Dr. Rao Vepachedu, JD, PhD, LLM
Chief Privacy Officer

CARDINAL INTELLECTUAL PROPERTY PRIVACY POLICY (CPP)

CARDINAL INTELLECTUAL PROPERTY (CIP) is the leading US based Intellectual Property Services (IPSs) provider with worldwide clientele, including Fortune 500 companies, small businesses, law firms, and educational institutions in need of procuring Intellectual Property Rights (IPRs) in the US.

CIP Human Resources (CIPHR) is committed to safeguarding the privacy of personal information that is collected concerning our prospective, current, and former employees for management, human resources, and payroll purposes. All CIP employees are US residents.

In general, therefore, the CIPHR does not procure any information from employees of CIP clients for CIPHR purposes at all. However, as part of IPSs, data limited to information required for procuring, managing and maintaining IPRs for clients, and to distribute inventor awards, as applicable may be processed at the request of our clients (the Purpose). All the information provided by the client is volunteered to procure IPRs under the US law and will be subject to IP Laws, Rules and the Privacy Act of 1974 (P.L. 93-579).

Subject to exceptions, such as 37 CFR 1.56 (duty to disclose information material to patentability; MPEP, Chapter 2000 Duty of Disclosure), US federal law generally prohibits service providers from disclosing information about their subscribers to government officials. In the absence of a court order, warrant, or subpoena, service providers must generally keep customer records or subscriber information confidential from the government and are also generally required to keep the contents of communications stored or maintained by the service confidential.

Accordingly, CIP protects and uses your personal information only to fulfill your requests and serve you better in the IPSs that CIP provides for you. CIP does not share your personal details with outside third parties without your consent. CIP will only send you materials you have indicated you want to receive according to your preferences, and CIP will honor your opt-out requests. CIP uses cookies and web beacons to help us understand the features that apply to visitors, provide better functionality, and offer you personalized content. CIP adopts careful procedures to protect your personal information.

The above principles are the core principles called the Fair Information Practice Principles (FIPPs). *The FIPPs are:*

- *Transparency: CIP is transparent and provides notice to the individual regarding its collection, use, dissemination, and maintenance of the Personal Data (PD).*
- *Individual Participation: CIP involves the individual in the process of using the PD and, seeks individual consent for the collection, use, dissemination, and maintenance of the PDCIP also provides mechanisms for appropriate access, correction, and redress regarding the CIP's use of the PD.*

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

- *Purpose: CIP collects only the required PD for the purpose or intended to be used for the Purpose upon the Data Subject's or its employer's request and voluntary submission of any required PD for the Purpose.*
- *Data Minimization: CIP collects PD directly relevant and necessary to accomplish the Purpose and only retain the PD for as long as is necessary to fulfill the Purpose only.*
- *Use Limitation: CIP uses the PD solely for the Purpose specified in the contract. Sharing PD outside CIP is compatible with or required for the Purpose for which the PD was collected.*
- *Data Quality and Integrity: CIP ensures that PD is accurate, relevant, timely, and complete.*
- *Security: CIP protects the PD (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*
- *Accountability and Auditing: CIP is accountable for complying with these principles, providing training to all employees and contractors who use the PD, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

CIP's Office of the Chief Privacy Officer, therefore, has adopted the FIPPs as its privacy policy framework and seeks to apply them to the full breadth and diversity of CIP programs and activities. Any questions regarding the application or implementation of these principles should be directed to the CIP's Office of the Chief Privacy Officer.

The CPP incorporates the above principles and applies the following privacy principles when CIP processes personal information collected from nations in Europe, Switzerland, the UK, and other countries. The CPP applies to personal data when CIP collects it directly from the data subject (being the person who the data identifies) or collects from employer of the data subject for Purpose.

Data Processing

Data processing is any operation or set of operations involving personal information, whether or not by automatic means, including collecting, using, disclosing, adapting, altering, correcting, retrieving, combining, blocking, erasing, transferring, destroying, recording, organizing, storing, disseminating, or otherwise making available, consulting, and using personal information.

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

Personal Information

As per the CPP, the phrase "Personal Information (PI) or Personal Data (PD)" is limited to the information relevant for the purposes of processing in compliance with the new data retention under the principles of the US-EU Privacy Shield, including Annex I (US-EU-PS), and in compliance with the framework of the US-Swiss Privacy Shield (US-S-PS), collectively "the Privacy Shield" designed by the US Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

CIP Complies with the Privacy Shield

All the information provided by the client is volunteered to procure IP Rights under the US law and will be subject to IP Laws and the Privacy Act of 1974 (P.L. 93-579) (the Privacy Act).

The Privacy Act requires that each individual be given certain information in connection with the submission of any forms related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, it is advised that: (1) the USPTO's general authority for the collection of this information is provided under 35 USC 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the USPTO is to process and/or examine client's submission related to a patent application or patent. If clients do not furnish the requested information, the USPTO may not be able to process and/or examine the submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

CIP follows the USPTO's Statement of Privacy Act in providing information required to procure IPRs volunteered by clients in need of such IPRs from the USPTO. The voluntary information and data including any HR data provided by the client in the USPTO forms and other papers submitted to the USPTO to procure IP rights in the US is subject to routine uses by the USPTO, and the USPTO may disclose the volunteered information to procure IPRs: to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act; to a court, magistrate, or administrative tribunal; to a Member of Congress; to a contractor of the USPTO; to the International Bureau of the World Intellectual Property Organization; to another US federal agency; to the Administrator of General Services or a designee; to the public after either publication of the application or issuance of a patent; to a Federal, State, or local law enforcement agency, as deemed appropriate by the USPTO under the Privacy Act and in compliance with international treaties.

In addition, for the benefit of CIP clients located in the EU, the UK and Switzerland, or US companies' subsidiaries located in the EU, the UK and Switzerland, CIP agrees and complies with

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

the Privacy Shield framework, effective April 12, 2017, in handling any voluntary data that is required by the USPTO or the US Government in procuring the IPRs for the client.

The CPP complies with the Privacy Shield framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. CIP has certified to the Department of Commerce that it adheres to the Privacy Shield framework principles. If there is any conflict between the terms in the CPP and the Privacy Shield framework, the Privacy Shield principles shall govern. To learn more about the Privacy Shield framework (https://www.privacyshield.gov/).

The Privacy Shield framework principles comprise a set of seven commonly recognized privacy principles combined with 16 equally binding supplemental principles, which explain and augment the first seven. Collectively, these 23 principles of the Privacy Shield framework (the Principles) lay out a set of requirements governing participating organizations' use and treatment of personal data received from the EU under the framework as well as the access and recourse mechanisms that participants must provide to individuals in the EU. The Privacy Shield framework requirements include ***notice, choice, access,*** and ***enforcement***.

CIP commits to comply with the Privacy Shield framework, enforceable under the US law; and certifies that it adheres to the Privacy Shield framework principles of ***notice, choice, onward transfer, security, data integrity, access, and enforcement***. To learn more about the Privacy Shield framework requirements, please visit: https://www.privacyshield.gov/.

- CIP provides **notice** to individuals of their data is being collected and about how it will be used.
    - CIP notifies individuals about the purposes for which the information is collected and used, and provides information about how individuals can contact the CIP with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.
- CIP provides **choice** to opt out of the collection and forward transfer of the data to third parties.
    - CIP gives individuals the opportunity to choose to opt out whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual.
- CIP provides **onward transfer (Transfers to Third Parties)** only to third parties that follow adequate data protection principles.
    - To disclose information to a third party, CIP applies the notice and choice principles. Where CIP wishes to transfer information to a third party that is acting as an agent, it makes sure that the third party subscribes to the Privacy Shield

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

principles or is subject to the Directive or another adequacy finding. As an alternative, CIP may enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles and the Standard Contractual Clauses contained in the annex to the European Commission decision 2010/87/EC of 5 February 2010.

- CIP provides **security**, by reasonable efforts to prevent loss of collected information.
    - CIP takes reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- CIP provides **data integrity** that is relevant and reliable for the purpose it was collected for.
    - CIP takes reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
- CIP provides **access to information** to individuals held about them, and correct or delete it if it is inaccurate.
- CIP provides effective **means of enforcing** these rules. In order to ensure compliance with the Privacy Shield framework principles, CIP commits:
  (a) to make readily available and affordable independent recourse mechanisms such as Federal Trade Commission (FTC) or other US courts that may have jurisdiction so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide;
  (b) to have implemented the procedures for verifying the CIP commitment to adhere to the Privacy Shield framework; and
  (c) to fulfill obligations to remedy problems arising out of a failure to comply with the principles through the FTC or other US courts and the Office of Chief Privacy Officer of CIP.

Accessing and Updating Your Personal Information

Whenever you use our services, CIP aims to provide you with access to your personal information. If that information is wrong, CIP strives to give you ways to update it quickly or to delete it – unless CIP has to keep that information for legitimate business or legal purposes. When updating your personal information, CIP may ask you to verify your identity before CIP can act on your request.

CIP may reject requests that are unreasonably repetitive, require disproportionate technical effort (for example, developing a new system or fundamentally changing an existing practice), risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes).

Where CIP can provide information access and correction, CIP will do so for free, except where it would require a disproportionate effort. CIP aims to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

from our services, CIP may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information CIP Shares

CIP does not share personal information with companies, organizations and individuals outside of CIP unless one of the following circumstances applies:

With Your Consent

CIP will share personal information with companies, organizations or individuals outside of CIP with your consent to do so. CIP requires opt-in consent for the sharing of any sensitive personal information.

CIP may contact you periodically in person, by e-mail, by fax, by mail, or by telephone to provide information regarding programs, products, services and content that may be of interest to you, unless you advise us that you do not wish to receive marketing or market research communications from us. If applicable law requires that CIP receives your explicit consent before CIP sends you certain types of marketing communications, CIP will only send you those types of communications after receiving your explicit consent.

For External Processing

CIP provides personal information to trusted businesses or persons to process it for us, based on our instructions and in compliance with our CPP, the Privacy Shield framework and any other appropriate confidentiality and security measures. CIP is bound by the liability under the Privacy Shield framework in cases of onward transfers to third parties.

CIP may transfer information out of the country in which it was collected to any country or territory in the European Economic Area and to any other country that is recognized by the European Union as having adequate privacy protections. CIP will transfer information to other areas only if:

- the transfer is necessary for the performance of a contract between you and CIP or for pre-contractual measures taken in response to your request; or
- if you consent to the transfer; or
- if the data will be adequately protected in the other country, by contract or other protection

CIP has arrangements with all of its offices that assure that personal information transferred among CIP offices is adequately protected, including transfers of personal information (which may include sensitive information) to CIP offices in the United States of America.

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

For Legal Reasons

It is the policy of CIP that a client's confidential information not be disclosed in civil, legislative, or administrative cases or proceedings, unless the client has waived the confidentiality, or under circumstances required by law.

CIP will share personal information with companies, organizations or individuals outside of CIP, only if CIP has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process or enforceable governmental request.
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security or technical issues.
- Protect against harm to the rights, property or safety of CIP, our users or the public as required or permitted by law.

Regarding Subpoena/Court Order/Warrant

Upon the service of any subpoena, court order, warrant or other legal process seeking or purporting to compel disclosure of any of the confidential information of a client; CIP shall promptly notify and will make a good faith effort to cooperate with the client who is the subject of the information so the client has a chance to object to the disclosure or seek qualified protective order from the court. CIP reserves the right to object to the disclosure and will comply with the order appropriately as required by law.

CIP may share aggregated, non-personally identifiable information publicly and with our partners. For example, CIP may share information publicly to show trends about the general use of our services.

If CIP is involved in a merger, acquisition or asset sale, CIP will continue to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes subject to a different CPP, which complies with the Privacy Shield framework.

Information Security

CIP works hard to protect CIP and users from unauthorized access to or unauthorized alteration, disclosure or destruction of information CIP holds. In particular:

- CIP encrypts services provided, where applicable.
- CIP reviews the information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
- CIP restricts access to personal information to authorized CIP employees, contractors and agents who require access for processing purposes, and who are subject to strict contractual confidentiality and non-disclosure obligations.

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

Application

The CPP, which complies with the Privacy Shield framework, applies to all of the services offered by CIP, including services offered on other sites, but excludes services that have separate privacy policies that do not incorporate this CPP.

The CPP, which complies with the Privacy Shield framework, does not apply to services offered by other companies or individuals, including products or sites that may be displayed to you in search results, sites that may include CIP services, or other sites linked from our services. Our CPP, which complies with the Privacy Shield framework, does not cover the information practices of other companies and organizations who advertise our services, and who may use cookies, pixel tags and other technologies to serve and offer relevant ads.

Enforcement, Compliance and Dispute Resolution

CIP regularly reviews its compliance with the CPP, which complies with the Privacy Shield framework. CIP also adheres to several self-regulatory frameworks. In compliance with the Privacy Shield framework, CIP commits to resolve complaints about our collection or use of your personal information. Enforcement of the Privacy Shield framework takes place in the United States in accordance with US law. CIP has procedures for verifying compliance, self-assessment, a dispute resolution system that will investigate and resolve individual complaints and disputes, and to remedy problems arising out of a failure to comply with the privacy principles under the CPP, which complies with the Privacy Shield framework.

CIP cooperates and complies with the EU Data Protection Authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with respect to such data, in order to satisfy the dispute resolution and remedy requirements.

Individuals in the European Union with inquiries or complaints regarding our CPP, which complies with the Privacy Shield framework should first contact CIP at:

Contact Office: *Office of the Chief Privacy Officer (OCPO)*
Contact Name: *Dr. Rao Vepachedu, JD, PhD, LLM*
Contact Title: *Chief Privacy Officer (CPO)*
Contact E-mail: *mail@Cardinal-ip.com*
Contact Phone: *(847) 905-7122 phone*
Contact Fax: *(847) 905-7123 fax*

When CIP receives formal written complaints, CIP will contact the person who made the complaint to follow up. CIP works with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that CIP cannot resolve with our users directly. CIP fully cooperates and complies with the DPAs and the FDPIC to investigate unresolved complaints. If you do not receive timely acknowledgment of your

complaint from us, or if we have not addressed your complaint to your satisfaction, please contact the DPAs and the FDPIC for more information or to file a complaint.

CIP has further committed to refer unresolved the Privacy Shield framework complaints to the DPAs and the FDPIC. CIP agrees to the binding arbitration under the Privacy Shield framework, under certain conditions, if the individual chooses to invoke such "binding arbitration" under the Privacy Shield framework principles. This arbitration option is available to an individual to determine, for residual claims, whether an organization has violated its obligations under the Privacy Shield framework as to that individual, and whether any such violation remains fully or partially un-remedied. This option is available only for these purposes. This option is not available, for example, with respect to the exceptions to the Privacy Shield framework.

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (1) raise the claimed violation directly with CIP and afford CIP an opportunity to resolve the issue within the timeframe set forth in the Privacy Shield framework; (2) make use of the independent recourse mechanism under the Privacy Shield framework, which is at no cost to the individual, at: https://www.privacyshield.gov/assistance; and (3) raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual. For more details, please visit the Privacy Shield framework, http://trade.gov/td/services/odsi/swiss-us-privacyshield-framework.pdf.

The Federal Trade Commission (FTC), the Department of Transportation (DOT), other US government agencies, and/or the states may provide overarching government enforcement of the Privacy Shield framework. The FTC and the DOT have both stated in letters to the European and Swiss Commissions that they will take enforcement action against organizations that state that they are in compliance with the Privacy Shield framework, but then fail to live up to the commitment.

The Department of Commerce will indicate on the public list it maintains of organizations self-certifying adherence to the Privacy Shield framework requirements, any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of the Privacy Shield framework benefits.

Changes

CIP may change the CPP from time to time. However, CIP will not reduce your rights under this CPP, which complies with the Privacy Shield framework, without your explicit consent. CIP will post any changes on this page and, if the changes are significant, provide a more prominent notice (including, for certain services, email notification of privacy policy changes). CIP will also keep prior versions of this CPP in an archive for your review.

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

Officer Certifying Compliance With the Privacy Shield framework

Corporate Officer Name: *Frank Nicolas*
Corporate Officer Title: *President*
Corporate E-mail*: mail@Cardinal-ip.com*
Contact Phone*: (847) 905-7122 phone*
Contact Fax: *(847) 905-7123 fax*

Current Certification Status: https://www.privacyshield.gov/list

This document is available at: http://Cardinal-ip.com/privacy-policy/

Previous Policies are Available at:

- CPP August 1, 2016
- *CPP June-2016.pdf*
- *CPP December-31-2015.pdf*
- *CPP December-2-2014*
- *CPP June-5-2014*
- *CPP April-26-2014*
- *CPPApril-2013*

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax

SELF CERTIFICATION

Corporate Officer who is certifying the CIP's adherence to the Privacy Shield:

Corporate Officer Name: *Frank Nicolas*
Corporate Officer Title: *President*
Corporate Officer Phone: *847.905.7122*
Corporate Officer Fax: *847.905.7123*
Corporate Officer Email: mail@cardinal-ip.com and *rao.vepachedu@Cardinal-ip.com*

Contact:

Contact Office: *Office of the Chief Privacy Officer (OCPO)*
Contact Name: *Dr. Rao Vepachedu, JD, PhD, LLM*
Contact Title: *Chief Privacy Officer (CPO)*
Contact E-mail: rao.vepachedu@Cardinal-ip.com and mail@cardinal-ip.com
Contact Phone: (847) 905-7122 phone
Contact Fax: (847) 905-7123 fax

Description of the activities of the organization with respect to personal information received from the EU:

Personal information required to procure, manage and maintain IPRs for clients and to distribute inventor awards as applicable.

Description of the organization's privacy policy for personal information:

See CPP at: http://www.cardinal-ip.com/privacy-policy/

Please enter the effective date of your organization's privacy policy:

December 31, 2002

Please provide the location of your organization's privacy policy:

The CPP is available at: http://www.cardinal-ip.com/privacy-policy/

The appropriate statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy:

Federal Trade Commission (FTC)

List any privacy programs in which your organization is a member for the Privacy Shield

None

What is your organization's verification method?

Self-assessment

What independent recourse mechanism is available to investigate unresolved complaints (See FAQ 11)?

Enforcement of the Privacy Shield takes place in the United States in accordance with US law. CIP has procedures for verifying compliance, self-assessment, a dispute resolution system that will investigate and resolve individual complaints and disputes, and to remedy problems arising out of a failure to comply with the Privacy Principles under the Privacy Shield. CIP cooperates and complies with the DPAs and the FDPIC with respect to such data, in order to satisfy the dispute resolution and remedy requirements.

What personal data processed by your organization is covered by the Privacy Shield?

Offline, on-line, manually processed data, and human resources data

Do you plan to cover human resources data?

Yes, limited to information required to procure, manage and maintain IPRs for clients and to distribute inventor awards as applicable.

Do you agree to cooperate and comply with the DPAs and the FDPIC?

Yes

Cardinal Intellectual Property Inc.
1603 Orrington Avenue, 20th Floor, Evanston, IL 60201
mail@cardinal-ip.com, (847) 905-7122 phone, (847) 905-7123 fax