Calabrio UK, Ltd. GDPR Employee Privacy Notice

Our Commitment

Calabrio UK Ltd. ('we' or 'us' or 'our' or 'Calabrio') are committed to ensuring the security and protection of any personal information that we process on account of your employment with us, and to providing a compliant and consistent approach to data protection. Our data protection program has always been effective, compliant with existing law, and adherent to all existing data protection principles. In furtherance of that goal, we recognise our obligations in updating and expanding our current program to meet the standards set forth within the General Data Protection Regulation ('GDPR').

Calabrio is a "data controller" meaning that we are responsible for deciding how we hold and use personal information about you ("Employee Data"). Our goal is to ensure the appropriate safeguarding of the personal information we hold. We have developed a data protection and privacy system that is effective and that shows our commitment to the principles of the GDPR. Our objectives for GDPR compliance are summarised in this Notice and have been implemented to operate in conjunction with our policies related to employment, benefits, and information security.

This Notice applies to all employees located in the European Union. It does not form part of any contract of employment. We may amend it at any time as permitted by applicable law and will notify you of any material changes.

Your Information: Categories of Employee Data

As your employer, Calabrio collects, maintains, and processes information about you for normal employment purposes throughout the course of your relationship with us, including without limitation:

- **Identification Data:** first and last name; age and date of birth; gender; marital status; race; citizenship; government-issued identification number; family information, including information about dependents; passport information; and other data collection permitted or required by applicable law;
- **Contact Data:** home and work address; phone numbers; personal email addresses; and emergency contact details;
- **Monitoring and Internal Investigation Data:** computer usage information about your use of company equipment, systems and other resources;
- **Financial Data:** salary information; tax, banking or financial information; bank account where employee salary and other work related payments are deposited; expense records and the related credit card statements; pension plans and related information;
- **Communication Data:** email content, business letter content, business documents and chat content;
- **Background Data:** professional photograph; curriculum vitae information; previous employment; certifications; and education and training;
- **Workforce Administration Data:** terms and conditions of employment; details of grade and job duties; absence records, including holiday records and self-certification forms; employee evaluation information; business travel data; details of any disciplinary or

grievance investigations and proceedings; training records; performance related information; employment and/or commission agreements; and documents related to termination;

- **System Usage Data:** user ID and passwords used by employee to access Calabrio premises, computer or telecommunications network; Internet Protocol (IP) address or other device location information of the desktop, laptop or other devices used by or on behalf of employee to access Calabrio's computer or telecommunications network onsite or through a remote connection.

We collect personal information about you through the application and recruitment process, either directly from you or sometimes from a recruitment agency. We may sometimes collect additional information from third parties including former employers or entities to which you provided services. We will also collect additional personal information in the course of job-related activities throughout the period that you work for us.

In addition, we collect, process, and use the following special categories of Employee Data about you from you or from authorised third parties (e.g., your supervisor, public authorities or public resources) in connection with your employment (collectively, "**Sensitive Employee Data**"):

- **Insurance and Benefits Data (to the extent permitted and in accordance with applicable law)** for the purposes of administering and processing health insurance and claims, employee compensation insurance and claims, and your life insurance and other insurance and claims (including information about you and your dependants that we provide to the insurer), and compliance with applicable laws and worker-related requirements (e.g., work safety, reporting obligations);
- **Sick Day Information** for purposes of administering and providing compensation, administering the workforce (e.g., workforce planning), and compliance with applicable laws and worker-related requirements (e.g., statutory wage tracking);
- **Work-related Accidents Information** for purposes of administering and providing compensation (e.g., insurance compensation), and compliance with applicable laws and worker-related requirements (e.g., work safety, reporting obligations);
- **Disability Information** (if provided voluntarily) for purposes of administering the workforce (e.g., making accommodations in the workplace) and compliance with applicable laws and worker-related requirements;
- **Information on Maternity Leave** for purposes of administering the workforce (e.g., workforce planning), and compliance with applicable laws and worker-related requirements;
- **Information regarding racial or ethnic origin** and relevant special categories of data necessary to monitor compliance with equal opportunities legislation;
- **Information required under Immigration Laws,** including citizenship data, passport data, details of residency, or work permit data; and
- **Unlawful or Objectionable Behavior** to enable us to assess an individual's suitability for a role.

Purposes and Basis for Processing Employee Data

Sensitive Employee Data is collected, processed, and used for the purposes mentioned above, and Employee Data is collected, processed, and used for the following purposes (collectively, "**Processing Purposes**"):

Processing Purposes	Categories of Employee Data Involved
Administering and providing compensation, including administering and providing payroll bonus, stock options and other applicable incentives	Identification data, contact data, communication data, financial data, workforce administration data and insurance and benefits data
Administering and providing applicable benefits and other work-related allowances, including reporting of benefit entitlements and use	Identification data, contact data, communication data, financial data, background data, workforce administration data, insurance and benefits data
Administering the workforce and performance management, including managing work activities, providing performance evaluations and promotions, producing and maintaining corporate organisation charts, matrix management, entity and intra-entity staffing and team management, managing and monitoring business travel, carrying out workforce analysis, conducting talent management and career development, leave management/approvals, providing references as requested, and administering ethics and compliance trainings	Identification data, contact data, financial data, communication data, background data, workforce administration data, system usage data, information required under Immigration Laws, insurance and benefits data, internal investigation data, and system usage data
Complying with applicable laws and worker-related requirements along with the administration of those requirements, such as income tax, national insurance deductions, and employment, worker and immigration laws	Identification data, contact data, communication data, financial data, background data, workforce administration data, information required under Immigration Laws, and insurance and benefits data
Monitoring of the use of company technology resource systems, databases and property, and ensuring compliance with applicable Calabrio policies and procedures	Identification data, contact data, communication data, monitoring and internal investigation data, workforce administration data, and system usage data

Communicating with you, other Calabrio employees, workers and consultants, and third parties (such as existing or potential business partners, suppliers, customers, end-customers or government officials)	Identification data, contact data, and communication data
Communicating with your designated contacts in case of an emergency, including when necessary to protect the health and safety of Calabrio employee and others, ensuring business continuity, securing IT infrastructure, and ensuring a systemic disaster recovery plan	Identification data and contact data
Responding to and complying with requests and legal demands from regulators or other authorities in or outside of your home country	Identification data, contact data, monitoring and internal investigation data, financial data, communication data, background data, workforce administration data, system usage data, insurance and benefits data, information required under immigration laws
Complying with corporate financial responsibilities, including audit requirements (both internal and external), accounting, and cost/budgeting analysis and control	Identification data, contact data, monitoring and internal investigation data, financial data, communication data, background data, and workforce administration data
Managing corporate information technology, including helpdesk, corporate/ active directory, IT support, and IT security	Identification data, contact data, monitoring and internal investigation data, and workforce administration data

Calabrio relies on the following legal grounds for the collection, processing, and use of Employee Data and Sensitive Employee Data:

Employee Data	Sensitive Employee Data
• Performance of the employment contract; • Legitimate interest of Calabrio, Calabrio's affiliates or other third parties (such as existing or potential business partners, suppliers, customers, end-customers, governmental bodies, or courts)	• Explicit consent, as permitted by applicable data protection law; • Carrying out the obligations and exercising the specific rights of Calabrio or you in the field of employment, worker, social security and social protection law as permitted by EU or applicable data

where the legitimate interest could be in particular - o implementation and operation of a group-wide matrix structure and group-wide information sharing, o right to freedom of expression or information, including in the media and the arts, o customer relationship management and other forms of marketing, o prevention of fraud, misuse of company IT systems, or money laundering, o operation of a whistleblowing scheme, o physical security, IT and network security, o internal investigations, and o intended mergers and acquisitions; • Consent, as permitted by applicable law; • Compliance with legal obligations, in particular in the area of labour and employment law, social security and protection law, data protection law, tax law, and corporate compliance laws; • Establishing, exercising, or defending legal claims or as required whenever courts are acting in their judicial capacity; • Protection of the vital interests of you or of another individual; and • Performance of a task carried out in the public interest or in the exercise of official authority vested in Calabrio.	protection law or by a collective agreement; • Protection of the vital interests of you or of another individual where you are physically or legally incapable of giving consent; • Public data as made public manifestly by you; • Establishing, exercising, or defending legal claims or as required whenever courts are acting in their judicial capacity; • For substantial public interest, as permitted by applicable data protection law; and • For assessment of your working capacity, as permitted by applicable data protection law.

• Where authorized by, and in accordance with, EU or EU member state law.	

We may process your Employee Data or Sensitive Employee Data for more than one reason depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific reason we are relying on to process your Employee Data or Sensitive Employee Data where more than one reason has been set out in the table above.

In general, you are required to provide Employee Data and Sensitive Employee Data when we request it, except in limited instances when we indicate that certain information is voluntary (e.g., in connection with employee or worker satisfaction surveys).

If you do not provide certain information when requested, there may be circumstances in which we are unable to comply with our obligations and we will provide information about the implications of that decision.

Our Use of Third Parties

We may share Employee Data or Sensitive Employee Data with third parties solely to support processing related to the purposes stated herein. Such third parties include without limitation payroll processing companies, human resources information systems (HRIS), travel and expense reporting, recruiting agencies, and other integral activities related to your employment.

If the Calabrio business for which you work is sold or transferred in whole or in part, or if Calabrio is acquiring and integrating another entity into the Calabrio business for which you work (or any similar transaction is being contemplated), your Employee Data or Sensitive Employee Data may be transferred to the other entity (e.g., the new employer, potential new employer, the new acquired entity, or potential new acquired entity) before the transaction (e.g., during the diligence phase) or after the transaction, subject to any rights provided by applicable law, including jurisdictions where the other entity is located.

Certain third party service providers, whether affiliated or unaffiliated, may receive your Employee Data or Sensitive Employee Data to process that data under appropriate instructions ("Data Processors") as necessary for the Processing Purposes. Such service providers will be subject to contractual obligations to implement appropriate technical and organisational security measures to safeguard the Employee Data or Sensitive Employee Data, and to process the Employee Data or Sensitive Employee Data only as instructed. All third parties who currently, or may in the future, have access to or process your Employee Data or Sensitive Employee Data will do so solely under a written agreement with us that includes assurances regarding protection of the confidentiality and integrity of your Employee Data or Sensitive Employee Data, including by ensuring appropriate GDPR-related safeguards are met while such third party has access to or processes your Employee Data or Sensitive Employee Data. If you have any questions about the third parties we use for processing of your Employee Data or Sensitive Employee Data, including the types of safeguards such third parties have implemented with respect to your Employee Data or Sensitive Employee Data please contact the Human Resources or Legal departments using the contact information contained in this Notice.

Except as otherwise provided herein, we will only disclose your Employee Data or Sensitive Employee Data to third parties if we are legally required to do so or in circumstances where we need to comply with our contractual duties to you, including for the purposes described above.

Calabrio UK Ltd. are owned and operated by Calabrio, Inc., located in the USA. As such, we may transfer your Employee Data or Sensitive Employee Data about you to Calabrio, Inc., located in the USA, and its affiliates and subsidiaries solely for purposes connected to your employment or the management of our business. In furtherance of this interest, your Employee Data or Sensitive Employee Data may be transferred outside of the European Union. We have implemented safeguards for the transfer of such information, including policies regarding information security and the protection of personal data, a required annual training program regarding security awareness, and other programs designed to ensure the security and integrity of your Employee Data or Sensitive Employee Data. Whenever we transfer your Employee Data and/or Sensitive Employee Data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- we will only transfer your Employee Data and/or Sensitive Employee Data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission;

- where we use certain service providers, we may use specific contracts approved by the European Commission which give Employee Data and/or Sensitive Employee Data the same protection it has in Europe; or

- where we use providers based in the USA, we may transfer information to them if they are part of the Privacy Shield which requires them to provide similar protection to personal information shared between the Europe and the USA.

Calabrio may also disclose your Employee Data or Sensitive Employee Data as required or permitted by applicable law to law enforcement agencies, government or regulatory authorities, court authorities, and external professional advisers.

Our Obligations

Employee Data or Sensitive Employee Data collected, processed, and maintained pursuant to the purposes listed in this Notice will be stored. by Calabrio or our service providers for no longer than is necessary for the performance of our obligations or to achieve the purposes for which the information is collected, or as may be permitted under applicable data protection laws.

To determine the appropriate retention period for Employee Data or Sensitive Employee Data, we consider the amount, nature, and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure of the data, the purposes for which we process the data and whether we can achieve those purposes through other means, and the applicable legal requirements.

When Calabrio no longer needs to use your Employee Data or Sensitive Employee Data, we will remove it from our systems and records or take appropriate steps to properly anonymise it so that

individuals can no longer be identified from it (unless we need to keep your Employee Data or Sensitive Employee Data to comply with legal or regulatory obligations that apply to Calabrio).

If in the future we intend to process your Employee Data or Sensitive Employee Data for a purpose other than the purpose in which it was initially collected, we will provide you with information regarding the new purpose, as well as any additional information you request regarding the new purpose for processing.

All Employee Data or Sensitive Employee Data will be handled by us strictly in confidence and by individuals on a need-to-know basis. All individuals handling Employee Data or Sensitive Employee Data under this Notice will have undergone an annual security awareness training, as described in the "*Our Use of Third Parties*" section, will conduct an annual review and signoff on the Global Security Policy, and will otherwise be bound by obligations of confidentiality to us that are requisite for the nature of the processing.

If we become aware of a confirmed breach of your Employee Data or Sensitive Employee Data, we will provide notification to you as soon as reasonably practicable, but in any case, in accordance with the timeframes mandated under GDPR.

Your Rights

Under the GDPR and other applicable data protection laws or authorities you have a number of rights with respect to your Employee Data or Sensitive Employee Data. You may have the right to request access to and rectification or erasure of your Employee Data or Sensitive Employee Data, the right to restrict or halt any processing of your Employee Data or Sensitive Employee Data, the right to object to processing, and the right to data portability. If you opt to restrict or halt processing of your Employee Data or Sensitive Employee Data or object to its processing, we will provide information about how that decision may affect certain aspects of the relationship (see further detail on each of these rights below).

Your request to access the information that we hold may include without limitation, access to the categories or classifications of personal data we maintain or process (including the data itself) and any uses which we may have made of your Employee Data or Sensitive Employee Data.

Please note that the rights mentioned above might be limited under the applicable national data protection law.

1. **Right of access:** You may have the right to obtain from us confirmation as to whether or not Employee Data or Sensitive Employee Data concerning you is processed, and, to request access to the Employee Data or Sensitive Employee Data. This is not, however, an absolute right, and the interests of other individuals may restrict your right of access. Further, you may have the right to obtain a copy of their Employee Data or Sensitive Employee Data undergoing processing. For additional copies, we may charge a reasonable fee based on administrative costs.

2. **Right to rectification**: You may have the right to obtain from us the rectification of inaccurate Employee Data or Sensitive Employee Data about you. Depending on the

purposes of the processing, you may have the right to have incomplete Employee Data or Sensitive Employee Data completed, including by means of providing a supplementary statement.

3. **Right to erasure (right to be forgotten):** Under certain circumstances, you may have the right to obtain from us the erasure of Employee Data or Sensitive Employee Data concerning you, and we may be obligated to erase that Employee Data or Sensitive Employee Data.

4. **Right to restriction of processing:** Under certain circumstances, you may have the right to prevent us from processing of your Employee Data or Sensitive Employee Data. In that case, your data will be marked and may only be processed by us for certain limited purposes.

5. **Right to data portability:** Under certain circumstances, you may have the right to receive the Employee Data or Sensitive Employee Data about you, which you have provided to us, in a structured, commonly used and machine-readable format, and you may have the right to transmit that data to another entity without hindrance from us.

6. **Right to object:** Under certain circumstances, you may have the right to object to the processing of your Employee Data or Sensitive Employee Data by us where we are relying on a legitimate interest and there is an impact on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override certain of your rights and freedoms.

If you have provided consent for the processing of your Employee Data or Sensitive Employee Data, you have the right in certain circumstances, to withdraw consent at any time. A withdrawal of consent will not affect the lawfulness of the processing prior to the withdrawal. If you request to restrict or halt processing or object to processing, or if you withdraw consent, there may be legal reasons requiring us to preserve your Employee Data or Sensitive Employee Data within our systems. We will only maintain your Employee Data or Sensitive Employee Data in conjunction with any legal obligations we have with respect to your Employee Data or Sensitive Employee Data, we will inform you of the decision to maintain your Employee Data or Sensitive Employee Data, and we will provide rationale for the legal basis.

Some of the Employee Data or Sensitive Employee Data we collect, process, and maintain is subject to a legal basis and not subject to consent and, if you withdraw consent or opt to restrict, halt, or object to processing, we will provide additional information into our legal basis for processing. In short, the legal basis for which we may collect, process, and maintain your Employee Data or Sensitive Employee Data is for the performance of a contract with you or to take steps to enter into a contract, to enable us to meet our statutory or legal obligations (such as auditing and regulatory purposes), and for our legitimate interests in processing such information, provided that the benefits of our legitimate interests are not outweighed by your fundamental rights or freedoms.

You have the right to issue a complaint to the Information Commissioners' Office if, at any given time, you believe we are not in compliance with the GDPR or DPA with respect to your Employee Data or Sensitive Employee Data.

To exercise your rights, please contact us via the Contact Information set out below.

Applicability

This Notice is intended to be applied concurrently with other policies established by us over the course of your employment, including any policies published by Human Resources with respect to employment matters or your benefits and any policies published by the business for information security, safeguarding information, and compliance. You should refer to these policies, which are provided and available to you over the intranet or through our HRIS.

Changes to this Notice

We recognise that the collection, holding, processing, and destruction of your Employee Data or Sensitive Employee Data throughout our relationship with you is an ongoing responsibility and we will review this Notice following the same review periods as we use for our other policies.

Our Contact Information

If you have any questions about this Notice, please contact Human Resources (hr@calabrio.com) or Legal (legal@calabrio.com).

Publication Date: March 15, 2019