110 Allen Rd.
Basking Ridge, NJ 07920
T: 973-889-5200
www.collabera.com

Collabera®

Privacy Policy

Collabera LLC henceforth referred to as ('Collabera') strives to comply with applicable laws and regulations related to personal data protection in countries where the company operates. This policy sets forth the basic principles by which the company processes the personal data of customers/clients, candidates, contractors, employees, and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data. The policy reflects Collabera's commitment to protect the personal information and handle it responsibly to meet business, legal and regulatory requirements related to personal data.

Collabera complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework(s) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Collabera has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

Management

To establish a comprehensive privacy policy and Privacy Shield program, Collabera has adopted internationally accepted principles of fair information practice as the basis for this policy. These principles were further aligned with concepts and requirements from the European Union's General Data Protection Regulation (GDPR) 2016/679. **They also follow the framework of the American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP) & the EU-US Privacy Shield and Swiss US privacy shield**

Notice

Collabera shall notify individuals about the purposes for which it collects, processes, stores and/or discloses information about them. Notice should be communicated in a clear and easy-to-understand manner before it uses such information for a purpose other than that for which it was

originally collected or processed by transferring organization or discloses it for the first time to the third party

a) At a minimum, the Notice statement should contain (unless it is evident from the context):

- Its participation in Privacy Shield and provide a link to, or the web address for, the Privacy Shield list.
- The type of personal data that is collected; and the entities and the subsidiaries of the organization adhering to the Principles.
- The purpose for which the personal information is collected and used for;
- Its commitment to subject to the Principles all personal data received from the EU and Switzerland in accordance on the privacy shield
- If there is a legal requirement to collect the personal information the fact will be provided on how the personal information will be used or processed.
- If the information will be collected by or disclosed to third parties, a statement of this fact and the purposes for doing so along with the type and identify of that third party.
- Collabera's liability in cases of onward transfer of information to the third parties
- The right of individuals to access the personal data,
- How individuals can access their information and correct or delete it if it is inaccurate; and how to contact Collabera with questions, corrections, complaints, and disputes including any relevant establishment in the EU and Switzerland that can respond to such inquiries or complaints
- Where feasible, Collabera shall provide the Notice to an individual at or before the time of the collection of Personal Information.
- The choices and means Collabera offers the individuals for limiting the use and disclosure of their personal data
- The requirement to disclose personal information in response to lawful requests by public authorities including to meet national security or law enforcement requirements.
- Under the Privacy shield the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual
- Under the EU-U.S Privacy Shield -Whether it is the panel established by DPA's, an alternative dispute resolution provider based in the EU or/and alternative dispute resolution provider based in the United states.
- Under the Swiss -U.S Privacy Shield the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual and whether it is Commission, an alternative dispute resolution provider based in Switzerland or an alternative dispute resolution provided based in United States.
- The possibility, under certain conditions, for the individual to invoke binding arbitration

Choice and Consent

Collabera shall obtain consent from individuals when required or appropriate. Collabera should also clearly communicate any choices available when personal data is collected or used by a third party or disclosed by Collabera to such parties.

Specifically, when consent is required or appropriate, Collabera shall:

- Request the consent of the individual using the type of consent (opt-out or opt-in) that is required or appropriate.
- Ensure that the choices provided to an individual are complete and clear (e.g., how to "opt-out");
- Inform individuals of the consequences for failing to consent or to provide their information.
- Verify that Collabera's use of individual personal data is consistent with consent obtained; and
- Obtain new consent if personal data will be used for a purpose other than originally disclosed to the individual.
- Inform the individual about the provision to withdraw the consent if required

Consent should be obtained in accordance with EU-U.S Privacy Shield and Swiss-U.S privacy shield laws and regulations (e.g., explicit and/or implicit consent). Additional safeguards that may be required, along with the definition of sensitive or special category of personal data, may vary.

For sensitive information (i.e., personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union member-ship or information specifying the sex life of the individual), Collabera shall obtain affirmative express consent (opt in) from individuals of such information is to be (i) disclosed to the third party or (ii) used for the purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, Collabera shall treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

Collection

Collabera should collect or obtain personal data only in a fair and lawful manner

Specifically, Collabera shall

- Collect only as much personal data as is required by law or needed for the purposes about which the individual has been informed;
- Collect personal data in a fair and non-deceptive manner;
- Clearly indicate to individuals which personal data is required and which is optional at the time of collection;
- Collect personal data from individuals consistent with local country and jurisdictional laws;
- Collect personal data directly from the individual, when possible; and
- Verify that personal data collected from third parties is reliable and legally obtained.

Use and Retention

Collabera shall use, process, store, and/or retain personal data only for legitimate business purposes or as authorized by the individual.

Specifically, Collabera will use, store, and/or process personal data consistent with:

- Stated purposes for which it was collected;
- Consent obtained from the individual; and
- Contractual, regulatory, and local country laws and requirements.

Collabera shall retain Personal data in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a. This obligation does not prevent organizations from processing personal information for longer periods for the time and to extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific and historical research, and statistical analysis. In these cases, such processing shall be subject to the other principles and provisions of the Framework and the personal information shall be destroyed according to applicable Collabera data retention policies and procedures.

Purposes of Use

Managing Personnel:

- To manage personnel and employment matters
- To set up a personnel file
- To administer compensation, bonuses, equity grants, other forms of compensation, and benefits

- To manage vacation, sick leave, and other leaves of absence
- To provide training
- To evaluate job performance and consider employees for other internal positions
- To develop a talent pool and plan for succession
- Career development activities
- For diversity and inclusion programs
- To conduct employee surveys
- To engage in crisis management
- To fulfill recordkeeping and reporting responsibilities
- To maintain an internal employee directory and for purposes of identification
- To facilitate communication, interaction, and collaboration among employees
- To arrange team-building and other morale-related activities
- To manage employee-related emergencies, including health emergencies
- To promote the Company as a place to work
- To arrange and manage Company sponsored events and public service activities
- Workforce reporting and data analytics/trend analysis
- To design employee retention programs

Monitoring, Security, And Compliance:

- To monitor use of Company information systems and other electronic resources
- To conduct internal audits
- To conduct internal investigations
- To administer the Company's whistleblower hotline
- To protect the safety and security of the Company's facilities employees
- law enforcement and cooperate in investigations

Conducting Our Business:

- For communications with prospective, current, and former customers
- To make business travel arrangements
- To engage in project management
- To manage business expenses and reimbursements
- To promote the business
- To provide a directory and contact information for prospective and current customers and business partners
- To facilitate administrative functions and information technology operations and for legal reasons and corporate transactions.
- To manage and operate information technology and communications systems, risk management and insurance functions, budgeting, financial management and reporting, strategic planning.

- To manage litigation involving the Company, and other legal disputes and inquiries and to meet legal and regulatory requirements;
- in connection with a corporate transaction, sale, or assignment of assets, merger, divestiture, or other changes of control or financial status of the Company or any of its subsidiaries or affiliates; and
- to manage licenses, permits and authorizations applicable to the Company's business operations.

Access & Correction

Collabera shall provide access to individuals about whom it processes personal data an opportunity to access and correct their information. Specifically, Collabera shall provide a:

- Response to the request for access to personal data in a timely manner, in a format convenient for both Collabera and the individual; and
- Chance to review the personal data, challenge its accuracy, and have it corrected, amended or deleted.

Collabera shall authenticate individuals before allowing access to or providing personal data. Access to personal data may be denied if an unreasonable request is made (e.g., requests that do not follow the procedure outlined in the privacy notice or requests which would provide personal data about others besides the requesting individual). However, in cases in which access is denied, Collabera shall provide a reason to the individual and a point of contact for further inquiry

Individual's (PII Principal's / Data Subject's) Rights

- **Right to Access the PII Principals Personal Information**
  - The PII Principals have the right to access the personal information that Collabera hold about you in many circumstances, by making a request. This is sometimes termed 'Subject Access Request'. If Collabera agrees that they are obliged to provide personal information to the PII Principals (or someone else on your behalf), Collabera shall provide it to the PII Principals or they free of charge / processing fees (if applicable) and aim to do so within 30 days from when your identity has been confirmed.
  - Collabera would ask for proof of identity and sufficient information about the PII Principals interactions with us that Collabera can locate your personal information.

- If the PII Principals would like to exercise this right, please contact us at privacy@collabera.com

- **Right to Correction the PII Principals Personal Information**
  - If any of the personal information Collabera hold about you is inaccurate or out of date, the PII Principals may ask us to correct it.
  - If the PII Principals would like to exercise this right, please contact us at privacy@collabera.com.
- **Right to Object / Stop or Limit Collabera's Processing of the PII Principals Data**
  - the PII Principals may instruct Collabera at any time not to process the PII Principals personal information for training & recruitment purposes. If you would like to exercise this right, please contact us at privacy@collabera.com
  - Collabera may withhold personal information that you request to the extent permitted by law.
  - To exercise your rights please send an email at privacy@collabera.com.
- **Other Rights:**

- the PII Principals may also exercise any of the following rights:

1.
    1. Object to the processing their PII for certain activities such as direct marketing purposes
    2. Object to decisions based solely on automated processing (including profiling), which produces legal effects or significantly affects them;
    3. Request for erasure of their personal data;
    4. Request to provide data to a different PII controller (data portability) in a structured, commonly used and machine readable format; and
    5. Withdraw consent to the storage and processing of their personal data.

- To exercise your rights please send an email at privacy@collabera.com.

Disclosure and Onward Transfer

Collabera may share an individual's personal data, acting as a controller, with Third Parties as required for normal business operations, including providing services to employees, customers/clients etc; complying with the notice and choice Principles. When disclosing information Collabera shall:

- Only disclose personal data to Third Parties for the purposes identified in the notice provided to individuals;

- Verify that Collabera's actions align with the consent provided by the individual, in addition to any legal and/or regulatory requirements;
- Require Third Parties, through contractual clauses and/or written agreements to adhere to a baseline of privacy and information security controls- as approved by the respective legal team; and
- Require Third Parties to process personal data in accordance with the individuals' choices and consent
- Take reasonable and appropriate steps to stop and remediate unauthorized processing by such third party.
- Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

Collabera director, officer, employee, or contractor is responsible for each Third Party relationship to ensure compliance with this Policy by such Third Party.

Security

Collabera shall take reasonable precautions, including administrative, technical, and organizational, personnel, and physical measures, to safeguard personal data against loss, misuse and unauthorized access, disclosure, alteration, destruction, and theft, taking into account the risks involved in the processing and the nature of the personal data.

- Collabera shall take reasonable technical and organizational precautions to prevent the loss, misuse, or alteration of your personal information.
- Collabera shall store all the personal information you provide on our secure (password- and firewall-protected) servers.

Data Integrity, Data Quality, Data Security & Purpose Limitation

Collabera shall employ reasonable processes to keep personal data accurate, complete, and up-to-date and in the event that personal data changes must update the change immediately. Shall limit the purposes for which it was collected Collabera shall not process personal information in a way

that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. Collabera undertakes to protect Personal Data using commercially reasonable organizational, technical, and administrative procedures to protect against unauthorized or unlawful access, processing, disclosure, alteration, destruction or accidental loss of your personal data. These precautions include password protections for online information systems and restricted access to Personal Data.

Collabera shall:

- Implement procedures to keep personal data as accurate, complete, and up to date as needed; and
- To the extent feasible, allow and encourage individuals to keep their personal data accurate, complete and up to date.
- Collabera may assign different types of data different security levels, with appropriate corresponding security precautions. Collabera also restricts access to Personal Data to those Personnel that have a legitimate business need for such access

Monitoring, Recourse, Enforcement & Liability

Collabera is committed to monitoring and enforcing ongoing compliance with this policy and with applicable privacy laws, regulations, and obligations.

- Collabera's Effective privacy protection includes robust mechanisms for assuring compliance with the principles, Monitoring the dataflow, recourse for individuals who are affected by non-compliance with the principles and consequences for the organization when the principles are not followed. At a minimum such mechanisms shall include:
    - readily available independent recourse mechanisms by which each individual's complaints and disputes are expeditiously resolved at no cost to the individual and by reference investigated and to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
    - follow-up procedures for verifying that the attestations and assertions about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
    - obligations to remedy problems arising out of failure to comply with the Principles by Collabera announcing their adherence to them and consequences in case of non-adherence.

Collabera and their selected independent recourse mechanisms shall respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield.

- Collabera is obligated to arbitrate claims and follow the terms, provided that an individual has invoked binding arbitration by delivering notice at issue and following the procedures and subject to conditions
- In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à- vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Privacy Shield Principles. This will be the most efficient way to address the often-overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.
- A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.
- In the context of an onward transfer, Collabera has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf and remains liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless Collabera proves that it is not responsible for the event giving rise to the damage.
- In any case if Collabera is subjected to an FTC or court order based on non- compliance, shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements.

Data Security Incident Notification

Where required by applicable law, Collabera shall follow applicable procedures to notify individuals, in a timely manner, when a data security incident has occurred, and has resulted or could result in unauthorized access or acquisition of personal information. Colleagues who suspect such an incident should immediately contact the privacy office.

Data Breach Management

All employees must inform their immediate supervisor, functional head, or the Privacy Team (privacy@collabera.com) immediately about potential or actual instances of violation of the terms of this policy. The Privacy Team will work with the functional head to minimize the impact of data loss, and jointly work out a communication plan. Depending on the classification of the data breach, e.g., whether sensitive data was lost or not, incident information will be shared with the data subject, customers, and business partners as appropriate.

Any reported privacy incident must be managed in the following manner

- Collabera shall classify the incident as a Major incident and follow the defined incident management procedure
- Collabera shall investigate if any Personal Data (PII) has been breached
- If any Personal Data (PII) is breached, Collabera shall identify the extent of the breach and impacted information
- Collabera shall notify the PII Principal / Data Subjects and the Supervisory Authorities immediately (ideally within 72 hours from the breach)
- Collabera shall take appropriate measures while closing the incident so that similar incident can be avoided in future
- Collabera shall perform a root cause analysis after the privacy incident is closed and record the details for future reference

Consequence of Non-Compliance

All Collabera businesses, functions, and regions not only internally by employees, but also by all Collabera temporary staff, contractors, service providers, and consultants are expected to fully comply with this policy.

EXCEPTIONS

Under certain -limited or exceptional circumstances, Collabera may, as permitted or required by applicable laws and obligations, process personal data without providing notice or seeking consent.

Examples of such circumstances include investigation of specific allegations of wrong doing or criminal activity; protecting employees, the public or Collabera from harm or wrongdoing; cooperating with law enforcement agencies; auditing financial results or compliance responding to legal requirements or process; meeting legal or insurance requirements or defending legal claims or interests; satisfying labor laws or agreements or other legal obligations; in emergency situations, when vital interests of the individual, such as life or health, are at stake etc.

In addition, Collabera may, as permitted or required by applicable law and obligations, process personal data without providing access, such as in the circumstances described above; when the privacy interests of others would be jeopardized; or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy.

Sensitive Data

Collabera is not required to obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:

- in the vital interests of the data subject or another person;
- necessary for the establishment of legal claims or defenses;
- required to provide medical care or diagnosis;
- carried out in the course of legitimate activities by a foundation, association or any other non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
- necessary to carry out the Collabera's obligations in the field of employment law; or
- related to data that are manifestly made public by the individual.

Performing Due Diligence and Conducting Audits

- The activities of auditors and background verification agencies may involve processing personal data without the consent or knowledge of the individual. This is permitted by the Notice, Choice, and Access Principles under the circumstances described below.
- Public stock corporations and closely held companies, including Privacy Shield organizations, are regularly subject to audits. Such audits, particularly those looking into potential wrongdoing, may be jeopardized if disclosed prematurely. Similarly, a Privacy Shield organization involved in a potential merger or takeover will need to perform, or be the subject of, a "due diligence" review. This will often entail the collection and processing of personal data, such as information on senior executives and other key personnel. Premature disclosure could impede the transaction or even violate applicable securities regulation. Investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of organizations' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures, or other similar transactions carried out by investment bankers or auditor
- If the personal information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, the organization would have to disclose that information even if it is relatively difficult or expensive to provide. If the personal information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, an organization would have to provide access to such information.

Limitation to access

An organization may set reasonable limits on the number of times within a given period that access requests from a particular individual will be met. In setting such limitations, an organization should consider such factors as the frequency with which information is updated, the purpose for which the data are used, and the nature of the information.

The Privacy Shield Principles are relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data, or the use of anonymized data does not raise privacy concerns.

The Data Protection Officer shall approve exemptions from adherence to particular provisions of this policy. Exemptions to this policy will only be considered if special circumstances do not allow for the practical implementation of a requirement, if a local or regional law or regulation supports a requested exemption, and if there are compensating controls in place to mitigate the risk.

Human Resource Data

Coverage by the Privacy Shield

Where Collabera HR/ Ops / Delivery team members in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Privacy Shield, the transfer enjoys the benefits of the Privacy Shield. In such cases, the collection of the information and its processing prior to transfer shall be subjected to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws shall be respected.

- The Privacy Shield Principles shall be relevant only when individually identified or identifiable records are transferred or accessed. Statistical reporting relying on aggregate employment data and containing no personal data, or the use of anonymized data does not raise privacy concerns.

Application of the Notice and Choice Principles

Collabera US receives employee information from the EU under the Privacy Shield may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where Collabera intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, Collabera shall provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information has been collected or subsequently authorized by the individual. Moreover, such choices shall not be used to restrict employment opportunities or take any punitive action against such employees.

- Certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.
- In addition, Collabera shall make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.
- To the extent and for the period necessary to avoid prejudicing the ability of Collabera as an organization in making promotions, appointments, or other similar employment decisions, does not need to offer notice and choice.

Application of the Access Principle

- The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, Collabera team members in the European Union shall comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. Collabera shall adhere to the Privacy Shield requirements of processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

Recourse mechanism(s) / Dispute Resolution:

In compliance with the Privacy Shield Principles, Collabera commits to resolve complaints about our collection or use of your personal information. European Union and Swiss, individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Collabera at: privacy@collabera.com

Collabera has further committed to refer unresolved Privacy Shield complaints to EU Data Protection Authorities (DPA's), an alternative dispute resolution provider located in the EU, or Switzerland, as applicable. If you do not receive timely acknowledgment of your complaint from us, or if we have not resolved your complaint, please contact The International Centre for Dispute Resolution (ICDR) by

Mail:
International Centre for Dispute Resolution Case Filing Services
1101 Laurel Oak Road, Suite 100
Voorhees, NJ 08043
United States

Or sending by email box: casefiling@adr.org
Collabera commits to cooperate with the panel established by the EU data protection authorities (DPAs) and/or the Swiss Federal Data Protection and Information Commissioner, as applicable and comply with the advice given by the panel and/or Commissioner, as applicable with regard to human resources data transferred from the EU and/or Switzerland, as applicable in the context of the employment relationship.