Employee and Job Applicant Data Protection Notice and Consent Form for the US & Canada

Please read this document carefully.

PURPOSE

The purpose of this Notice is to inform you about the Personal Data that Cook will collect and process about you in connection with your employment, job application, or services for Cook. It is also intended to inform you about your responsibilities with respect to Personal Data and other confidential, non-public information that you are likely to come in contact with by virtue of your employment with (or temporary employment services for) or job application process at Cook.

DEFINITIONS

- **Personal Data** – Personal Data refers to any data that can directly or indirectly lead to the identification of a specific individual.

- **Confidential Information** – Confidential Information refers to any non-public information that you may have access to by virtue of your services to Cook. This includes but is not limited to Personal Data about other employees and our customers, as well as information about our business, products, practices, and systems.

- **Intellectual Property** – Intellectual Property refers to Cook's patents, trademarks, copyrighted material, logos, branding, and any other proprietary information associated with our identity or marketing.

SCOPE

This Notice covers all Personal Data, Confidential Information, and Intellectual Property in any format, including, for example, that which is collected and processed electronically, in paper form, or communicated in conversations. The Notice also addresses all types of unauthorized access and disclosures of that information, including but not limited to those that may violate applicable privacy/data protection, security, trade secret or intellectual property laws or regulations. Please note that while this Notice applies to our employees and job applicants who are residents of California, we also provide further disclosures for our California employees and job applicants as required under the California Consumer Privacy Act ("CCPA"). For more information, see our Privacy Statement for California Applicants & Employees.

DATA PROTECTION – YOUR PERSONAL DATA

This section of the Notice and Consent Form is intended to inform you about the Personal Data that we collect, process, share and store about you in connection with your employment, job application, or services for Cook.

Collection and Processing. Cook limits the collection and processing of Personal Data about you to that which is necessary or legitimate in relation to administering your employment/temporary services or job application to us, including that which you voluntarily agree to provide in relation to any optional programs

offered to use (such as voluntary employee wellness or community service programs). The data that we collect in relation to your employment or job application includes your name and contact details, your work history and qualifications, your department and supervisor at Cook, your performance information at Cook, your compensation details, and other information that is required for human resource oversight and administration as well as tax and regulatory reporting purposes. We also may collect some employee health information, including Covid-19 status, for contact tracing purposes. Certain employees may also be asked to provide their vaccination status if their role at Cook requires a vaccine. For California employees and job applicants, we provide further information about our collection and processing practices in our Privacy Statement for California Applicants & Employees.

Source of the Personal Data. In general, most of the Personal Data collected and processed about you will come from you. However, a portion of the data will come from others, such as performance feedback collected from your managers, or reference checks and confirmations of your job qualifications, which may come from prior employers.

Accurate, Relevant and Up-to-Date. Cook takes steps to ensure that the information we collect about you is accurate, relevant and up-to-date. We also rely on our employees and temporary personnel to update their information on file with us, such as your home address and, as applicable, dependent information (for employee benefits purposes). If your information changes during your employment, please update it by informing your local HR team of all applicable changes or updates to your information.

Disclosing Your Data. Cook may disclose limited amounts of your Personal Data with third-parties who assist us with legitimate business activities. Before disclosing any Personal Data with business partners, we require those third-parties to agree in writing to adhere to privacy and security safeguards that are as protective of your Personal Data as those that we have put in place. In addition, we may be required by law to share a small amount of your Personal Data with government agencies, such as for tax reporting purposes or contact tracing purposes. Depending upon your country's privacy laws, those agencies are also generally required to protect your data from unauthorized access and ensure that it is appropriately safeguarded.

We do not sell or share your Personal Data with any third parties for their own separate use, or use it in ways that are unrelated to your employment or job applicant status with us. (As noted above, you may be eligible to participate in certain voluntary programs offered by Cook in some countries, such as our employee wellness program. If you decide to participate, relevant Personal Data will be collected and processed for those programs. The same standards apply to any third-parties that assist Cook with those programs.)

Security and Storage of Your Personal Data. We take steps to ensure that your Personal Data is appropriately protected from loss, misuse, alteration, destruction, and unauthorized access. Our safeguards are updated to address new threats and risks as they become known, and as the requirements change. Your Personal Data may be transmitted and stored in computerized as well as manual formats. We also restrict access to your Personal Data such that it is not provided to others who do not have a legitimate purpose to access it in connection with their responsibilities for Cook.

Transfer of Your Personal Data to Other Countries. Cook is a global company. As such, your Personal Data may be transferred out of your country and may be processed or stored in other countries. The privacy and security laws that may apply to your Personal Data in those countries may be different than those required in your home country and may not require the same level of protection. However, Cook has taken steps to ensure that your Personal Data is reasonably and appropriately protected and safeguarded, regardless of the country where it is located.

Individual Rights. Depending on where you are located, you have different individual rights protected by law. In certain countries, including Canada and some states within the US, you may have the right to request erasure/deletion of your data, the right to be forgotten, the right to access and port your data, the right to object to the processing of your data for a direct marketing or certain other purposes (including to limit the

use and sharing of your Sensitive Personal Data), and the right not to be discriminated against for exercising your rights. For details regarding individual rights available to California employees, please see our Privacy Statement for California Applicants & Employees. If you wish to exercise any of your rights, you may reach us by contacting privacy@cookgroup.com, or contacting your Human Resources office.

Retention of Your Data. Cook retains your data consistent with applicable legal and business requirements, and in accordance with the Cook records retention schedule. When the retention time is reached, and absent a litigation hold or other legitimate reason for continued retention, your data is securely destroyed.

Questions, Concerns, or Grievances. If you have any questions about our data protection practices or wish to contact us for any other reason, you may reach us by contacting your Human Resources office or emailing privacy@cookgroup.com. Should you believe that your data has been mismanaged by Cook, you also have the right to file a complaint with us or with the relevant data protection supervisory authority in your local country. Cook takes all complaints seriously and has an internal process for addressing them.

Data Protection Consent and Signature. By signing this form, you confirm that you have read and understand how your Personal Data will be collected and processed by Cook. You give your permission to collect and use the Personal Data that you submit for the above purposes. You also confirm that the information that you provide to us is accurate and complete to the best of your knowledge. Yes, I agree to the collection and processing of my Personal Data by Cook as described in this Notice and Consent Form.

Print Name:	
Signature:	
Date:	

CONFIDENTIALITY AND INTELLECTUAL PROPERTY

You agree, both during and for an unlimited time after your involvement with Cook, that you will not disclose or make available to any third party (except as specifically authorized or required by Cook or ordered by a court of law or regulatory authority) any confidential information or intellectual property used or possessed by Cook, clients of Cook, or our business partners and that you will adhere to the terms of your Employee Confidentiality Agreement.

Per your Employee Confidentiality Agreement, unauthorized access to, and/or any disclosure of, confidential information is prohibited. Failure to comply with this requirement may result in your association with Cook being terminated. You may also be subject to additional legal action by Cook or the relevant enforcement authorities. Any violation of an individual's privacy protections as a result of your actions, such as unauthorized viewing or disclosure of their Personal Data, may result in personal liability to you for damages as well as legal prosecution in your country and elsewhere.

These restrictions will not apply to information you are required to disclose by law or which has become available to the public generally, otherwise than through unauthorised disclosure as a result of your actions or omissions.

SYSTEM ACCESS RESPONSIBILITIES

Cook may provide you with access to our computer systems (including administrative access to servers, databases, and computers, as well as our internet and e-mail systems). In this case, you agree to the following terms and conditions of use:

- Use those systems only in a professional manner that is respectful of Cook, our employees, clients, business partners and other individuals whose personal data and other information may be accessible to you;

- Use those systems only for the purposes of performing the services for which you have been hired or retained by Cook;

- Use those systems in compliance with Cook's applicable standards and guidelines for computer systems use and security;

- Understand and agree that you are strictly prohibited from using Cook's systems for any purpose other than for legitimate purposes in connection with your job responsibilities for Cook;

- Ensure that you abide by all Cook policies with respect to the proper use of our computer and electronic systems;

- Refrain from downloading any software or installing any hardware or other devices that may disrupt Cook's systems or compromise their security;

- Never handle Cook's data, including any confidential information or personal data in a manner that could reasonably expose the data to unauthorized access;

- Immediately report any real or suspected security incidents about which you become aware to your manager and local IT department on the same day as discovery;

- Maintain the integrity of all Cook information entrusted to you;

- Inform Cook at once if you believe you are in any way unfit to continue your obligations of confidentiality;

- Recognize that Cook may monitor your use of all Cook systems supplied by or on behalf of Cook to ensure compliance and security of the workplace, and to otherwise safeguard its equipment.

POLICIES AND PROCEDURES – COMPLIANCE COMMITMENT

You confirm that you will comply with Cook's Policies and Procedures which apply to your job responsibilities for Cook, as well as any training provided to you by or on behalf of Cook. This includes (but is not limited to) data privacy, data security, intellectual property, and Ethics & Compliance policies.

OWNERSHIP OF COOK'S INFORMATION

Per your Employee Confidentiality Agreement, you understand that all notes, emails, and other records (however stored or prepared) which relate to our business, the business of our clients, or that are stored on our servers or equipment, belong to Cook and are not considered personal. You confirm that upon completion of your responsibilities for Cook, you will promptly and securely return all information to us which you received in the course of performing your responsibilities for us, or, at the company's discretion. You will ensure that all company information has been securely purged and/or irreversibly erased (including proper purging from any electronic devices of your own, such as smart phones, which you may have been authorized to use during your employment with Cook.)

GOVERNING LAW

This Notice is governed and construed in accordance with the laws of the country in which the Cook office retaining you is located.

YOUR ACCEPTANCE

If there is anything in this Notice that you do not agree with or wish to discuss, please contact your manager. Otherwise, please sign and return this form to us indicating your acceptance of its terms.

I confirm my undertaking to be bound by the obligations in this Notice:

Signed:	
Name:	
Job title:	
Cook company:	
Country of residence:	
Date:	

Privacy Statement for California Applicants & Employees

Last Updated: August 2024

The California Consumer Privacy Act, as amended by the California Privacy Rights Act, and its implementing regulations (collectively, the "CCPA"), gives California residents certain rights and requires businesses to make certain disclosures regarding their Collection, use, and disclosure of Personal Information. This Privacy Statement for California Applicants & Employees (the "Policy") provides such notice to Cook's ("we," "us," "our") California job applicants ("Applicants") and California employees, independent contractors, and other individuals who interact with Cook in an employment-related capacity (collectively, "Employees").

Please note that this Policy only addresses Cook's Collection, use, and disclosure of employment-related Personal Information and only applies to residents of California. This Policy does not apply to individuals who are residents of other U.S. states or other countries and/or who do not interact with Cook in an employment-related capacity. For further details about our privacy practices pertaining to non-Applicant/Employee Personal Information, please see our Privacy Statement.

As an Employee, you have the right to know what categories of Personal Information Cook Collects, uses, discloses, Sells, and Shares about you. This Policy provides that information and other disclosures required by California law.

A. DEFINITIONS

- **Personal Information**: As used in this Policy, "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Consumer or household. Personal Information includes Sensitive Personal Information.

- **Sensitive Personal Information**: As used in this Policy, "Sensitive Personal Information" includes Personal Information that reveals, among other things, social security number, driver's license number, state identification card number, passport number, racial or ethnic origin, union membership, or the contents of a Consumer's mail, email, and text messages, unless Cook is the intended recipient of the communication. Sensitive Personal Information also includes information concerning the Applicant or Employee's health, sex life, or sexual orientation.

- **Other CCPA Definitions**: As used in this Policy, the terms "Collect," "Processing," "Service Provider," "Third Party," "Sale," "Share," "Consumer," and other terms defined in the CCPA and their conjugates, have the meanings afforded to them in the CCPA, whether or not such terms are capitalized herein, unless contrary to the meaning thereof.

B. APPLICANTS

- **Collection & Processing of Personal Information**

  We, and our Service Providers, may have Collected and Processed the following categories of Personal Information from Applicants in the preceding 12 months:

  (1) Identifiers, such as name, alias, online identifiers, account name, physical characteristics or description;
  (2) Contact and financial information, including phone number, address, email address, financial information;
  (3) Characteristics of protected classifications under state or federal law, such as age, gender, race, physical or mental health conditions, and marital status;
  (4) Internet or other electronic network activity information, such as browsing history and interactions with our websites or advertisements;
  (5) Audio, electronic, visual and similar information, such as call and video recordings;
  (6) Professional or employment-related information, such as work history and prior employer;
  (7) Education information, as defined in the federal Family Educational Rights and Privacy Act, such as student records and directory information;
  (8) Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics; and

(9) Sensitive Personal Information, including:
    a. Personal Information that reveals:
        i. Social security, driver's license, state identification card, or passport number;
        ii. Racial or ethnic origin

- **Categories of Applicant Personal Information We Disclose to Service Providers & Third Parties**

  We disclose the following categories of Applicant Personal Information to Service Providers and Third Parties:

  (1) Identifiers, such as name, alias, online identifiers, account name, physical characteristics or description;
  (2) Contact information, including phone number, address, or email address;
  (3) Characteristics of protected classifications under state or federal law, such as gender, race;
  (4) Professional or employment-related information, such as work history and prior employer;
  (5) Education information, as defined in the federal Family Educational Rights and Privacy Act, such as student records and directory information;
  (6) Sensitive Personal Information, including:
      a. Personal Information that reveals:
          i. Social security, driver's license, state identification card, or passport number;
          ii. Racial or ethnic origin

- **Purposes for Processing Applicant Personal Information**

  We, and our Service Providers, Collect and Process Applicant Personal Information (excluding Sensitive Personal Information) described in this Policy to:

  - Evaluate a potential Employee relationship with you;
  - Perform background checks and verify past employment, educational history, professional standing, and other qualifications;
  - Evaluate, determine, and arrange compensation, payroll, and benefits;
  - Assess your fitness and physical capacity for work; and
  - Contact you regarding your application and potential Employee relationship with us.

  In addition to the purposes identified above, Cook may use and disclose any and all Applicant Personal Information that we Collect as necessary or appropriate to:

  - Comply with laws and regulations, including, without limitation, applicable tax, health and safety, anti-discrimination, immigration, labor and employment, and social welfare laws;
  - Monitor, investigate, and enforce compliance with and potential breaches of Cook policies and procedures and legal and regulatory requirements;
  - Comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons; and
  - Exercise or defend the legal rights of Cook and its employees, affiliates, customers, contractors, and agents.

C. EMPLOYEES

- **Collection & Processing of Personal Information**

  We, and our Service Providers, may have Collected and Processed the following categories of Personal Information from Employees in the preceding 12 months:

  (1) Identifiers, such as name, alias, online identifiers, account name, physical characteristics or description;
  (2) Contact and financial information, including phone number, address, email address, financial information, medical information, health insurance information;
  (3) Characteristics of protected classifications under state or federal law, such as age, gender, race, physical or mental health conditions, and marital status;

(4) Internet or other electronic network activity information, such as browsing history and interactions with our websites or advertisements;
(5) Geolocation data, such as device location;
(6) Audio, electronic, visual and similar information, such as call and video recordings;
(7) Professional or employment-related information, such as work history and prior employer;
(8) Education information, as defined in the federal Family Educational Rights and Privacy Act, such as student records and directory information;
(9) Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics; and
(10) Sensitive Personal Information, including:
    a. Personal Information that reveals:
        i. Social security, driver's license, state identification card, or passport number;
        ii. Account log-in, financial account number, password, or credentials for allowing access to an account;
        iii. Precise geolocation;
        iv. Racial or ethnic origin, religious or philosophical beliefs
    b. Personal Information Collected and analyzed concerning a Consumer's health

- **Categories of Employee Personal Information We Disclose to Service Providers & Third Parties**

  We disclose the following categories of Employee Personal Information to Service Providers and Third Parties:

(1) Identifiers, such as name, alias, online identifiers, account name, physical characteristics or description;
(2) Contact and financial information, including phone number, address, email address, financial information, medical information, health insurance information;
(3) Characteristics of protected classifications under state or federal law, such as age, gender, race, physical or mental health conditions, and marital status;
(4) Internet or other electronic network activity information, such as browsing history and interactions with our websites or advertisements;
(5) Geolocation data, such as device location;
(6) Audio, electronic, visual and similar information, such as call and video recordings;
(7) Professional or employment-related information, such as work history and prior employer;
(8) Education information, as defined in the federal Family Educational Rights and Privacy Act, such as student records and directory information;
(9) Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics; and
(10) Sensitive Personal Information, including:
    a. Personal Information that reveals:
        i. Social security, driver's license, state identification card, or passport number;
        ii. Account log-in, financial account number, password, or credentials for allowing access to an account;
        iii. Precise geolocation;
        iv. Racial or ethnic origin, religious or philosophical beliefs
    b. Personal Information Collected and analyzed concerning a Consumer's health

- **Purposes for Processing Employee Personal Information**

  We, and our Service Providers, Collect and Process Employee Personal Information (excluding Sensitive Personal Information) described in this Policy to:

  - Manage your employee relationship with us;
  - Manage and provide compensation, payroll, tax, and benefits planning, enrollment, and administration;
  - Provide you access to Cook systems, networks, databases, equipment, and facilities;
  - Manage our workforce and its performance, including personnel planning, productivity monitoring, and evaluation;
  - Manage workforce development, education, training, and certification;

- Monitor, maintain, and secure Cook systems, networks, databases, equipment, and facilities;
- Authenticate your identity and verify your access permissions;
- Arrange, confirm, and monitor work-related travel, events, meetings, and other activities;
- Assess your working capacity or the diagnosis, treatment, or care of a condition impacting your fitness for work, and other preventative or occupational medicine purposes (including work-related injury and illness reporting);
- Contact and communicate with you regarding your employment, job performance, compensation, and benefits, or in the event of a natural disaster or other emergency;
- Contact and communicate with your designated emergency contact(s) in the event of an emergency, illness, or absence; and
- Contact and communicate with your dependents and designated beneficiaries in the event of an emergency or in connection with your benefits.

In addition to the purposes identified above, Cook may use and disclose any and all Employee Personal Information that we Collect as necessary or appropriate to:

- Comply with laws and regulations, including (without limitation) applicable tax, health and safety, anti-discrimination, immigration, labor and employment, and social welfare laws;
- Monitor, investigate, and enforce compliance with and potential breaches of Cook policies and procedures and legal and regulatory requirements;
- Comply with civil, criminal, judicial, or regulatory inquiries, investigations, subpoenas, or summons; and
- Exercise or defend the legal rights of Cook and its employees, affiliates, customers, contractors, and agents.

D. PROCESSING SENSITIVE PERSONAL INFORMATION

We, and our Service Providers, Collect and Process the Sensitive Personal Information described in this Policy only for:

- Performing the services or providing the goods reasonably expected by an average Consumer who requests those goods or services;
- Ensuring security and integrity to the extent the use of the Consumer's Personal Information is reasonably necessary and proportionate for these purposes;
- Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a Consumer's current interaction with us; provided that we will not disclose the Consumer's Personal Information to a Third Party and/or build a profile about the Consumer or otherwise alter the Consumer's experience outside the current interaction with the business;
- Performing services on our behalf, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on our behalf;
- Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by us, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by us.

E. SOURCES FROM WHICH WE COLLECT APPLICANT AND EMPLOYEE PERSONAL INFORMATION

We Collect Personal Information directly from Applicants and Employees, as well as from joint marketing partners; public databases; providers of demographic data; publications; professional organizations; educational institutions; social media platforms; Service Providers and Third Parties that help us screen and onboard individuals for hiring purposes, provide reference checks, or confirm prior employment; your managers (i.e., to provide performance feedback); and Service Providers and Third Parties when they disclose information to us.

F. CATEGORIES OF ENTITIES TO WHOM WE DISCLOSE APPLICANT AND EMPLOYEE PERSONAL INFORMATION

- **Affiliates & Service Providers.** We may disclose Applicant and Employee Personal Information to our affiliates and Service Providers for the purposes described in Sections B and C, respectively, of this Policy. Our Service Providers provide us with Applicant selection and related hiring services, benefits and wellness services, website services, as well as other products and services, such as web hosting, data analysis, customer service, infrastructure services, technology services, email delivery services, legal services, and other similar services. We grant our Service Providers access to Personal Information only to the extent needed for them to perform their functions, and require them to protect the confidentiality and security of such information.

- **Third Parties.** We may disclose your Personal Information to the following categories of Third Parties:

    - **At Your Direction.** We may disclose your Personal Information to any Third Party with your consent or at your direction.

    - **Business Transfers or Assignments.** We may disclose your Personal Information to other entities as reasonably necessary to facilitate a merger, sale, joint venture or collaboration, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings).

    - **Legal and Regulatory.** We may disclose your Personal Information to government authorities, including regulatory agencies and courts, as reasonably necessary for our business operational purposes, to assert and defend legal claims, and otherwise as permitted or required by law.

G. DATA SUBJECT RIGHTS

- **Data Subject Rights Available to You.** As an Applicant or Employee, you have the following rights regarding our Collection and use of your Personal Information, subject to certain exceptions:

    - **Right to Receive Information on Privacy Practices:** You have the right to receive the following information at or before the point of Collection:
        - The categories of Personal Information to be Collected;
        - The purposes for which the categories of Personal Information are Collected or used;
        - Whether or not that Personal Information is Sold or Shared;
        - If the business Collects Sensitive Personal Information, the categories of Sensitive Personal Information to be Collected, the purposes for which it is Collected or used, and whether that information is Sold or Shared; and
        - The length of time the business intends to retain each category of Personal Information, or if that is not possible, the criteria used to determine that period.

      We have provided such information in this Policy, and you may request further information about our privacy practices by contacting us at the contact information provided below.

    - **Right to Deletion:** You may request that we delete any Personal Information about you that we Collected from you.

    - **Right to Correction:** You may request that we correct any inaccurate Personal Information we maintain about you. Employees may also correct certain Personal Information by reaching out to your local Human Resources office.

    - **Right to Know:** You may request that we provide you with the following information about how we have handled your Personal Information in the 12 months preceding your request:

        - The categories of Personal Information we Collected about you;
        - The categories of sources from which we Collected such Personal Information;
        - The business or commercial purpose for Collecting, Selling, or Sharing Personal Information about you;
        - The categories of Third Parties with whom we disclosed such Personal Information; and
        - The specific pieces of Personal Information we have Collected about you.

- **Right to Receive Information About Onward Disclosures:** You may request that we disclose to you:

    - The categories of Personal Information that we have Collected about you;
    - The categories of Personal Information that we have Sold or Shared about you and the categories of Third Parties to whom the Personal Information was Sold or Shared; and
    - The categories of Personal Information we have disclosed about you for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

- **Right to Non-Discrimination:** You have the right not to be discriminated against for exercising your data subject rights. We will not discriminate against you for exercising your data subject rights. For example, we will not make hiring, firing, promotion, or disciplinary decisions based on or in consideration of your exercise of your data subject rights. We also will not deny goods or services to you, charge you different prices or rates, or provide a different level of quality for products or services as a result of you exercising your data subject rights.

- **Rights to Opt-Out of the Sale and Sharing of Your Personal Information and to Limit the Use of Your Sensitive Personal Information:** You have the right to opt-out of the Sale and Sharing of your Personal Information. You also have the right to limit the use of your Sensitive Personal Information to the purposes authorized by the CCPA. We do not Sell or Share Personal Information. Further, we do not use Sensitive Personal Information for purposes beyond those authorized by the CCPA. Relatedly, we do not have actual knowledge that we Sell or Share Personal Information of California Consumers under 16 years of age. For purposes of the CCPA, a "Sale" is the disclosure of Personal Information to a Third Party for monetary or other valuable consideration, and a "Share" is the disclosure of Personal Information to a Third Party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

- **How to Exercise Your Rights.** You may exercise your data subject rights by contacting our Global Chief Privacy Officer by phone or email listed below.

  Phone: 812.331.1025
  Email: Privacy@CookMedical.com

- **Verification Process**

  Depending on the type of data subject request you submit, we may need to verify your identity in order to process your request. If so, within 10 business days of Cook receiving your request, you will be contacted and guided through a process to verify your identity and your request. We will confirm receipt of your request, but before responding, we will verify your request by comparing the information you submit with the request to the information we have in our systems. In some cases, we may ask you for additional information to confirm that we have identified the correct customer record. If you designate an agent to make a request your behalf, we may require the agent to provide proof of signed permission from you to submit the request, or we may require you to verify your own identity to us or confirm with us that you provided the agent with permission to submit the request. Subject to certain exceptions that may apply under the law, if we are able to verify your request, we will accommodate it.

H. OTHER DISCLOSURES

- **Retention of Personal Information**: Cook retains your Personal Information consistent with applicable legal and business requirements, and in accordance with the Cook records retention schedule. We intend to retain your Personal Information only for as long as necessary to fulfill the purpose for which it was collected or a related and compatible purpose consistent with an average employee's expectation. We consider the following criteria when determining how long to retain your Personal Information: why we collected the Personal Information, the nature of the Personal Information, the sensitivity of the Personal Information, our legal obligations related to the Personal Information, and risks associated with retaining the Personal Information. When the retention time is

reached, and absent a litigation hold or other legitimate reason for continued retention, your Personal Information is securely destroyed.

- **California Residents Under Age 18.** If you are a resident of California under the age of 18 and a registered user of our website, you may ask us to remove content or data that you have posted to the website by writing to Privacy@CookMedical.com. Please note that your request does not ensure complete or comprehensive removal of the content or data, as, for example, some of your content or data may have been reposted by another user.

- **Financial Incentives for California Consumers.** Under California law, we do not provide financial incentives to California Consumers who allow us to Collect, retain, Sell, or Share their Personal Information. We will describe such programs to you if and when we offer them to you.

- **Changes to this Policy.** We reserve the right to amend this Policy at our discretion and at any time. When we make material changes to this Policy, we will notify you by posting an updated Policy on our website and listing the effective date of such updates.

- **Contact Us**: More information about our privacy practices can be found in our Privacy Statement. If you have any questions regarding this Policy or Cook's Collection and use of your Personal Information, please contact us at Privacy@CookMedical.com. If you are unable to review or access this notice due to a disability, you may contact us at Privacy@CookMedical.com to access this notice in an alternative format.