Cigniti

CPL028_Privacy Policy

Version 9.0

1.0 Cigniti's privacy policy

"We are committed to maintaining the privacy and security of the personal information provided by all of our clients and employees".

2.0 Scope

This policy applies to the any personal information which Cigniti Technologies Limited may collect when you visit our website (https://www.cigniti.com), visit our office premises, during the process of prospecting, marketing, recruitment and exchanging information for the purpose of new business or expansion.

This privacy policy also covers the type of personal information that we collect and what do with do with the information collected through various sources. This policy also describes the cookies being used at the website and about third parties' use of cookies.

This policy applies in both the capacities - where we are acting as a data processor – for the Quality & Digital Assurance services that we deliver to our existing and potential clients and also where we are acting as a Data controller with respect to the personal data of our website visitors, employees, email recipients and personal data collected from public sources; in other words, where we determine the purposes and means of the processing of that personal data.

If you are a California resident, please see the below section on our specific privacy policy statement for California residents. For visitors from the EU/EEA, please see the section below 'Visitors from the EU/EEA' for additional rights under the General Data Protection Regulation (GDPR) and Legal basis for processing Personal Data.

This privacy policy does not apply to the practices of any legal entities or companies that Cigniti does not control or own, or to any people that Cigniti does not manage or employ. In this policy, "we", "us" and "our" refers to Cigniti Technologies Limited. For more information about us, please visit https://www.cigniti.com.

3.0 Information we collect

Cigniti collects and processes your personal information to meet our legal, statutory and contractual obligations and to provide you with our quality engineering and testing services. We will never collect any unnecessary personal data from you and do not process your information in any way, other than as specified in this notice. Reference to a data subject means a natural person whose personal data is processed by a data controller or a data processor.

All the personal information mentioned in the table below is collected 'directly' (example - when you provide information to sign up for a newsletter, whitepaper, web resource or register to comment on a forum website) and 'indirectly' (example - through our website's technology or cookies) including third-parties such as public authorities, websites and social media and networking platforms, suppliers/vendors proving or selling legitimate personal data. It is completely up to you to decide before providing any personal information.

We collect personal data of our clients, vendors/suppliers, prospects, website users, visitors (website and physical site), employees, candidates/potential employees, business contacts and shareholders. For any other specific data collection requirement not listed here and arising out of business requirements or required by law, we will issue the concerned individuals appropriate notice of the data to be collected and purpose for the same.

Please refer the table below for the categories of personal data and associated details –

Personal Information Category	Details
Personal details	Name, Company, Email address and Phone number
Contact details and identifiers	Name, Company, Email address, Phone number and attachments, if any
Marketing, Lead generation/Inside Sales and related information	Name, Company, Email address and Phone number. Social media identifiers including the posts on social media by individual or company, publicly available information and identifiers including any analytics and profiles of the individual available, details from the third-party owned/sold personal data. Data coming through online and offline marketing events including seminars, marketing campaigns (including ads), webinars, guest speakers, testimonials, workshops, road shows, business calls and meetups, trade fairs and similar events. IP address, web history data, including operating system and browser type, page tracking data, traffic data, location data, blogs and other communication data coming in through chat bots. Professional details, employment details including title/designation/role, company name, location and contact details coming through social networking sites, client referrals, publicly available sources and purchased contact lists.
Cookies	Cookies and related geolocation data as per the Cookie policy described below.
Employment, recruitment and related data (for employees, consultants, contractors)	Name, Company, Email address and Phone number.
Sensitive personal data (Special category of personal data)	We may collect certain types of sensitive personal data such as health related data, medical information about individuals and family members only when permitted by local law and required for Mediclaim or medical insurance purposes. Other sensitive information such as biometric information or facial recognition might be used for authentication and/or surveillance purposes. Data captured in audio or video formats - This category includes personal data coming in through pictures, audio/video footage captured and recorded on CCTV cameras or surveillance monitoring systems and visitor management system. Sensitive personal data includes unique national

	identification number, social security number, family information including marital/partnership status, ethnicity, beneficiary, parents, children (minor), dependents, health records (including disability) and related medical insurance information, emergency contact information, current and permanent residential address details. Information about education and employment history, background verification details including criminal convictions and offences. These details are required to comply with legal obligations and to abide to our Code Of Business Conduct & Ethics (COBC). Immigration related data including citizenship, passport data, residency or work permit details. Payroll, taxation and related banking account data for processing paychecks and payments to vendors and other parties. Information coming in from CV/resumes submitted through online portals, referrals, walk-ins, and emails including the sensitive personal information coming along with it. Recruitment related information coming from third-party recruitment vendors, placement firms or job website or job fairs.
Employment, recruitment and related data (for employees, consultants, contractors)	Name, Company, Email address and Phone number.
Audiovisual content	Images/audio/footage captured or recorded on CCTV or other video systems when visiting Cigniti office(s) or captured in the course of recruitment events or video interviews or during any other virtual and live events (including recordings during virtual workshops or similar events).

If you provide us with personal information on behalf of another data subject (example – referral candidate, visiting cards or email addresses in marketing events, purchased databases) you would be considered responsible for ensuring that you have the data subject's consent for sharing the information with us.

We are also committed to protect the privacy of children aged 13 years or under (The UK has set this limit at age 13, but other Member States have set different age limits).

Where point (a) of Article 6(1) applies (of the EU), in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

In case you belong to this category, kindly get your parent/guardian's consent/written permission for sharing any personal information with us. Cigniti will not be liable for any unsolicited information provided by you. You consent to us using such information as per our privacy policy.

Please refer the table below for the purposes related to your personal data and the legal basis –

Purpose	Legal basis
Marketing, Sales and lead generation (including B2B marketing)	Legitimate interest for the proper administration of our website, business growth and communications with users/prospects
Providing content and information through website and other marketing events	Consent. Submitting consent through 'Contact Us' forms, emails or through website (example - "I agree", "By continuing to use this website, you agree to our cookie & privacy policy") shall be considered as your agreement to collect and process the Personal Information for the stated purpose
Contractual relationship	Necessary for the performance of a contract to which the data subject is a party
Managing business operations	Legitimate interest for the proper administration and business growth
Complying with any legal obligation, or to enforce or apply our terms of use; or to protect the rights, property, or safety of Cigniti, our clients, or others	Legal obligation for the protection and assertion of our legal rights, your legal rights and the legal rights of others involved. We may process any of your personal data identified in this policy where necessary for the legal purposes such as Personal data collected under UKEU laws such as taxation, disclosure of employee salary details to HMRC (Her Majesty's Revenue and Customs) establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure
Social Media information (processing information found on publicly available sources, social media, networking site, analytics, cookies, stakeholder needs and sentiments)	Legitimate interest for the proper administration and business growth
All the activities related to recruitment/staffing (sourcing profiles, scheduling and conducting online/offline interviews, managing candidate databases and activities managed through Applicant Tracking System)	Legitimate interest for ensuring that Cigniti recruits suitable employees
Communication with data subjects	Legitimate interest for ensuring that Cigniti effectively communicates with data subjects within and outside the organization

All activities related to employment (onboarding, background verification, employment stint, payroll/benefits, insurance and employee exit)	Legitimate interest for the proper administration and employee benefits
Operating and managing our business operations including provision of our services to our clients and their employees/contractors/customers. For instance, collecting their data as part of surveys, data analytics, Marketing research or other purposes.	Legitimate interest for the proper administration and business growth

As per GDPR Article 6(1)(f) - Processing shall be lawful only if and to the extent that at least one of the following applies:
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third-party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
While we consider legitimate interests as reasonable grounds to process your personal information, we also ensure that these legitimate interests are not overridden by your interests and rights or freedoms you have in relation to the processing activities.
Where mandated by law, we will obtain your prior consent for processing your personal information for the purposes mentioned above based. Submitting consent through forms, emails or through website (example - "I agree", "By continuing to use this website, you agree to our cookie & privacy policy") shall be considered as your agreement to collect and process the Personal Information for the stated purpose.
In the event of a medical emergency or authorized by law, we may use your personal information considering the following lawfulness of processing as per GDPR Article 6(1)(d) and 6(1)(e) -

- 6(1)(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person
- 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

We do not generally seek to collect or process sensitive personal data also known as special categories (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) through this site. In the limited cases where we may seek to collect such data, we will do this in accordance with local data privacy law requirements.

Special category or sensitive personal data: Where the information we process is special category data, for example our health data, the additional bases for processing that we rely on are:

- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.

» Article 9(2)(j) for archiving purposes in the public interest.

4.0 What do we do with the information collected?

Cigniti requires this information to better understand the needs that you may have in terms of the services we offer and provide you with the better experience and services. We may also use this information for:

» Internal records for correspondence.

» Providing you with information you request, process online requests (job applications, resources) and for other purposes.

» Improve our service offerings and personalize your experience.

» Periodically sending promotional emails about new service offerings, webinars, technology events or any other information which we think you may find interesting using the email address which you have provided.

» Send information to you, including marketing communications relating to our business, which we think may be of interest to you by post, email, or other means.

» To send commercial e-mail to individuals or other companies with whom we want to develop or maintain a business relationship in accordance with applicable marketing laws.

» Contacting you for collection of feedback/surveys.

» Collected information is used to update, maintain and track the marketing/lead generation efforts in a Customer Relationship Management (CRM) tool/database.

» Any postings, comments or other content that you may post on our website or social media platforms.

» We may transfer personal data to our contracted service providers and advisors who may be located in other countries. Adequate data protection is provided before any such data transfers are made.

» Disclosing your personal data to third parties in the event that we sell or liquidate any part of our business or assets.

» We may share your personal data (including special category of personal data) with third parties for a specific purpose (example – prospecting, recruitment, background verification, insurance). Any personal data processing conducted by an external agent or entity (third-party service provider) on our behalf shall be evidenced by a valid written contract between the involved parties. Such contract shall specifically set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, the obligations and rights of the company.

» International transfers of personal data may happen to countries outside the European Economic Area (“EEA”). Cigniti has global presence in other geographies outside the headquarter in Hyderabad, India. Please refer the list of our global office locations at – https://www.cigniti.com/offices-locations/. Transfers to any of our global offices will be protected by appropriate safeguards included in our Terms of Contract for data processing agreed between Cigniti and the other parties. This transfer or a set of transfers of personal data to a third country or an international organization shall take place when the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of

pre-contractual measures taken at the data subject's request. During this process UK/EU employee data also gets transferred or processed as part of legitimate interest to grow our business.

» Cigniti's formal compliance to ISO 27001 (Information Security Management Systems), Cyber Essentials and System and Organization Controls (SOC) ensure the adequacy of appropriate technical and organizational safeguards.

» Cigniti uses and complies with the UK and European Commission-approved standard contractual clauses ("SCCs") for the transfer of Personal Data from the EU/EEA to the United States or other countries that do not have equivalent privacy and data protection laws. We are responsible for processing such Personal Data we receive under the SCCs and for any subsequent onward transfer to a third-party who provides services to us and is acting as a representative on our behalf.

5.0 How secure is the information collected?

Cigniti is committed to ensuring that your personal information is secure. In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online. Cigniti is certified with ISO 27001 (Information Security Management System) demonstrating formal compliance to protecting confidentiality, integrity and availability of the information collected, processed and stored. We also have a formal compliance towards System and Organization Controls (SOC) for Service Organizations - internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service. Cigniti is also certified with Cyber Essentials Plus – a Government-backed, industry-supported certification and run by National Cyber Security Centre (NCSC), UK. Cyber Essentials Plus is the highest level of certification offered under the Cyber Essentials scheme. It is a more rigorous test of company's cyber security systems where external cyber security experts carry out vulnerability tests to make sure that the company is protected against basic hacking and phishing attacks.
The IT team shall continuously develop and evaluate the Company's security policy with respect to the processing of personal data. We strive to protect your information from unauthorized access, alteration, disclosure or destruction and have some key information security and physical security policies in place to safeguard the information. Some of the examples are – encryptions, physical and logical access control, user authentication, secure login using One Time Password (OTP), firewalls and latest antivirus and likewise.

Regarding your use of our websites it should be noted that the open nature of the Internet is such that information and personal data may flow over networks connecting you to our systems without security measures in some cases and may be accessed and used by people other than those for whom the data is intended. You acknowledge that, Cigniti can't prevent the use (or misuse) of such personal data by others.

In case you follow a link to any of the sites which may be arising out of Cigniti's website, please note that these sites have their own privacy policies and that we do not accept any responsibility or liability for these policies or sites. Please check these policies before you submit any personal data to these sites.

6.0 For how long do we retain the data?

We will retain your personal data only for as long as is necessary. Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. If you have an association with us, we will only keep the data while your association is active or for as long

as needed to provide services to you and, as further needed for us to comply with our legal and contractual obligations.
If you have elected to receive marketing communications from us, we retain information about your marketing preferences for a reasonable period of time from the date you last expressed interest or received our content or services. We would also retain information derived from cookies and other tracking technologies for a reasonable period from the date such information was created/received. When the personal data that has been collected is no longer required, Cigniti shall destroy or delete it in a secure manner in accordance with our information security policies and/or as per the official contract made with the other party.
Compelled Disclosure – Cigniti reserves the right to use or disclose the Personal Data we collect if required by law or if we reasonably believe that use or disclosure is necessary to protect our rights, employees, protect your safety or the safety of others, investigate fraud, or comply with a law, court order, or legal process.

7.0 How we use cookies? Cookie policy.

Cigniti respects data privacy and adopts best practice in compliance with applicable privacy law and regulations, including the UK DPA 2018 and EU General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA"). A cookie is a packet of information sent by a server to a World Wide Web browser and then sent back by the browser each time it accesses that server (source: Wikipedia). Cookies are text files containing small amounts of information which are downloaded to your computer or mobile device when you visit any website and allow the website to recognize your device. Cookies are used for authentication, tracking, and maintaining user-specific information and often contain a unique and anonymous identifier. Most web browsers automatically accept cookies, but you can change the settings in your browser to allow you to accept or decline cookies depending upon your preferences.

We analyze your IP and browser information to determine what is most effective about our website, to help us identify ways to improve it and make it more effective. Cigniti's website does not usually refer to any other external website. In case where there is a reference to other website(s), Cigniti's privacy policy does not apply to those websites. You are requested to read the privacy policy of these websites to gain more information.

By using our website, you agree that we can place cookies and other similar technologies on your device (including mobile devices) as explained in this Cookies policy. By continuing to use your mobile device to access this website, you agree that the following information may be collected: your unique device identifier, mobile device IP address, information about your device's operating system, mobile carrier details and your location related information (to the extent permissible under applicable law).

- **Why do we use cookies?** – To ensure a better experience. Cookies do a lot of different things, such as navigating between different pages efficiently, remembering user preferences and helping us to ensure that content that is seen is more relevant to you and your interests.
- **How do we use cookies –** We use a Customer Relationship Management (CRM) platform to manage and track or 'do not track' cookies.
- **Do we use cookies for marketing and analytics? –** Yes. Cigniti, based on the requirement, may use information collected from our cookies to identify user behavior and to serve content and offers based on your profile, and for the other related purposes. Some of the cookies we use don't collect information that identifies a visitor. For example - Performance cookies (refer below) and Targeting cookies (refer below) where you are not a registered user. In other cases, we can

associate cookie information with an identifiable individual. For example – If we send you a targeted email which includes web beacons, cookies or similar technologies we will know whether you open, read, or delete the message; and when you click a link in a marketing e-mail you receive from us, we will also use a cookie to log what pages you view and what content you download from our websites, even if you are not registered at or signed into our site.

» **Type of cookies used –**

  - Cigniti also uses "Session" cookies which are temporary and once you close the browser window, they are deleted from your device.
  - Along with this Cigniti also uses "Persistent" cookies which remain on your device for a longer period and are used by the website to recognize your device when you return.
  - Strictly Necessary cookies – These cookies are essential in order to enable you to navigate around the site and use its features. Without these, services you have asked for cannot be provided and may result into a meagre user experience.
  - Functionality cookies – These cookies allow a site to remember choices you make (such as your username or the region you are in) and provide more enhanced, personal features. These cookies cannot track your browsing activity on other websites. They don't gather any information about you that could be used for advertising or remembering where you've been on the Internet outside our site.
  - Performance cookies – These cookies collect information about your visit and use of this website, for instance which pages you visit the most often, and if you get error messages from web pages. These cookies don't collect information that identifies a visitor. All information these cookies collect is anonymous and is only used to improve how this website works.
  - Targeting cookies – These cookies are used to deliver content more relevant to you and your interests; and limit the number of times you see the same content; and also, to help measure the effectiveness of the advertising campaign, if any; and understand users' behavior. They are usually placed on behalf of advertising networks with the site operator's permission. They remember that you have visited a site and quite often they will be linked to site functionality provided by the other organization. Cigniti does not use third-party advertising on our site, so we do not use these Targeting cookies for advertising but we use them for gathering analytics and intelligence about the site.

» **Do we analyze personal data? –** We may. Cigniti, based on the requirement and as part of Social Engineering, may combine data from publicly available sources, and from our e-mail, website, and personal interactions with you (this includes information collected across our different sources). We combine this data to better assess your experience, to better offer and sell relevant goods and/or services and to perform the other activities described throughout our privacy policy. The legal basis for this processing and analysis is our legitimate interest for the proper administration and business growth.

» **Do we use cookies from any third parties?** – Some cookies we use are from third-party companies, such as Google Analytics, LinkedIn Analytics and through the Customer Relationship Management (CRM) tool to provide us with web analytics and intelligence about our sites. These companies use programming code to collect information about your interaction with our sites, such as the pages you visit, the links you click on and how long you are on our sites. This code is

only active while you are active on our website. For more information on how these companies collect and use information on our behalf, please refer to their respective privacy policies. Cigniti may use non-tracking cookie technologies such as web beacons (including conversion pixels) or other technologies for similar purposes as above and we may include these on our sites, in marketing e-mail messages or our newsletter, to determine whether messages have been opened and links clicked on. Web beacons do not place information on your device, but they may work in conjunction with cookies to monitor website activity. From time to time, we may receive Personal Data about you from third-party sources including partners with which we engage in joint marketing activities.

» **Do we allow not to use cookies? –** Possible to an extent. By using Cigniti's website you agree that we can place cookies on your device including mobile device. If you want to remove existing cookies from your device you can do this using your browser options. If you want to block future cookies being placed on your device you can change your browser settings to do this. Please bear in mind that deleting and blocking cookies will have an impact on your user experience as parts of the site may no longer work or take more time than usual to load the required contents. Unless you have adjusted your browser settings to block cookies, our system will issue cookies as soon as you visit our site or click on a link in a targeted email that we have sent you, even if you have previously deleted our cookies.

» **GDPR and Your EU Privacy Rights –** The General Data Protection Regulation ("GDPR"), (Regulation (EU) 2016/679) created a few new rights for European Union residents and strengthened some existing data protection rights. To the extent that any cookie placed by Cigniti or a third-party, as described above, can uniquely identify a device, or the person using that device, under GDPR, this falls under Personal Data. Hence, the Privacy Policy and the 'Visitors from the EU/EEA' section may also apply to any such Personal Data collected from its Users.

» **CCPA and Your California Privacy Rights** – Similarly, the California Consumer Privacy Act ("CCPA") created a few new rights for California consumers with for additional data protection. To the extent that any cookie placed by Cigniti or a third-party, as described above, can uniquely identify a device, or the person using that device, under CCPA, this may be considered Personal Data. Hence, the Privacy Policy and the 'Privacy statement for California residents' section may also apply to any such Personal Data collected from its Users.

» **Changes to Cookie Policy** – Cigniti reserves the right to amend/update this Cookie Policy from time to time, as need be. We will notify about such changes on the website, but you are also required to check the website periodically to review the current policy.

8.0 How can you control the information provided? Your rights.

We would like to make sure you are fully aware about the all the data protection rights. Every data subject is entitled (in the circumstances and under the conditions, and subject to the defined exceptions, as set out in applicable law) to following rights for individuals –

» The right to be informed - where personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards.

- The right of access - You have the right to request us for copies of your personal data that we may hold. We may ask you to confirm the identity and/or charge you a small fee for this service.

- The right to rectification - You have the right to request us to correct any information that you believe is inaccurate or incomplete.

- The right to erasure ('right to be forgotten') - You have the right to request us to erase your personal data, under certain conditions as defined by the GDPR.

- The right to restriction of processing - You have the right to request us to restrict the processing of your personal data, under certain conditions as defined by the GDPR.

- The right to data portability - You have the right to request us that we transfer the data that we have collected to another organization, or directly to you, under certain conditions as defined by GDPR.

- The right to object - You have the right to object to our processing of your personal data, under certain conditions as defined by GDPR.

- Rights in relation to automated individual decision-making, including profiling – You have the right not to be subject to a decision based solely on automated processing, including profiling.

- The right to withdraw consent – You shall have the right to withdraw your consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, you shall be informed thereof. It shall be as easy to withdraw consent as to give it.

- The right to lodge a complaint – You shall have the right to lodge a complaint with supervisory authority in case you believe that your data privacy rights have been violated. You are encouraged to seek resolution of complaint from us while still having the right at all times to register a complaint directly with the relevant supervisory authority or to make a claim against Cigniti with a competent court (either in the country where you live or work or where the privacy rights have been violated).

    - You may use the following link to raise a complaint with the ICO (Information Commissioner's Office) - the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals) https://ico.org.uk/make-a-complaint/

    - **Contact details of ICO, UK are as follows –**
      Information Commissioner's Office,
      Wycliffe House, Water Lane, Wilmslow
      Cheshire, SK9 5AF
      Telephone: +44 303 123 1113
      Fax: +44 1625 524510

We shall provide information on action taken on a request under GDPR Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be

extended by two further months where necessary, taking into account the complexity and number of the requests. We shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. Certain data subject rights are unavailable for certain types of lawful basis. For example - Contract and Consent basis does not have right to object (but you still have the right to withdraw consent) and Legitimate Interest does not have right to portability.

As a user, you may choose to restrict the information that we have collected or the way in which the same would be used, in the following ways:

- Whenever you are providing personal information through, ensure that the explicit consent is checked. In case you do not want to provide the consent, personal information shall not be collected in the first place.
- Contact us (info@cigniti.com) if you wish to update your personal information.
- In case you have previously subscribed or agreed to us for sharing your personal information for direct marketing purposes, you may opt out the same anytime by writing an email to unsubscribe@cigniti.com. You may also unsubscribe from our marketing communications by clicking on the "unsubscribe" link located on the bottom of our e-mails.
- We do not use automated decision making (including profiling) when processing your data.

Cigniti shall not sell, distribute or lease your personal information to third-parties unless we have your explicit consent to do so or are required by law to do so.

Cigniti may transfer personal information if it acquires, or is acquired by or merged with, another company. In this event, we will notify you before your personal information is migrated/ported to the new organization or comes under the jurisdiction of another privacy policy.

For more details on these rights, you may refer the Information Commissioners Office (ICO) website or EU text here.

9.0 Privacy statement for California residents

We are not directly in the business of selling personal information, but there may be limited circumstances where we share personal information in a manner that may be a "sale" as defined under California law. The following definition are referred as per CCPA 1798.140 –

- (o) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.
- (o) (2) "Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.
- (o) (3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

» (t) (1) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third-party for monetary or other valuable consideration.

This privacy notice enables you to request us to refrain from selling your personal information in accordance with California law. As a California resident, you have specific privacy rights under the California Consumer Privacy Act (CCPA). You may opt-out from any selling (as defined in “CCPA”) of your personal information by contacting us for ‘Do Not Sell My Personal Information (CCPA)’ via an email to unsubscribe@cigniti.com. Please note that this right is limited to only California residents and is not absolute. We reserve the necessary rights to question, ask to prove the identity and deny the request in the event of any suspicious or fraudulent opt-out requests.

Note about the California Privacy Rights Act (CPRA) - In November 2020, California voters approved Proposition 24, the California Privacy Rights Act (CPRA), which sought to amend the CCPA. Some of the Attorney General’s responsibilities under the CCPA will transition over to the California Privacy Protection Agency created under CPRA. However, the Attorney General will retain the authority to go to court to enforce CPRA. Enforcement of CPRA will begin in 2023. A copy of the approved regulations can be found here.

10.0 Visitors from the EU/EEA

Visitors to our website(s) from the EU/EEA have additional rights under the General Data Protection Regulation (GDPR).

Legal basis for processing Personal Data (EU/EEA visitors only) - If you are a visitor to our website(s) and are located in the European Union (“EU”)/European Economic Area (“EEA”), Cigniti’s legal basis for collecting and using the Personal Data described in this policy will depend on the Personal Data concerned and the specific context in which we collect it. However, we will normally collect Personal Data from you only where we have your consent to do so (example – contact us form on the website), where we need the Personal Data to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms.

International Transfer of Personal Data – Cigniti complies with the European Commission-approved standard contractual clauses (“SCCs”) for the transfer of Personal Data from the EU/EEA to the United States or other countries that do not have equivalent privacy and data protection laws. We are responsible for processing such Personal Data we receive under the SCCs and for any subsequent onward transfer to a third-party who provides services to us and is acting as a representative on our behalf.

Updates to your Personal Data – You can request access, correction, updates, or deletion of your Personal Data. You can object to processing of your personal data, ask us to restrict processing of your personal data or request portability of your Personal data. If we have collected and process your Personal Data with consent, then you may withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your Personal Data conducted in reliance on lawful processing grounds other than consent.

» Contact us (info@cigniti.com) if you wish to update your personal information.

» In case you have previously subscribed or agreed to us for sharing your personal information for direct marketing purposes, you may opt out the same anytime by writing an email to unsubscribe@cigniti.com.

» To exercise any rights, for questions, concerns, or complaints or if you wish to contact our Data Protection Officer (DPO), you may also write to privacy@cigniti.com.

11.0 Contact us

If you have any queries or complaints regarding this privacy policy or in case you would like to contact our Data Protection Officer (DPO), please feel free to write an email to privacy@cigniti.com or via post at the below address –

India Address: Cigniti Technologies Limited
6th Floor, ORION Block, "The V" (Ascendas),
Plot No#17 Software Units Layout, Madhapur,
Hyderabad, Telangana, India – 500081

UK Address: Cigniti Technologies (UK) Limited
WeWork, 8 Devonshire Square
London, EC2M 4PL
Phone: +44 (0) 203 865 6044

Alternatively, you may visit our website - https://www.cigniti.com/contact-us/.

12.0 Employee Privacy Notice

12.1 Privacy statement

At Cigniti Technologies Ltd. (hereinafter referred as “Cigniti” or “company”), we are committed to safeguarding the privacy of our employees, contractors and consultants. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). References to the EU GDPR are also considered in the same privacy notice. This notice applies to current and former employees, consultants and contractors. It does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

12.2 Personal data we collect

We may collect, store, and use the following categories of personal information about you (including but not limited to) –

- Personal contact details such as name, title, addresses, telephone/mobile numbers, and personal email addresses;
- Day and Date of birth;
- Gender;
- Marital status and dependants;
- Next of kin and emergency contact information;
- National Identity number or copy of driving licence, passport, birth and marriage certificates, as submitted for identification purpose;
- Bank account details, payroll records and tax status information;
- Job title;
- Salary, annual leave, pension and benefits information;
- Date of joining and, if different, the date of your continuous employment;
- Last working day (Date of exit) and date and your reason for leaving;
- Location of employment or workplace;
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process);
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships);
- Compensation history;
- Work performance information;
- Disciplinary and grievance information;
- Information about your use of our information and communications systems;
- CCTV images used to monitor access to work premises/buildings etc;

- Photographs or videos of events;
- Passport details (including number, expiry date and place of issue);
- Details about your company assets such as desktop/laptop/mobile, etc.
- Username, Employee ID and title;
- Personal data related to the online training platform of the company (including full name; corporate email address; module undertaken; completion status; assessment status; date undertaken & performance analytics);
- Electronic signatures, if any
- Responses to employee surveys (only if this data is not anonymised)

We may also collect, store and use the following more sensitive types of personal data (including but not limited to) –

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions for equality and diversity monitoring purposes;
- Trade union membership;
- Information about your health, including any medical condition, health and sickness records etc.;
- Details of any absences (other than routine leaves and holidays) from work including time on statutory parental leave and sick leave;
- Information about criminal convictions and offences;
- Biometric data, including fingerprint authorisation to access IT systems, wherever applicable
- Data collected through Visitor Management System for guests, clients and employees (in case ID card is forgot or lost) wherever applicable.

12.3 Why we wish to hold it

We collect personal information about employees, consultants and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers, credit reference agencies or background verification agencies.

We will collect additional personal information in the course of job-related activities throughout the period that you work for us and will only use your personal information when the law allows us to. The lawful basis for processing your personal data depends on the processing activity and we rely on the following lawful basis for processing your personal data under the UK Data Protection Act 2018/UK GDPR and EU GDPR:

- Article 6(1)(a) where we have your consent;
- Article 6(1)(b) which relates to processing necessary for the performance of a contract;
- Article 6(1)(c) so we can comply with our legal obligations as your employer;

- Article 6(1)(d) in order to protect your vital interests or those of another person;
- Article 6(1)(e) for the performance of our public task;
- Article 6(1)(f) for the purposes of our legitimate interest. (In accordance with best practice a Legitimate Interests Assessment (LIA) will always be conducted when this lawful basis is used)

Special category or sensitive personal data: Where the information we process is special category data, for example our health data, the additional bases for processing that we rely on are:

- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.
- Article 9(2)(j) for archiving purposes in the public interest

12.4 What we do with the information

Information related to your employment, conduct, performance and training shall be used for:

- Deciding about your appointment;
- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK/EU/USA or other countries where we operate or may operate in the future;
- Renumeration and, if you are an employee or deemed employee for tax purposes, deducting tax and insurance contributions;
- Providing annual leave allotment including maternity, paternity leaves and associated pay;
- Pension and other flexi benefits as applicable;
- Assessing your work performance through appraisal;
- Learning and development needs required for your role;
- Administering the contract, we have entered into with you;
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;
- Ascertaining your fitness to work, managing sickness absence and keeping in touch during an absence, including occupation health & safety (also known as Workplace Safety and Health);
- Dealing with any employer/employee related disputes;
- Gathering evidence for grievances and respect at work matters and investigations to which you may be a party or witness;
- Whistleblowing concerns raised by you, or to which you may be a party or witness;

- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Disciplinary processes/procedures and documentation related to any investigations, hearings and warnings/penalties issued;
- Complying with Legal obligations and regulations, including but not limited to, health and safety obligations, data privacy regulations (as applicable) and information security obligations with clients/prospects;
- Meeting the training and development needs required for your role;
- Maintaining visitor/client/guest and employee records in Visitor Management System to enable smooth and secure entry and exit in the premises;
- Sending internal communication to all employees for various purposes such as policy awareness, birthdays and work anniversary wishes, messages/announcements from leaders, internal departments, etc.

Additional scenarios where we may process your personal information (including but not limited to) -

- Business management and planning, including accounting and auditing;
- To prevent fraud;
- To make travel arrangements, via a third-party data processor, with organisations who provide travel services;
- To monitor your use of our information and communication systems to ensure compliance with our IT policies;
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- To conduct data analytics studies to review and better understand employee retention and attrition rates;
- Equal opportunities monitoring;
- To protect all associates from the health risks of working in the office provided environment, working from home and working with devices such as desktops, laptops, tablets and smartphones;
- Following the pandemic remote working and shut down, we would like to identify possible sites which would support our employees working in a more flexible way – such as existing premises and working from home. To determine which locations might be appropriate for consideration, it is necessary for us to understand the areas where our employees currently live, compared to our existing offices;
- To comply with instructions and directions from Government, including requirements to increase openness and transparency in organisations performing public tasks and provide public assurance regarding use of taxpayers' money.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. If you fail to provide certain information when requested, we may

not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our associates).

12.5 How long it will be kept for

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available with the respective HR Business Partners and in the Controller Documentation too.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. However, your information may be held beyond the specified retention periods where there is the potential for it to fall under the remit of ongoing government independent inquiries.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we will use such information without further notice to you. Once you are no longer an employee, consultant or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy as defined in ISMS OR according to the applicable laws and regulations for our Head Office.

12.6 Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

12.7 Reasons we may or may not need your consent

We do not need your consent if we use special category personal data in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Regarding information about criminal convictions, we will only collect information about the same if it is appropriate given the nature of the role and where we are legally able to do so. The information will be collected as part of the recruitment process or we may be notified directly by yourself in the course of

you working for us. Cigniti does not currently make any automated decisions about its employees, consultants, contractors or visitors/guests.

12.8 How we protect your personal data

We'll use our existing physical and technical security measures associated with storage, retention and transfer for all electronic data. Such controls have restricted and password access in place. Where data is stored on papers, it'll be kept in a secured place with access to only authorized personnel. Personal Data stored in electronic media shall be encrypted (only after authorization from IT team) when need be. This data shall be protected from unauthorized access, accidental loss, and other attempts at data stealing. We have put in place procedures to deal with any suspected data security or personal data breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. We may also transfer your personal data outside of the EU/EEA. If this is the case you can expect a similar degree of protection in respect of your personal information.

12.9 Data sharing

We will in some circumstances have to share your data with third parties, including third-party service providers (such as insurance, background verification, etc.) and other Civil Service bodies. We require third parties to respect the security of your data and to treat it in accordance with contract with them and the law as well. All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions. We will in some circumstances transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

12.10 Your data protection rights

As a Data Subject, legislation provides and strengthens the rights of individuals, which includes -

- The right to be informed (which this notice fulfils);
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

For more details on these rights, you may refer the Information Commissioners Office (ICO) website (The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals); Data protection in the EU here and EU text here.

13.0 Recruitment Privacy Notice

13.1 Privacy statement

At Cigniti Technologies Ltd. (hereinafter referred as “Cigniti” or “company”), we are committed to safeguarding the privacy of our clients, employees and job applicants to the extent possible. As a company, for the purpose of your candidature and interview, we need to collect and hold data about you to enable us to process your job application and potential employment subsequently (purpose of Personal Data collection and processing). This privacy notice is primarily aimed at new job applicants (full time/contractor/consultants). This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA). References to the EU GDPR are also considered in the same privacy notice. The General Data Protection Regulation (GDPR) places a further obligation for employers to tell their job applicants in more detail why we collect your data, what we do with it, and how long we expect to retain it.

13.2 Personal data we collect

Following is the sample list of the data we wish to obtain and hold (including but not limited to the following) –

- Recruitment data –
  - First name, last name, job title, data of birth, passport and visa data, Government ID, social security number, if applicable, residential address, personal email and telephone number, emergency contact number, if applicable.
  - Previous employers, contracts of employment, types of job held at other companies, previous salaries, skills and qualifications obtained.
  - Application form (manual or through tool), references, records of absence, and records required for background verification.
- Ethnic monitoring data - Equality of Opportunity (Ethnicity, Disability details) under Special Categories

We may get the above information about you directly or indirectly (when you apply online, send email for knowing job opportunities, through referrals, third-party recruiting agencies or public sources such as professional networking platforms). We would like your consent to hold personal and special data about you in order that we can process your employment application coming from the website/portal https://www.cigniti.com/cigniti-careers/. We will never process your data where these interests are overridden by your own interests.

13.3 Why we wish to hold it

Cigniti has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. It is in our legitimate interests to decide whether to appoint you to the role since it would be beneficial to our business to appoint a suitable candidate to that role.

Data related to ethnic monitoring (Special category of Personal Data) will help us to understand the ethnic make-up of our workforce and job applicants and it allows us to inform our recruitment team if we believe we do not have the correct diversity.

13.4 How we use personal data

Your Personal Data will be used to process your employment application by our recruiter(s). We do use automated application/CV scanning and tracking software (an applicant tracking system (ATS) is a software application that enables the electronic handling of recruitment needs) to search for key essential job criteria (e.g. relevant qualifications or skills). If you would like your application to be examined by one of our recruiters only, please make this clear in your application or interaction with the recruiter.

13.5 How long it will be kept for

In case of successful recruitment (where a job offer is made, the candidate accepts the same and joins the company) candidate's data will be held under the company's Data Privacy Framework and associated polices, valid as long as the candidate is employed by the company. More details about such policies will be made available upon the day of joining or a couple of days prior to the date of joining. A comprehensive GDPR consent form (for employees) may also be issues based on the candidate's details. Unsuccessful candidate's data (candidates not joining post accepting offer or candidates rejected during the screening or interview process) will be held of a period of 12 months where upon it will be confidentially destroyed.

13.6 Reasons we may share personal data

We may share your Personal Data with our Human Resources (HR) and other internal enabling function(s) to aid our selection process. We may also share your Personal Data in the following cases –

- There is an issue that puts the safety of our employees/recruiters at risk
- We need to liaise with other agencies or third parties like background verification – we or the associated vendor for such activities will seek consent as necessary before doing this
- Law enforcement and government bodies where we are legally required to do so, including for - the prevention or detection of crime and/or fraud, criminal background verification, the apprehension or prosecution of offenders, where the disclosure is required to satisfy our compliance and/or legal obligations

In limited and necessary circumstances, your information may be transferred outside of the European Economic Area (EEA) to comply with our legal or contractual requirements. We have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we may transfer in this case.

13.7 How we protect your personal data

We'll use our existing physical and technical security measures associated with storage, retention and transfer for all electronic data. Such controls have restricted and password access in place. Where data is stored on papers, it'll be kept in a secured place with access to only authorized personnel. Personal

Data stored in electronic media shall be encrypted (only after authorization from IT team) when need be. This data shall be protected from unauthorized access, accidental loss, and other attempts at data stealing.

13.8 Your rights - How to access & control your personal data

As a Data Subject, you may exercise your right to make a 'Subject Access Request' (SAR) to gain more information or to restrict the information that we have collected or the way in which the same would be used. The company shall analyze your request and get back to you on the further actions. In case you would like to withdraw, erase, update/modify the personal information that we hold about you, please inform us by writing an email to privacy@cigniti.com and we shall do the needful. While responding to SAR we –

- may ask the Data Subject or the individual requesting on behalf of the Data Subject to provide 2 forms of identification
- may contact the requester via phone to confirm whether the request was made and/or to seek additional details and will provide information free of charge
- will respond without delay and within 1 (calendar) month of receipt of the request
- may get back to the requestor for time extension in case of complex or multiple requests and will comply to such requests within maximum of 3 (calendar) months
- may refuse to act on SAR if the same is found to be baseless/excessive/ repetitive, or charge a reasonable fee for the related administrative cost

As a Data Subject, legislation provides and strengthens the rights of individuals, which includes -

- The right to be informed (which this notice fulfils);
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

For more details on these rights, you may refer the Information Commissioners Office (ICO) website or EU text here.

14.0 Updates to privacy policy and notices

Cigniti may change this policy from time to time and the latest copy shall be made available at https://www.cigniti.com/privacy-policy/. Users of the policy are requested to occasionally visit the link provided for latest updates to ensure that they make themselves aware of any changes. You continue to agree with the updated privacy policy till you explicitly convey us about your disagreement.
This policy was last updated on 31-Oct-2022.