



Cardinal Privacy Policy (CPP)

Cardinal is the leading intellectual property services company in the United States. Our clients include Fortune 500 companies, law firms, and educational institutions.

Subject to exceptions, such as *37 CFR 1.56. Duty to disclose information material to patentability* (<http://www.uspto.gov/web/offices/pac/mpep/mpep-2000.pdf>), 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, **Cardinal** protects and uses your personal information only to fulfill your requests and serve you better in the intellectual property services that we provide for you. We do not share your personal details with outside third parties without your consent. We will only send you materials you have indicated you want to receive according to your preferences, and we will honor your opt-out requests. We use cookies and web beacons to help us understand the features that apply to visitors, provide better functionality, and offer you personalized content. We adopt careful procedures to protect your personal information.

Cardinal Privacy Policy (CPP) incorporates the above principles and applies **the following** privacy principles when we process personal information collected from nations in Europe, the Middle East, and Africa. **CPP** applies to personal data when we collect it directly from the data subject (being the person who the data identifies), and also when we collect data from one person (or company or other legal entity) that identifies another person.

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.

Personal information

Personal information is information relating to you that we can use to specifically identify you, such as:

- name
- telephone number
- e-mail address
- date of birth
- address
- social security number or other national identifier
- account number
- any other information that identifies or could identify you and relates to you

As per **CPP**, when we use the phrase personal information, we include sensitive information unless we specifically state otherwise. Sensitive information is personal information revealing or relating to your health,



your racial or ethnic origin, religious or philosophical beliefs, sex life, political affiliation, or trade union membership.

Cardinal Complies with Safe Harbor Principles

CPP complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. Cardinal has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, please visit <http://www.export.gov/safeharbor/>, and to view Cardinal's certification, <http://www.cardinal-ip.com/privacy-policy/>.

- Cardinal provides **notice** to individuals of their data is being collected and about how it will be used.
 - Cardinal notifies individuals about the purposes for which the information is collected and used, and provides information about how individuals can contact the Cardinal 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.
- Cardinal provides **choice** to opt out of the collection and forward transfer of the data to third parties.
 - Cardinal 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.
- Cardinal provides **onward transfer (Transfers to Third Parties)** only to third parties that follow adequate data protection principles.
 - To disclose information to a third party, Cardinal applies the notice and choice principles. Where Cardinal wishes to transfer information to a third party that is acting as an agent, it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding. As an alternative, Cardinal 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.
- Cardinal provides **security**, by reasonable efforts to prevent loss of collected information.
 - Cardinal takes reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
- Cardinal provides **data integrity** that is relevant and reliable for the purpose it was collected for.
 - Cardinal takes reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
- Cardinal provides **access to information** to individuals held about them, and correct or delete it if it is inaccurate.
- Cardinal provides effective **means of enforcing** these rules.
 - In order to ensure compliance with the safe harbor principles, Cardinal makes (a) readily available and affordable independent recourse mechanisms such as Federal Trade Commission or other 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) procedures for verifying that the commitments companies make to



adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles.

Accessing and updating your personal information

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

We 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 we can provide information access and correction, we will do so for free, except where it would require a disproportionate effort. We aim to maintain our services in a manner that protects information from accidental or malicious destruction. Because of this, after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

Information we share

We do not share personal information with companies, organizations and individuals outside of Cardinal unless one of the following circumstances apply:

With your consent

We will share personal information with companies, organizations or individuals outside of Cardinal when we have your consent to do so. We require opt-in consent for the sharing of any sensitive personal information.

We 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 we receive your explicit consent before we send you certain types of marketing communications, we will only send you those types of communications after receiving your explicit consent.

For external processing

We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

Cardinal 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. We will transfer information to other areas only if:



- the transfer is necessary for the performance of a contract between you and Cardinal 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

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

For legal reasons

It is the policy of Cardinal 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.

We will share personal information with companies, organizations or individuals outside of Cardinal if we have 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 Cardinal, 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; Cardinal 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. Cardinal reserves the right to object to the disclosure and will comply with the order appropriately as required by law.

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

If Cardinal is involved in a merger, acquisition or asset sale, we 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 privacy policy.

Information Security

We work hard to protect Cardinal and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold. In particular:

- We encrypt many of our services
- We review our information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.



- We restrict access to personal information to authorized Cardinal employees, contractors and agents who require access for processing purposes, and who are subject to strict contractual confidentiality and non-disclosure obligations.

Application

Our Privacy Policy applies to all of the services offered by Cardinal and its affiliates, including services offered on other sites (such as our advertising services), but excludes services that have separate privacy policies that do not incorporate this Privacy Policy.

Our Privacy Policy 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 Cardinal services, or other sites linked from our services. Our Privacy Policy 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

We regularly review our compliance with our Privacy Policy. We also adhere to several self regulatory frameworks. When we receive formal written complaints, we will contact the person who made the complaint to follow up. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that we cannot resolve with our users directly.

The Federal Trade Commission and the states may provide overarching government enforcement of the Safe Harbor Privacy Principles, under federal or state law prohibiting unfair and deceptive acts. The Department of Commerce will indicate on the public list it maintains of organizations self-certifying adherence to the US/EU/Swiss Safe harbor Framework requirements.

Cardinal cooperates and complies with the EU Data Protection Authorities (DPAs) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) to investigate unresolved complaints. Cardinal elects to satisfy the requirement in points (a) and (c) of the Safe Harbor Enforcement Principle by committing to cooperate with the EU DPAs and Swiss FDPIC; Will cooperate with the EU DPAs and Swiss FDPIC in the investigation and resolution of complaints brought under the Safe Harbor; and Will comply with any advice given by the EU DPAs and Swiss FDPIC when the organization needs to take specific action to comply with the Safe Harbor Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the EU DPAs and Swiss FDPIC with written confirmation that such action has been taken.

The US-EU Safe Harbor Framework, as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from EU member countries to companies in the United States, requires that participating U.S. companies have in place appropriate independent recourse mechanism/s (IRMs) for dispute resolution. Accordingly, Cardinal agrees to participate in the dispute resolution procedures of the panel established by the EU DPAs to resolve disputes pursuant to the Safe Harbor Privacy Principles.



Residents of the EU/EEA whose inquiry has not been addressed to their satisfaction may contact the EU DPAs panel ec-dppanel-secr@ec.europa.eu or individual EU DPAs directly using the information provided at http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_en.htm. Swiss residents whose inquiry has not been addressed to their satisfaction may contact the Swiss FDPIC using the information provided at <http://www.edoeb.admin.ch/kontakt/index.html?lang=en>.

Changes

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

Contact

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

This document is available at: **Cardinal Privacy Policy** (<http://www.cardinal-ip.com/privacy-policy/>)

Previous policy is available at:

<http://www.cardinal-ip.com/wp-content/uploads/2013/04/Cardinal-Privacy-Policy-final.pdf>
<http://www.cardinal-ip.com/wp-content/uploads/2013/04/Cardinal-Privacy-Policy-old.pdf>



SELF CERTIFICATION

Contact Phone: 847.905.7122 Fax: 847.905.7123 Email: mail@cardinal-ip.com

Corporate Officer who is certifying the organization's adherence to the Safe Harbor Framework

Corporate Officer Name: Frank Nicholas
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

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

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

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

See Cardinal privacy policy 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:

Cardinal privacy Policy 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 Safe Harbor purposes (See FAQ 6): None

What is your organization's verification method: In-house

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

Enforcement of the Safe Harbor program takes place in the United States in accordance with U.S. law. Cardinal 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 Safe Harbor Privacy Principles. Cardinal cooperates and complies with the EU data protection authorities and the Swiss Federal Data Protection and Information Commissioner with respect to such data, but may choose to cooperate with the appropriate data protection authorities in order to satisfy the dispute resolution and remedy requirements even where organization human resources data is not involved.

What personal data processed by your organization is covered by the Safe Harbor?

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

Do you plan to cover human resources data? Yes

Do you agree to cooperate and comply with the European Data Protection Authorities? Yes