operations essential to delivering our services, including:
    - Providing analytics and data insights
    - Document management and record keeping
    - Training and development services
    - Generating business intelligence reports
    - Strategic decision making
- **Auditing and Compliance**: To conduct audits related to advertising, such as counting unique visitors and verifying ad quality, and compliance with the CCPA as well as other applicable data protection laws and legal standards.
- **Security and Integrity**: To maintain the security and integrity of our services, including protection against fraudulent or illegal activities. This includes validating your identity as necessary.
- **Debugging and Error Repair**: To identify and fix errors affecting service functionality.
- **Short-term Use**: For transient, non-personalized advertising during your current interaction with us, without third-party disclosure or profile building.
- **Advertising and Marketing**: To provide advertising and marketing services, excluding behavior-based advertising. Note: We do not combine opted-out consumer information with other sources for these purposes.
- **Research and Development**: For internal technological research and development.
- **Quality Assurance and Improvement**: To maintain and improve the quality and safety of our services.
- **Customization**: To enhance your experience with our services, we may use your data to personalize features, content, and recommendations, in line with applicable laws and your preferences.

- **Professional Services**: Providing or receiving a range of specialized services, including but not limited to legal, accounting, consulting, and security assessments, as well as other similar services.
- **Additional Uses Described**: In any other way we may describe when you provide the information or any other purposes for which you provide your consent.

4.2.2 Less Common Uses

While less frequent, there are other scenarios where we may use or disclose your personal information:

- **Audits Involving External Entities**: Sharing data with external organizations, including those we collaborate with or those that evaluate our business operations, to ensure compliance with industry standards, certifications, or legal obligations.
- **Legal Obligations**: Fulfilling legal obligations such as responding to subpoenas, court orders, or other binding government requests. In the rare event of litigation, we may use your data to establish, exercise, or defend legal claims.
- **Reorganization**: In the event of a business transaction such as a sale, merger, consolidation, acquisition, change in control, transfer of substantial assets, bankruptcy, or reorganization, your personal information may be shared or transferred. This also includes any subsequent integration activities post-transaction.
- **Business Transfers**: In the event of a divestiture, investment, or other asset transfer that is not part of a broader business transaction like a merger or acquisition, your personal information may be shared or transferred.

4.2.3 Profiling

Profiling involves the automated processing of your personal information to evaluate certain aspects of your behavior and preferences. We do not engage in profiling.

4.2.4 Data Aggregation

We may aggregate your personal information with that of other users for analytical and reporting purposes. This aggregated data is anonymized and does not identify you personally. Aggregated data may be used for various purposes, including statistical analysis, without further notice to you and without obtaining additional consent.

4.3 Data Disclosures and Sales

Your privacy is important to us, and we want you to understand how we may disclose your personal information to other entities.

Disclosures for Business Purposes

We may provide your personal information to companies that provide services on our behalf, such as payment processing, order fulfillment, customer service, website hosting, and other IT operations. These companies, known as "service providers," are contractually obligated to use your data only for the service they're providing and cannot use it for anything else. Details on these types of disclosures can be found in the Data Use and Sharing Table.

Sales and Sharing

In the context of data protection laws, a "sale" refers to the act of providing your personal information to third parties in exchange for monetary or other valuable consideration. These third parties are then authorized to use the data for their own purposes. "Sharing" is a more specific term that involves disclosing your personal information to third parties for the purpose of cross-context behavioral advertising, irrespective of whether we receive compensation.

We do not sell or share your personal information for targeted advertising or financial gain. Your data may be disclosed to select service providers for operational purposes, but these providers are contractually bound to use your information solely for the services they deliver.

4.4 Data Use and Sharing Table

The following Data Use and Sharing Table provides an overview of how we have collected, used, shared, and disclosed your personal information over the past 12 months. It also serves as an indicative guide to our typical practices for collecting, using, and sharing personal information.

This table is designed to offer transparency in compliance with all applicable data protection laws. Please review it carefully to understand how your data is handled.

Data Category	Processing Purpose(s)	Categories with whom disclosed for a business purpose	Categories with whom sold or shared
Identifiers	Service Fulfillment, Business Operations, Auditing and Compliance, Security and Integrity, Debugging and Error Repair, Quality Assurance and Improvement	Service Providers, Affiliates, Internet Service Providers, Operating Systems and Platforms, Social Networks, Data Analytics Providers, Internet Cookie Recipients (like Google Analytics)	Not sold or shared
Categories from California Consumer	Service Fulfillment, Business Operations, Auditing and	Service Providers, Affiliates, Internet Service Providers,	Not sold or shared

Records Statute (Overlaps with other Categories)	Compliance, Security and Integrity, Debugging and Error Repair, Quality Assurance and Improvement	Operating Systems and Platforms, Social Networks, Data Analytics Providers, Internet Cookie Recipients (like Google Analytics)	
Protected Classification Characteristics	We do not collect or process this category of data.		
Commercial Information	Service Fulfillment, Business Operations, Auditing and Compliance, Security and Integrity, Debugging and Error Repair, Quality Assurance and Improvement	Service Providers, Affiliates, Internet Service Providers, Operating Systems and Platforms, Social Networks, Data Analytics Providers, Internet Cookie Recipients (like Google Analytics)	Not sold or shared
Biometric Information	We do not collect or process this category of data.		
Internet and Other Network Activity	Business Operations, Auditing and Compliance, Security and Integrity, Debugging and Error Repair, Quality Assurance and Improvement	Service Providers, Internet Service Providers, Operating Systems and Platforms, Data Analytics Providers, Internet Cookie Recipients (like Google Analytics)	Auditing and Compliance, Security and Integrity, Debugging and Error Repair, Quality Assurance and Improvement
Geolocation Data	Business Operations, Auditing and Compliance, Security and Integrity	Service Providers, Affiliates, Internet Service Providers, Operating Systems and Platforms, Data Analytics Providers, Internet Cookie Recipients (like Google Analytics)	Not sold or shared
Sensory Data	Service Fulfillment, Business Operations, Security and Integrity	Service Providers	Not sold or shared
Professional or Employment-Related Data	We do not collect or process this category of data for general users. Workforce members and job applicants should review the separate Notices at Collection applicable to them.		
Non-Public Education Information	We do not collect or process this category of data.		
Inferences Drawn from Other Personal Information	We do not collect or process this category of data.		

4.5 Sensitive Personal Information Practices

We do not collect any data considered to be sensitive personal information under applicable data protection laws. You can rest assured that we prioritize your privacy and take extra precautions to not collect or process such sensitive categories of information.

4.6 Data Retention

We retain your personal information only as long as needed to fulfill the purposes we collected it for, including satisfying legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider:

i. the amount, nature, and sensitivity of the personal information;
ii. the potential risk of harm from unauthorized use or disclosure of your personal information;
iii. the purposes for which we process your personal information and whether we can achieve those purposes through other means; and
iv. the applicable legal requirements.

Additionally, we may anonymize your personal information (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

If you have any questions about the specific retention periods for different types of your personal information, please feel free to contact us using the Contact Information provided below.

5 Third-Party Links and Services

This Privacy Policy applies only to our Services. Our Services may contain links to other websites, applications, or services that are not operated or controlled by us. This section outlines our policies regarding third-party interactions.

5.1 General Policy

We are not responsible for the content, privacy policies, or practices of any third-party websites, applications, or services. When you click on a third-party link, you will be directed to that third party's site or service. We strongly advise you to review the Privacy Policy of every site or service you visit.

5.2 Third-Party Data Collection

We permit third parties to use tracking technologies on our websites and mobile apps. These technologies are used for analytics, management, and other types of work services. These third parties may collect information about your online activities over time and across different websites when you use our Services. The information

collected may then be used to provide advertising about products and services tailored to your interests, which may appear either on our websites or on other websites.

5.3 Specific Third-Party Services

We may use third-party services for various purposes, including but not limited to analytics, advertising, and customer support. Below are some specific third parties that we may use.

5.3.1 Google Analytics

We use Google Analytics to collect information about how visitors use our Services. This includes details about where you come from, how often you visit, what pages you view, and what actions you take within our Services. Google Analytics collects only the IP address assigned to you on the date you visit, rather than your name or other identifying information. Google Analytics uses cookies to collect this data. We do not combine the information collected through the use of Google Analytics with personally identifiable information.

Google's ability to use and share information collected by Google Analytics about your visits to our Services is restricted by the Google Analytics Terms of Service and the Google Privacy Policy. You can prevent Google Analytics from recognizing you on return visits by disabling cookies on your browser or by following these instructions from Google.

5.3.2 Facebook Pixel

We use Facebook Pixel to understand and make our advertising efforts more efficient. Facebook Pixel collects data that helps us track conversions from Facebook ads, optimize ads, build targeted audiences for future ads, and remarket to people who have already taken some kind of action on our website. The data collected includes information about how you interact with our Services, such as the pages you visit and the actions you take.

Facebook Pixel collects only the data necessary to achieve the aforementioned purposes. Facebook's ability to use and share information collected by Facebook Pixel is governed by the Facebook Business Tools Terms. For more information on how Facebook collects and uses data, you can visit their Privacy Policy. If you wish to opt out of the collection and use of information for ad targeting, you can access the following links: About Ads and Your Online Choices.

5.3.3 Other Third-Party Services

- Google Tags: For website analytics and tracking.
- Google Maps: For location-based services and mapping.
- YouTube: For video content delivery.

Please note that these third parties may have their own privacy policies, and we recommend reviewing those policies before interacting with these services.

6 Your Privacy Choices

You can control the collection and use of personal information for some of our processing activities. These choices are generally available to all users. Residents of certain jurisdictions may have additional rights and choices concerning their personal information depending on local laws.

6.1 Adjusting Communication Preferences

We respect your preferences concerning how we communicate with you. Below are the avenues through which you can manage the types of communications you receive from us:

Email: To opt out of promotional emails, you may follow the 'unsubscribe' instructions located at the bottom of each email. Alternatively, you may contact us directly using the information provided in the Contact Information section. Please be advised that opting out of promotional communications will not preclude you from receiving transactional emails, such as those related to purchases or account activity.

Mail Promotions: Should you wish to be removed from our mailing list for physical promotions and solicitations, please send a written request to our customer service department using the address provided in the Contact Information section of this Privacy Policy. Ensure your full name and mailing address are included in your correspondence.

6.2 Blocking Cookies

Cookies are small data files stored on your device to enhance your browsing experience and enable certain website functionalities. You have the ability to manage how your web browser interacts with cookies. While most browsers are configured to accept cookies by default, you can modify this behavior through your browser's "Privacy" or "Security" settings. For guidance on how to manage cookies on popular web browsers, you may click on the following links:

- Safari (Desktop) and Safari Mobile (iOS).
- Firefox
- Chrome
- Microsoft Edge
- Brave

6.3 "Do Not Track" (DNT) Signals

We value your privacy and strive to provide you with the best user experience possible. While some web browsers offer a 'Do Not Track' option, which sends signals to websites visited by the user about tracking preference, it's important to note that there is no consensus among industry participants as to what 'Do Not Track' means in this context. As such, like many websites, we do not currently respond to 'Do Not Track' browser settings or signals.

7 Security

We implement recognized physical, technical, and organizational safeguards tailored to protect the confidentiality, integrity, and availability of the specific categories of personal information we collect and process. These safeguards are designed to prevent unauthorized or unlawful access, destruction, loss, alteration, or disclosure of your personal data. However, despite our best efforts, no controls can provide absolute protection against all security threats, and we cannot guarantee that unauthorized access or loss will never occur.

Key examples of the technical and organizational safeguards we employ are provided below.

7.1 Technical Safeguards

Examples of our technical safeguards include the following:

- Safeguarding sensitive data in transit and at rest;
- Implementing access controls, authentication protocols, and authorization procedures;
- Conducting vulnerability scanning, penetration testing, and security audits;
- Employing security monitoring capabilities and incident response plans;
- Maintaining business continuity provisions and disaster recovery processes;
- Following secure software development lifecycle processes;
- Patching, updating, and securing software configurations on a regular basis;
- Establishing network security and segmentation measures;
- Handling, storing, and destroying records and data in a secure manner; and
- Using endpoint device protections and remote device management.

7.2 Organizational Controls

Examples of our organizational controls include the following:

- Documenting information security policies, standards, procedures;
- Employing information security personnel and governance;
- Conducting risk assessments, impact analyses, and threat modeling;
- Providing training and education to personnel on security practices;

- Performing background checks for employees and third parties;
- Limiting access on a need-to-know basis;
- Reviewing and auditing controls, processes, and responses; and
- Maintaining security incident response plans.

8 Data Transfers

Our primary operations are based in the United States, and as such, the majority of data processing occurs within the United States. However, the nature of our Services may necessitate the transfer of your personal information across different locations, including countries other than the one where the information was originally collected. We implement appropriate measures to ensure that your personal information remains protected and secure during these transfers.

8.1 Within the United States

For residents of the United States, your personal information may be transferred and processed in different states for the various purposes outlined in this Policy.

8.2 International Transfers

For international users, be aware that your personal information may be transferred to and processed in the United States or other countries that may not have the same data protection laws as your home country.

9 Children's Privacy

Our Services are not designed for, nor intended to attract, individuals under the age of 16. Nevertheless, we are committed to ensuring the privacy and safety of minors who may inadvertently access our Services.

9.1 Minimum Age Requirement

We do not knowingly collect, use, sell, share, or disclose personal information from individuals who are under the age of 16. If you are below this age threshold, we kindly ask that you refrain from using our Services and submitting any personal information to us.

9.2 Parental Intervention

Should we discover that we have inadvertently collected personal information from someone under the age of 16, we will take immediate steps to delete that information. Parents or guardians who suspect that their minor has provided personal information to us are encouraged to contact us promptly.

10 Updates to This Privacy Policy

We reserve the right to modify this Privacy Policy at any time to reflect changes in our practices, services, or legal obligations. Any modifications will be effective upon the date specified in the updated Privacy Policy. Your continued use of our Services following the posting of changes constitutes your acceptance of such changes.

10.1 Revisions

We will indicate the date of the last revision at the top of this Privacy Policy. We encourage you to periodically review this Policy to stay informed about how we are protecting your personal information.

10.2 Notification Methods

If we make material changes to this Privacy Policy that significantly affect your rights or the way we use your personal information, we will notify you through the most appropriate channels. Generally, this will be done by updating the date at the top of this page. However, other notification methods may include sending an email to the address you have provided, posting a notice on our Services, or other methods as required by law.

11 Contact Information

If you have any questions or concerns about this Privacy Policy or our data practices, you can reach out to us through the following means:

Contact: Prime Electric, Inc.
Address: 3460 161st Avenue SE
Bellevue, WA 98008
Email: PGI-PrivacyPolicy@primee.com
Phone: 425-747-5200

12 Additional Rights and Choices (Where Applicable)

These rights apply only to residents of the following jurisdictions:

- **Select U.S. States:** *California, Colorado, Connecticut, Utah, and Virginia.*

Residents of certain jurisdictions are afforded additional rights under applicable data protection laws. These rights offer additional control over personal information and are subject to limitations and exceptions.

12.1 User Data Rights

The following rights are apply if you live in one of the jurisdictions mentioned above. Depending on where you live, the details of a given right may vary. For details tailored to your location, see the supplemental notices for each jurisdiction.

12.1.1 Right to Access
You have the right to request access to the personal information we hold about you. This includes the right to be informed about the categories and specific pieces of personal information we have collected, the sources from which we collected it, the purposes for collecting it, and the categories of third parties with whom we have shared it. This is also commonly referred to as the "Right to Know."

12.1.2 Right to Correct
You have the right to request that we correct any inaccurate or incomplete personal information about you. We will make reasonable efforts to ensure that the information is accurate and up to date. This is also known as the "Right to Rectification."

12.1.3 Right to Delete
You have the right to request the deletion of your personal information, subject to certain exceptions. This is often referred to as the "Right to Erasure" or "Right to Be Forgotten."

12.1.4 Right to Portability
You have the right to request that we provide you with a copy of your personal information in a structured, commonly used, and machine-readable format. You also have the right to request that we transfer this information to another data controller, where technically feasible.

12.1.5 Right to Opt Out of Sale/Sharing of Personal Information
You have the right to direct us not to sell or share your personal information with third parties. The specifics of this right may differ depending on your jurisdiction. For a complete understanding, please refer to the supplemental notices tailored to your location.

12.1.6 Right to Opt Out of Certain Data Processing
You may have the right to object to specific types of data processing activities we conduct. The types of processing you can object to and how to do so will vary by jurisdiction. For more information, consult the supplemental notices for your specific location.

12.1.7 Right to Non-Discrimination
You have the right not to be discriminated against for exercising any of your data protection rights. This means that we will not deny you goods or services, charge you different prices or rates, or provide you with a different level or quality of goods or services based solely on your exercise of these rights.

12.2 Exercising Your Data Rights

To exercise any of the rights outlined above, you have multiple options. These methods are designed to provide you with convenient and secure ways to take control of your personal information.

12.2.1 Email Requests

You can submit your requests via email. To do so, please send a detailed email specifying the right you wish to exercise to PGI-PrivacyPolicy@primee.com . The email should include sufficient information to allow us to verify your identity and where you reside.

12.2.2 Global Privacy Control (GPC) Signals

Global Privacy Control (GPC) is a standard that allows you to express your privacy preferences to websites you visit. Because we do not sell or share your personal information, the activation of a GPC signal on your web browser or mobile application will not have any impact on how we handle your data. For more information on GPC signals, you can visit https://globalprivacycontrol.org/.

12.3 Using an Authorized Agent

You have the option to designate an authorized agent to submit requests on your behalf for exercising your data rights. An authorized agent can be either a person or a business entity that you have formally authorized to act on your behalf.

To use an authorized agent:

1. **Signed Authorization**: You must provide the authorized agent with a signed written authorization to act on your behalf. This document should clearly indicate that you grant them the authority to submit requests for you.
2. **Agent Submission**: The authorized agent can then submit a request via the methods outlined above. The agent should attach a copy of the written authorization you provided.
3. **Identity Verification**: We may contact you directly to confirm that you have authorized the agent to act on your behalf. This is a security measure designed to protect your personal information.

Please note that we reserve the right to deny requests from agents who do not provide proof of authorization or if we cannot verify the agent's identity.

12.4 Verification Procedures

To ensure the security and confidentiality of your personal information, we have established verification measures that must be completed prior to fulfilling any request to exercise your data rights. These measures may involve confirming your

identity through a series of questions or requiring documentation that substantiates your identity or authority to make the request. Should we be unable to verify your identity or authority adequately, we reserve the right to decline the request and will provide an explanation for our decision.

12.5 Response and Timing

Upon receiving a verified request to exercise your data rights, we will acknowledge receipt of the request within 10 business days. We aim to respond substantively to your request within 45 calendar days from the date of receipt. If we require more time to process your request, we will inform you of the reason and extend the period by an additional 45 calendar days.

Please note that not all requests will be granted. Certain legal exceptions may apply, such as if we are unable to verify your identity, or if there are legal or contractual reasons that prevent us from fulfilling a deletion request. Regardless of the outcome, you will receive a written response that either details the actions we took or explains why no action was possible.

12.6 Appealing a Response

If you are dissatisfied with our initial response, you may seek further review. To initiate an appeal, please email us at [PRIVACY/APPEAL EMAIL] within 30 days of receiving our initial response. Your email should include a copy of your original request, our response, and a detailed explanation of why you are seeking reconsideration. You may also attach any additional supporting information and documents that you believe are relevant. We will review your appeal and provide a final determination within 60 days.

13 U.S. State-Specific Provisions

Several U.S. states have enacted unique privacy laws and regulations. This section provides details on those state-specific requirements, supplementing the general privacy practices previously outlined.

13.1 California

This section is tailored to meet the specific requirements imposed by California law. While this section outlines state-specific rights for California residents, the preceding sections of this Privacy Policy also apply to them.

13.1.1 The California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) was enacted in 2018 to enhance privacy rights and consumer protection for residents of California. It was subsequently amended in 2020 by the California Privacy Rights Act (CPRA), which enhanced consumer rights, introduced new obligations for businesses, and established the

California Privacy Protection Agency (CPPA) for enforcement. Throughout this Privacy Policy, the acronym "CCPA" refers to the law as it has been updated by the CPRA.

The CCPA provides California residents with specific rights and protections concerning their personal information, including the right to access, correct, and delete their data, among others. It also imposes certain disclosure and compliance obligations on businesses. This privacy policy, including the Additional Rights and Choices section and this California-specific section, is designed to be in full compliance with the newly-amended CCPA.

13.1.2 Data Collection and Use

For a comprehensive understanding of the types of personal information we collect, the sources from which we collect it, and the purposes for which we use it, please refer to the following sections of this Privacy Policy:

- Section 3: Describes the sources from which we collect personal information.
- Section 4: Outlines the categories of personal information collected and the business purposes for which this information is used.

Both sections are designed to provide you with a complete picture of our data collection and use practices in compliance with the CCPA. We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated, or incompatible purposes without providing you notice.

13.1.3 Notice of Right to Opt Out of Sale/Sharing

We neither sell nor share your personal information; therefore, there is no need to opt out.

13.1.4 Notice of Right to Limit Processing of Sensitive Personal Information

We do not collect sensitive Personal Information as defined by the CCPA. Therefore, the right to limit the use of sensitive personal information is not applicable.

13.1.5 Shine the Light

California Civil Code Section § 1798.83, also known as the "Shine the Light" law, permits California residents to request and obtain from us once a year, free of charge, a list of the third parties to whom we have disclosed their personal information (if any) for direct marketing purposes in the preceding calendar year, as well as the type of personal information disclosed. To make such a request, please send an email with the subject "Shine the Light Request" to the email address in our Contact Information.

13.2 Colorado, Connecticut, Utah, and Virginia

This section is specifically designed to address the particular legal requirements imposed by Colorado, Connecticut, Utah, and Virginia While this section outlines

state-specific rights for residents of these states, the preceding sections of this Privacy Policy also apply to them.

13.2.1 Applicable State Laws
This section is intended to comply with the requirements of the following state laws:

- Colorado Privacy Act (CPA)
- Connecticut Data Privacy Act (CTDPA)
- Utah Consumer Privacy Act (UCPA)
- Virginia Consumer Data Protection Act (VCDPA)

All these laws (collectively, "Applicable State Laws") aim to enhance consumer privacy rights and impose certain obligations on businesses that process personal data.

13.2.2 Opt-In Requirements for Sensitive Information
The Applicable State Laws require explicit consent for the processing of sensitive data. If you are a resident of Colorado, Connecticut, Utah, or Virginia, we will obtain your explicit consent prior to processing your sensitive data. However, we do not collect or process sensitive data.

13.2.3 Additional Rights and Choices
For additional rights and choices provided by the Applicable State Laws, including the right to appeal decisions related to your personal data, please refer back to Section 12 of this Privacy Policy.