

EMPLOYEE PRIVACY NOTICE



Table of Contents

| | |
|---|----|
| 1. Scope & Applicability..... | 3 |
| 2. Purpose..... | 3 |
| 3. Data Protection Office..... | 3 |
| 3.1. Contact Us..... | 3 |
| 4. Cyber Security Data Protection..... | 4 |
| 4.1. Login and Passwords (Long, Unique, Complex)..... | 4 |
| 4.2. Updates Patches | 4 |
| 4.3. Don't Overshare, Click, or Download | 4 |
| 4.4. Recover from being Hacked..... | 5 |
| 5. Data Subject Rights | 5 |
| 5.1. Right to Request Access | 5 |
| 5.2. Data portability..... | 6 |
| 5.3. Right to restriction of processing | 6 |
| 5.4. Right to withdraw consent..... | 6 |
| 5.5. Right to object to processing justified on legitimate interest grounds | 7 |
| 6. Types of Personal Data..... | 7 |
| 6.1. Categories of Data Processed..... | 8 |
| 7. Collection, Use | 11 |
| 7.1. Collection and Use..... | 11 |
| 8. Sources of Personal Data..... | 11 |
| 8.1. Provided by You..... | 11 |
| 8.2. Recruitment Process..... | 11 |
| 8.3. Leadership..... | 12 |
| 8.4. Third Parties | 12 |
| 8.5. Monitoring Devices..... | 12 |
| 8.6. Disclosure about providing personal data | 12 |
| 9. Data Processing..... | 13 |
| 9.2. Special Categories Processing | 21 |
| 9.3. Criminal Offenses Data Processing..... | 22 |
| 10. Retention of Personal Data..... | 23 |

11. Transfer of Personal Data23

12. Delete Personal Data.....23

13. Disclosure of Personal Data24

14. Children’s Privacy25

15. Notice of Changes25

1. Scope & Applicability

This Employee Cyber Security & Data Privacy Notice ("Notice") principally applies to all CGS Global, CGS Arizona, CGS California, CGS Central, CGS East, CGS Southeast, CGS West, hereinafter may be referred to as "CGS" or "company", employees even after the end of their employment but, where relevant, it also applies to workers, job applicants, interns, agency workers, consultants, clients, and third parties whose information is provided to us in connection with the employment or work relationship (for example emergency contact information, benefits, workers comp, or arbitrators). CGS may use the term employee or employment other than for purposes of this notice, but this does not in any way indicate that the individual is an employee of CGS (for example those who work for or partner with us on a basis other than employment to the extent it is relevant).

This Notice does not form part of any contract of employment and does not confer any contractual right on you or place any contractual obligation on us. We may update or otherwise amend this Notice at any time.

2. Purpose

This Notice sets out the types of information that CGS collects about you, the purposes for which it is collected, the basis on which we process it, and how CGS handles your personal data. It is intended to comply with our obligations to provide you with information about CGS's processing of your personal data under applicable cyber security and privacy laws.

3. Data Protection Office

- a) CGS has a Data Protection Office who is responsible for CGS's compliance with cyber security, privacy, and data protection law.
- b) You may contact CGS's Data Protection Office securely and confidentially at any time if you have general concerns about the processing of your personal data, or any data protection issue.

3.1. Contact Us

You also have certain rights in respect of your personal data, which you can exercise by contacting us using the contact details below.

- **Email:** dpo@cgsglobal.com
- **Website:** www.cgsglobal.com
- **Phone:** (480) 219-9795
- **Mail:**

CGS Global Corporate
Attn: Data Protection Office
14269 N 87th St Suite 201,
Scottsdale, AZ 85260

If you have any questions regarding the processing of your personal data, believe your privacy rights have been violated, or are aware of an unauthorized data disclosure of your CGS data, please contact CGS's Data Protection Office.

4. Cyber Security Data Protection

The protection of Your Personal Data is important to us, and we strive to use commercially reasonable and feasible means to protect Your Personal Data. However, no method of transmission over the Internet, or method of electronic storage is 100% secure and we cannot guarantee its absolute security.

You play an important role in protection Your Personal Data. At a minimum the following leading practices should be followed when accessing Your Personal Data:

4.1. Login and Passwords (Long, Unique, Complex)

- Do not share your username or password
- Use **long** passwords, passwords should be a minimum of 15 characters long.
- Use **unique** passwords for each account, never reuse passwords.
- Use **complex** passwords should be a combination of upper- and lower-case letters, numbers, and special characters.
e.g., MyDog+MyotherDog=4legs (think of as a passphrase).
- Use a password manager (for example managers like; [Keeper](#), [1Password](#), [NordPass](#), [Last Pass](#))
- Use Multifactor Authentication (MFA) when possible.
MFA may include biometrics (think face ID scans or fingerprint access), security keys or apps that send you unique, one-time codes when you want to log on to a sensitive account
- Change password a minimum of annually, and immediately if your account has been compromised (hacked/breached).

See how long it takes to hack your password at: PasswordMonster <https://www.passwordmonster.com/>

4.2. Updates | Patches

Keep all devices, personal computers, smartphones, tablets, current.

- Install latest updates for devices, hardware, operating systems, software, web browsers and apps. It is recommended that you configure your devices to automatically update or notify you when an update is available.
In addition to new features this also provides critical patches to security vulnerabilities or weaknesses.
- Only update your devices from known sources and official app stores
The device, software, or app developer itself should be sending you updates. Pirated, hacked, or unlicensed software can often spread malware, viruses, grant unwanted access, or other cyber security weaknesses to your network.

4.3. Don't Overshare, Click, or Download

EMAIL, IM, SOCIAL NETWORKING, AND WEB BROWSING

Malicious links in email, tweets, texts, posts, social media messages and malicious online advertising (known as malvertising) are a direct way for hackers to scam you, harvest your sensitive information for identity theft, password guessing, grant unwanted access, spread malware or viruses, or create other cyber security havoc to your network.

- Be cautious (*on any device or application*) and do not click on unknown links, pop-up windows, or download anything that comes from a stranger or that you were not expecting. Especially implying urgency or demanding you act immediately.
- It is recommended that you visit the site directly or from your password manager, rather than navigating from a link where possible.
- Do not overshare, providing and posting too much personal or private information. In addition to cyber security risk, you introduce physical risks. (e.g., providing the best time to burglarize your house)
- Avoid utilizing 3rd party apps that may collect, share, or even sell your personal and sensitive information.

4.4. Recover from being Hacked

Once hackers have your personal information it is important that you take action.

1. Call the companies where the fraud occurred

If you believe your CGS account has been compromised and your personal information has been exposed, please report immediately to

CGS Cyber Security
Email: dpo@cgsglobal.com
Phone: (833) 247-2677

2. Place credit freezes on the major credit bureaus, credit freeze, also called a security freeze, makes it less likely that an identity thief could open a new account in your name.

You have the right to place a free credit freeze on your credit report, anytime. It is recommended that you put these in place before you become a victim of identity theft.

3. Place a fraud alert and get your credit reports, may want to sign up for a credit monitoring service
4. Monitor your bank and credit card statements
5. Visit [IdentityTheft.gov](https://www.identitytheft.gov/#/Steps) for more instruction and information.

5. Data Subject Rights

You have a right to access, correct and delete your personal data.

CGS aims to ensure that all personal data we store is correct. You also have a responsibility to ensure that changes in personal circumstances (for example, change of address and bank accounts) are notified to CGS so that we can ensure that your data is up to date.

5.1. Right to Request Access

5.1.1. You have the right to request access to any of your personal data that CGS may hold, and ask us to:

- a) Confirm whether we are processing your personal data;
- b) Give you a copy of that data;
- c) Provide you with other information about your personal data such as what data we have, what we use it for, who we disclose it to, whether we transfer it abroad and how we protect it, how long we

keep it for, what rights you have, how you can make a complaint, where we got your data from and whether we have carried out any automated decision making or profiling.

5.1.2. You have the right to request us to rectify any inaccurate personal data relating to you.

5.1.3. You have the right to request erasure of any irrelevant personal data we hold about you, but only where:

- a) it is no longer needed for the purposes for which it was collected or otherwise processed; or
- b) you have withdrawn your consent (where the data processing was based on consent) and there is no other legal ground for the processing;
- c) following a successful right to object;
- d) it has been processed unlawfully; or
- e) to comply with a legal obligation to which we are subject.

5.1.4. We are not required to comply with your request to erase your personal data if the processing of your personal data is necessary:

- a) for compliance with a legal obligation; or
- b) for the establishment, exercise or defense of legal claims.
- c) There are other certain circumstances in which we are not required to comply with your erasure request, although these two are the most likely circumstances in which we would deny that request.

5.2. Data portability

Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal data is processed by automatic means,

- a) You have the right to receive all such personal data which you have provided to CGS in a structured, commonly used and machine-readable format,
- b) and to request us to transmit it to another controller where this is technically feasible and reasonable.

5.3. Right to restriction of processing

You have the right to restrict our processing of your personal data where:

- a) You contest the accuracy of the personal data until we have taken sufficient steps to correct or verify its accuracy.
- b) The processing is unlawful.
- c) We no longer need personal data for the purposes of the processing.
- d) You have objected to processing justified on legitimate interest grounds pending verification as to whether CGS has compelling legitimate grounds to continue processing (see Data Processing section; or
- e) Personal data is subjected to restriction in this way we will only process it with your consent or for the establishment, exercise or defense of legal claims.

5.4. Right to withdraw consent

- a) Where you have provided us with your consent to process data, you have the right to withdraw such consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- b) In some instances, you can do this yourself by deleting the relevant data from the Workforce system (although note that in this case it may remain in back-ups and linked systems until it is deleted in accordance with our data retention policy).

5.5. Right to object to processing justified on legitimate interest grounds

- a) Where we are relying upon legitimate interests to process data, then you have the right to object to that processing.
 - If you object, we must stop that processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defense of legal claims.
- b) Where we rely upon legitimate interest as a basis for processing, we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.
- c) You also have the right to lodge a complaint with a supervisory authority, in the state or local jurisdiction in which you are employed with CGS, if you consider that the processing of your personal data infringes applicable law.

6. Types of Personal Data

Individual/Data Subject: is a natural person who can be identified, directly or indirectly from personal data.

Personal Data also known as “personal information”: identifiers such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. Personal information can be sensitive or non-sensitive.

Sensitive Personal Data also known as “Personally Identifiable Information (PII)” is personal data that either alone, or when combined with other personal or identifying information can be reasonably used to distinguish, trace, or be linked (directly or indirectly) to a particular consumer or household. Furthermore, if compromised, or breached may result in identity theft, unlawful destruction, loss, alteration, unauthorized disclosure of, unauthorized use of, or access to.

Non-Sensitive Personal Data: does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

- if data elements used to identify the individual are removed the remaining data becomes non-personal information, and privacy and data protection laws generally do not apply

Note: Non-Sensitive Personal Data can become Sensitive Personal Data that when combined with other publicly available information, could be used to identify an individual.

Examples of personal information identifiers include but are not limited to the following:

- name
- signature
- social security number
- physical characteristics or description
- address
- telephone number
- passport number
- driver’s license or state identification card number
- insurance policy number
- education
- employment
- employment history
- bank account number
- credit card number, debit card number, or any other financial information
- medical information or health insurance information

EMPLOYEE PRIVACY NOTICE



CGS Global
CGS ARIZONA | CGS CALIFORNIA | CGS CENTRAL
CGS EAST | CGS SOUTHEAST | CGS WEST

Additionally Personal information may include Protected Classifications like the following

- Race
- Color
- Religion
- sex/gender
- gender identity
- gender expression
- sexual orientation
- marital status
- medical condition
- military or veteran status
- national origin
- ancestry
- disability
- genetic information
- request for family care leave
- request for leave for an employee's own serious health condition
- request for pregnancy disability leave
- retaliation for reporting patient abuse in tax-supported institutions and age

6.1. Categories of Data Processed

The types of personal data which we process will may include, but not limited to, the following:

6.1.1. Personal Details

Name, date of birth, gender, personal contact details, emergency contact/next of kin details, immigration and eligibility to work data and languages spoken.

6.1.2. Basic Work Details

Work contact details (email address and telephone numbers), employee number, photograph, job title, job description, assigned business unit or group, reporting lines, primary work location, working hours and your terms and conditions of employment.

6.1.3. Disciplinary and Grievance Data

Personal data contained in records of allegations, investigations and meeting records and outcomes.

6.1.4. Employee Claims, Complaints and Disclosures Data

Personal data in the subject matter of employment-based litigation and complaints, employee involvement in incident reporting and disclosures.

6.1.5. Equality and Diversity Data

Where permitted under applicable law, data regarding gender, age, race, nationality, religious belief and sexuality (stored anonymously for equal opportunities monitoring purposes).

6.1.6. Health and Safety Data

Personal data contained in your attendance records, medical forms, reports or certificates and records relating to accommodation or adjustments.

6.1.7. Leave Data

Holiday, personal time off, and family-related leave records.

6.1.8. Professional Qualifications, Training, and Development Data

Where applicable, certifications, training records, or other data relating to training and development needs or received.

6.1.9. Payroll and Benefits Data

Details of your pay and benefits package, bank account details, grade, social security number, tax information and third-party benefit recipient information.

6.1.10. Performance Management Data

For example, colleague and manager feedback, appraisals, outputs from talent programs and formal and informal performance management processes.

6.1.11. Recruitment/Selection Data

For example, any personal data contained in your CV, application form, record of interview or interview notes, records of assessments and vetting and verification documentation.

6.1.12. Termination Data

For example, dates and reason for leaving, termination arrangements and payments, exit interviews and references.

6.1.13. Special categories of personal data

- a) To the extent permitted by applicable laws, CGS may also collect and process a limited amount of personal data falling into special categories. Within this category, CGS collects and records information relating to health (including details of accommodations and adjustments) as permitted by applicable laws.
- b) We may also process information relating to memberships such as labor or trade union memberships, only where you provide this to us and as permitted by applicable laws.

6.1.14. Usage Data

- c) Usage Data may be collected automatically when using some of the Services.
- d) Usage Data may include information such as Your Device's Internet Protocol address (e.g., IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.
- e) When You access Services by or through a mobile device, we may collect certain information automatically, including, but not limited to, the type of mobile device You use, your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.
- f) We may also collect information that Your browser sends whenever You use our Services or when You access the Services by or through a mobile device.

6.1.15. Monitoring & Incident Response Data

Where permitted under applicable law, identifiable images contained in CCTV footage, system and building login and access records, keystroke, download and print records, call recordings, and data monitored by Cyber & Physical Security programs, filters, tolls, and devices.

Personal data in audits, risk assessments and incident reports.

6.1.16. Tracking Technologies and Cookies

We may use Cookies and similar tracking technologies to track the activity on Our Service and store certain information.

Tracking technologies that may be used are beacons, tags, and scripts to collect and track information and to improve and analyze Our Service. The technologies We use may include:

6.1.17. Web Beacons.

Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the CGS, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

6.1.18. Cookies or Browser Cookies.

A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, you may not be able to use some parts of our Service. Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.

Cookies can be "Persistent" or "Session" Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser. Learn more about cookies at FTC site: <https://www.ftc.gov/policy-notices/privacy-policy/internet-cookies> .

We may use both Session and Persistent Cookies for the purposes set out below:

6.1.18.1. Necessary / Essential Cookies

a) **Type:** Session Cookies

Administered/Governed by: CGS

Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.

6.1.18.2. Cookies Notice / Notice Acceptance Cookies

b) **Type:** Persistent Cookies

Administered/Governed: CGS

Purpose: These Cookies identify if users have accepted the use of cookies on the Website.

c) **Type:** Persistent/Functionality Cookies

Administered/Governed: CGS

Purpose: These Cookies allow us to remember choices You make when You use the CGS website, such as remembering your login details or language preference. The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

6.1.19. Any other personal data

Which you choose to disclose to CGS personnel during your employment, whether verbally or in written form (for example, emails).

7. Collection, Use

7.1. Collection and Use

- a) CGS collects and uses personal details which you provide as part of the recruitment and onboarding processes, together with additional personal data collected throughout the course of your employment or engagement (for instance, in relation to payroll, timekeeping, workers comp, drug and alcohol screening, performance reviews, disciplinary processes, and participation in voluntary benefits schemes).
- b) The personal data CGS collects is used primarily for the recruitment process, managing the workforce, and complying with contracts of employment. The data may be stored in systems based around the world and may be processed by third-party service providers acting on CGS's behalf.
- c) We need your data in order to commence, perform, terminate your employment and for performing the related contractual or statutory obligations. Without this data, we will not be able to enter into a contract with you or to perform our obligations under such a contract.
- d) It is our policy to strive to protect your data, and comply with U.S. federal, state, and other applicable local laws. This includes due diligence when working with third party partners who may process your data on behalf of CGS.
- e) You also have a critical role in protecting the security of personal data, and you should be careful to whom you disclose personal data, and how you protect your communications and devices.

Please refer to section 3, Security of Personal Data – section for more information about your responsibilities.

8. Sources of Personal Data

8.1. Provided by You

- a) Primarily the personal data we process about you will have been provided by you, either during your application for employment or engagement, the on boarding process, or on an ad hoc basis during the course of your employment or engagement. This will particularly include your personal and basic work details as well as equality and diversity data.

8.2. Recruitment Process

- a) During the recruitment process, we may request references from third parties, and carry out screening and vetting processes using third party sources.
- b) We carry out such screening and vetting processes only to the extent permitted by applicable laws. These may include credit and employment history checks and are set out more fully in [policy].
- c) Credit checks will only be carried out if you are applying for a type of position within CGS which, according to applicable laws, allows us to perform such checks (e.g., if you are applying for a key, sensitive, or management position).

8.3. Leadership

- a) We also receive information which may include your personal data from your line manager (for example, in respect of performance reviews) or, from time to time, from other managers or colleagues (for instance, in the course of conducting an investigation).

8.4. Third Parties

- a) We may also receive personal data about you from other third parties, for example clients, tax authorities, benefit providers, brokers and regulatory bodies to the extent permitted by applicable laws.

8.5. Monitoring Devices

- a) In some circumstances, data may be collected indirectly from monitoring devices or by other means (for example, building and location access control and monitoring systems, telephone logs and recordings and email and Internet access logs), if and to the extent permitted by applicable laws.
 - In these circumstances, the data may be collected by CGS or a third-party provider of the relevant service. This type of data is generally not accessed on a routine basis, but access is possible.
 - Access may occur, for instance, in situations where CGS is investigating possible violations of CGS policies such as those relating to travel and expense reimbursement, use of the Internet, or employees conduct generally, or where the data are needed for compliance purposes.
 - More frequent access to such data may occur incidental to an email surveillance program, if and to the extent permitted by applicable laws.
 - CGS will not use any such collected data for any purpose other than explicitly stated in this Notice.

8.6. Disclosure about providing personal data

- a) Where we ask you to provide personal data to us on a mandatory basis, we will inform you of this at the time of collection, and if information is required by the contract or statute this will be indicated.
- b) Failure to provide any mandatory information will mean that we cannot carry out certain Workforce processes. For example, if you do not provide us with your bank details, we will not be able to pay you.
- c) In some cases, it may mean that we are unable to continue with your employment or engagement as CGS will not have the personal data we believe to be necessary for the effective and efficient administration and management of our relationship with you.
- d) Apart from personal data relating to yourself, you may also provide CGS with personal data of other third parties, notably your referees, dependents and other family members or friends, for purposes of WORKFORCE administration and management, including employment verification, the administration of benefits and to contact your next of kin in an emergency.
- e) Before you provide such third-party personal data to CGS you must first inform these third parties of any such data which you intend to provide to CGS and of the processing to be carried out by CGS, as detailed in this Notice.

Please contact us if you have any questions regarding the source of your personal data or would like more detail than is set out in this Notice.

9. Data Processing

- a) CGS processes your personal data. In this context, “processing” means dealing with the data in any way, such as using, disclosing or destroying it.
- b) The types of personal data which we process will vary depending on your role, your location and any terms and conditions of employment or engagement relevant to you. Typically, the types of personal data will include, for example, your personal and basic work details and details of your wages and benefits.
- c) Your personal data is collected and processed for various business purposes, in accordance with applicable laws and any applicable collective bargaining agreements. Data may occasionally be used for purposes not obvious to you where the circumstances warrant such use (e.g., in investigation or disciplinary proceedings).
- d) Where applicable data protection laws require us to process your personal data on the basis of a specific lawful justification, we generally process your personal data under one of the following bases:
 - 1) you have given your consent for one or more specific purposes;
 - 2) the processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into such a contract;
 - 3) processing is necessary for compliance with a legal obligation to which CGS is subject;
 - 4) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
 - 5) 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 CGS;
 - 6) processing is necessary for the purposes of the legitimate interests pursued by CGS 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.

We process your personal data for recruitment decisions, the performance of the employment contract and the termination of the employment relationship. These purposes each relate to a lawful basis for processing, as required under applicable law.

| Purpose for Processing | Lawful Basis |
|--|---|
| <p>9.1.1. Recruitment and selection</p> | <p>This processing is necessary to take steps at the applicant's request to enter a contract of employment or contract of services.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in fully reviewing and deciding on applications for employment or engagement to ensure that only suitable and appropriate candidates are assessed, shortlisted and selected.</p> |
| <p>9.1.2. Appropriate vetting for recruitment and team allocation including, right to work verification, relevant employment or engagement history, relevant regulatory status, academic / education checks and professional qualifications and bringing you on-board and creating an employment record.</p> | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in managing its business operations in the most appropriate and effective way and wishes to maintain its world class reputation and continue to attract and appoint high caliber employees.</p> |
| <p>9.1.3. Providing and administering wages, benefits and incentive schemes and reimbursement of business costs and expenses and making appropriate tax and social security deductions and contributions;</p> | <p>This processing is necessary to perform the contract between you and CGS and necessary for compliance with legal obligations.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in managing its workforce and operating its business. This includes ensuring that employees are properly rewarded, remunerated as well as remain engaged for the duration of their employment or engagement</p> |
| <p>9.1.4. General employee management, including:</p> <ul style="list-style-type: none"> – allocating and managing duties and responsibilities and the business activities to which they relate; – business travel; – employee certification, licensing and regulatory requirements; – budgeting, financial review and internal business reporting; – planning and allocating work and measuring working hours; – maintain emergency contact and beneficiary details; – manage health and safety at work and investigate and report on incidents. | <p>This processing is necessary to perform the contract between you and CGS and, where necessary, for compliance with legal obligations.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in managing its workforce and ensuring that each employee undertakes appropriate duties, are properly trained and undertake their roles correctly and in accordance with appropriate procedures.</p> |

| Purpose for Processing | Lawful Basis |
|---|---|
| <p>9.1.5. Identifying and communicating effectively with employees and other employees, including managing internal directories to facilitate contact and effective working and communication;</p> | <p>This processing is necessary to perform the contract between you and CGS.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in undertaking normal business operations and maintaining a dialogue with employees to ensure effective management and job satisfaction.</p> |
| <p>9.1.6. Managing and operating appraisal, conduct, performance, capability, behavioral, absence and grievance related reviews, allegations (including those received as part of any whistleblowing/speak-up report), complaints, investigations and processes and other informal and formal WORKFORCE and legal compliance processes and making related management decisions;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in addressing employee related concerns and issues and resolving the same and complying with applicable laws and regulations.</p> |

| Purpose for Processing | Lawful Basis |
|---|---|
| <p>9.1.7. Training, development, promotion, career and succession planning and business contingency planning;</p> | <p>This processing is necessary to perform the contract between you and CGS and for the compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in effective employee management to support its long-term business goals and outcomes to ensure it continues to retain as well as attract high caliber employees.</p> |

| Purpose for Processing | Lawful Basis |
|--|---|
| <p>9.1.8. Consultations or negotiations with employee representatives;</p> | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in ensuring that employee undertakes appropriate duties, are properly trained, supported by management and undertake their roles correctly and in accordance with appropriate procedures.</p> |
| <p>9.1.9. Processing information about absence or medical information regarding physical or mental health or condition in order to:</p> <ul style="list-style-type: none"> – assess eligibility for incapacity or permanent disability related wages or benefits; determine fitness for work; facilitate a return to work; adjust or accommodations to duties or the workplace; make management decisions regarding employment or engagement or continued employment or engagement or redeployment; and conduct related – management processes; | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in ensuring that employees undertake appropriate duties, are properly trained, supported by management and undertake their roles correctly and in accordance with appropriate procedures.</p> |
| <p>9.1.10. For planning, managing and carrying out restructuring or redundancies or other change programs including appropriate consultation, selection, alternative employment searches and related management decisions;</p> | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in making decisions relating to the future of its business in order to preserve its business operations or grow its business.</p> |

| Purpose for Processing | Lawful Basis |
|---|--|
| <p>9.1.11. Complying with reference requests where CGS is named by the individual as a referee;</p> | <p>CGS considers that it is in the legitimate interests of a new employer to receive confirmation of employment or engagement details from CGS for the purposes of confirming the former employee's employment or engagement history.</p> |
| <p>9.1.12. Operating email, IT, internet, social media, Workforce related and other company policies and procedures. To the extent permitted by applicable laws, CGS carries out monitoring of CGS's systems to protect and maintain the integrity of CGS's systems and infrastructure; to ensure compliance with CGS's policies and to locate information through searches where needed for a legitimate business purpose;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in managing its workforce and operating its business Workforce Technology systems. The Cyber Security and Technology function is essential to ensuring that this can be carried out in the most effective way.</p> |
| <p>9.1.13. Protecting the private, confidential and proprietary information of CGS, its employees, clients and third parties and protecting the security of our sites, systems, employees and visitors;</p> | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in ensuring that its business, clients, employees and systems are protected. This includes protecting our assets and the integrity of our systems; and detecting and preventing loss of our confidential information and proprietary information.</p> |
| <p>9.1.14. Complying with applicable laws and regulations (for example, maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws and regulations);</p> | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> |

| Purpose for Processing | Lawful Basis |
|---|---|
| <p>9.1.15. Planning, due diligence and implementation in relation to a commercial transaction or service transfer involving CGS that impacts on your relationship with CGS for example mergers and acquisitions or a transfer of your employment under applicable automatic transfer rules;</p> | <p>This processing is necessary for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS needs to make decisions relating to the future of its business in order to preserve its business operations or grow its business.</p> |
| <p>9.1.16. Vision of information to CGS's owners, investors, asset managers, lenders for use, review, analysis in their capacity as such or pursuant to performance of contract;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in sharing information with its owners, investors, asset managers and lenders in order for them to be able to carry out the necessary reviews and analyses in their capacities.</p> |
| <p>9.1.17. For business operational and reporting documentation such as the preparation of annual reports or tenders for work or client team records, including the use of photographic images;</p> | <p>This processing is necessary to perform the contract between you and CGS.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in ensuring that each employee undertakes appropriate duties and undertaking normal business operations.</p> |
| <p>9.1.18. Where relevant, for publishing appropriate internal or external communications or publicity material (including via social media in appropriate circumstances);</p> | <p>This processing is necessary to perform the contract between you and CGS.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest to support its long-term business goals and outcomes and CGS wishes to maintain its world class reputation.</p> |
| <p>9.1.19. To support WORKFORCE administration and management and maintaining and processing general records necessary to manage the employment, employees or other relationship and operate the contract of employment or engagement;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in effective employee management to support its long-term business goals and outcomes.</p> |

| Purpose for Processing | Lawful Basis |
|---|---|
| <p>9.1.20. To change access permissions, including creating IT and building access rights;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in complying with CGS policies and access controls.</p> |
| <p>9.1.21. To provide technical support, including and maintenance for WORKFORCE information and other IT systems;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in managing its The WORKFORCE IT function which is essential.</p> |
| <p>9.1.22. To enforce our legal rights and obligations, and for any purposes in connection with any legal claims, reports of violations or allegations made by, against or otherwise involving you;</p> | <p>This processing is necessary for the purpose of the legitimate interests pursued by CGS. CGS has a legitimate interest in protecting its organization from breaches of legal obligations owed to it and defending itself against litigation. This is needed to ensure that CGS's legal rights and interests are protected appropriately, to protect CGS's reputation and to protect CGS from other damage or loss.</p> <p>This processing is also necessary to perform the contract between you and CGS and for the compliance with legal obligations to which CGS is subject.</p> |
| <p>9.1.23. Make decisions on continuation of employment or engagement and administer terminations;</p> | <p>This processing is necessary to perform the contract between you and CGS and for compliance with legal obligations to which CGS is subject.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in managing its workforce.</p> |
| <p>9.1.24. To comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities;</p> | <p>This processing is necessary for the purpose of the legitimate interests pursued by CGS. CGS considers that it has a legitimate interest in protecting its organization from breaches of legal obligations owed to it and to defend itself from litigation.</p> |

| Purpose for Processing | Lawful Basis |
|--|--|
| <p>9.1.25. Other purposes permitted by applicable laws, including legitimate interests pursued by CGS where these are not overridden by the interests or fundamental rights and freedoms of employees.</p> | <p>This processing is necessary to comply with our legal obligations.</p> <p>This processing is also necessary for the purpose of the legitimate interests pursued by CGS.</p> |

Please note that this is not an exhaustive list and we may process your personal data for other purposes that are consistent with the legal basis on which we process your personal data. Further, additional information regarding specific processing of personal data may be notified to you locally or as set out in applicable policies.

9.2. Special Categories Processing

In addition, where we process special categories of personal data, this will always be justified on the basis of an additional lawful condition.

The processing of special categories of personal data (for example, data relating to health, sexual life, sexual orientation, racial or ethnic origin, trade union membership, political opinions or religious or philosophical beliefs) will be justified by one of the following special conditions:

- a) The processing is necessary for the purposes of carrying out obligations under employment law, social security law and for social protection, if there is no reason to believe that your legitimate interests for excluding the processing of your personal data prevails (for example, complying with health and safety rules, statutory sick pay, making reasonable adjustments for someone with a disability or ensuring any dismissal is fair).
- b) The processing is voluntary and is carried out subject to your explicit consent for one or more specific purposes (for example if you wish to participate in an additional support program or benefit related to incapacity or health promotion). If we are relying on consent, we will be clear about this and will not rely on consent if there is another relevant lawful condition.
- c) The processing is necessary for the establishment, exercise or defense of legal claims (whether a claim is made by you or a third party).
- d) The processing is necessary for an assessment of your working capacity carried out by a health professional (for example, an occupational health report).
- e) The processing is necessary for reasons of substantial public interests authorized by local law (for example, preventing or detecting unlawful acts or equal opportunities monitoring where permitted by local law). or
- f) In exceptional circumstances, the processing is necessary to protect your vital interests and you are incapable of giving consent (for example in a medical emergency).

This may include the following, although this is not an exhaustive list;

| Purpose for Processing | Lawful Basis |
|---|---|
| <p>9.2.1. Assess and review eligibility to work for CGS in the jurisdiction in which you work;</p> | <p>This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or CGS in the field of employment law, social security and social protection law, to the extent permissible under applicable laws.</p> |
| <p>9.2.2. Compliance with employment, health and safety or social security laws. For example, to provide statutory incapacity or maternity benefits, avoid breaching legal duties to you, to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to administer CGS's private medical and long-term disability schemes, to make reasonable accommodations or adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard;</p> | <p>This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or CGS in the field of employment law, social security and social protection law, to the extent permissible under applicable laws.</p> <p>To the extent that this data is managed by our occupational health advisers, this processing is necessary for the purposes of preventive or occupational medicine, for the assessment of your working capacity and management support that can be provided in terms of reasonable work adjustments, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services, to the extent permitted by applicable laws.</p> |
| <p>9.2.3. Management and investigation of any complaint under CGS's grievance policy (or other relevant policies), where such characteristics or information are relevant to the complaint, in order to comply with employment law obligations.</p> | <p>This processing is necessary for the purposes of carrying out the obligations and exercising the rights of you or CGS in the field of employment law, social security and social protection law, to the extent permissible under applicable laws.</p> <p>The processing is also necessary in order for CGS to establish, exercise and defend legal claims as a result of a complaint under CGS's policies.</p> |

We may seek your consent to certain processing which is not otherwise justified under one of the above bases. If consent is required for the processing in question, it will be sought from you separately to ensure that it is freely given, informed and explicit. Information regarding such processing will be provided to you at the time that consent is requested, along with the impact of not providing any such consent. You should be aware that it is not a condition or requirement of your employment or engagement to agree to any request for consent from CGS.

9.3. Criminal Offenses Data Processing

We will process criminal data relating to you should any criminal activity take place in connection with the workplace, in order to further investigate such activities and if necessary, take legal action.

If such personal data constitutes criminal data as allowed by applicable laws, we will only process such data if necessary to establish, exercise or defend legal claims.

10. Retention of Personal Data

- a) We only retain employee personal data for as long as required to satisfy the purpose for which it was collected by us or provided by you. We therefore will retain your personal data as a minimum for the duration of your employment with us or for a shorter period if your personal data is no longer necessary for the purpose for which it was collected or no longer accurate/up to date.
- b) In certain cases, legal or regulatory obligations (for example in the case of tax related matters) require us to retain specific records for a set period of time, including following the end of your employment. In the case of tax/bookkeeping related matters we are for example obliged to keep data concerning your wages for at least seven years.
- c) We are using the following criteria to establish our retention period:
 - as long as we have an ongoing employment relationship with you (or for a shorter period provided that the personal data is no longer necessary in relation to the purposes for which they were collected);
 - as required by legal obligations to which we are subject (such as tax and accounting obligations);
 - as advisable considering our legal position (such as applicable statutes of limitations) in order to establish, exercise and defend against legal claims; and
 - as necessary to meet our legitimate business needs (such as for forecasting, planning, follow-up etc.).

11. Transfer of Personal Data

- a) The global nature of our business means that your personal data may be disclosed to members of the CGS group outside of the state you reside or are working in. Certain suppliers and service providers may also have personnel or systems located outside of the state in which you reside or are employed in.
- b) In this context, your personal data may be transferred outside the state you reside or work in for the purposes set forth in this Notice.
- c) CGS has data transfer agreements in place which strive to ensure that your personal data receives an adequate level of protection.
- d) You have a right to request a copy of any data transfer agreement under which your personal data is transferred, or to otherwise have access to the safeguards used by contacting us. Any data transfer agreement made available to you may be redacted for reasons of commercial sensitivity.

12. Delete Personal Data

You have the right to delete or request that We assist in deleting the Personal Data that We have collected about You.

- a) Our Service may give You the ability to delete certain information about You from within the Service.
- b) You may update, amend, or delete Your information at any time by signing into Your Account, if you have one, and visiting the account settings section that allows you to manage Your personal information. You may also contact Us to request access to, correct, or delete any personal information that You have provided to Us.

- c) Please note, however, that We may need to retain certain information when we have a legal obligation or lawful basis to do so.

13. Disclosure of Personal Data

- a) Internally your direct and indirect line managers, Workforce professionals supporting your work area, and in some cases, certain colleagues will have access to some of your personal data where relevant to their role.
- b) We routinely share your personal data with other members of the CGS group where required to, for example, run processes, carry out group wide reporting, or assist with workforce planning.
- c) Certain basic personal data, such as your name, location, job title, contact information and any published skills and experience profile may also be accessible to other staff.
- d) We may also be required to disclose your personal data to third parties where permitted under local law. This will include suppliers which help us provide workforce services, tax or other authorities, a regulator, or a professional adviser.

Examples of third parties with whom your data may be shared include tax authorities, medical/occupational health professionals, regulatory authorities, law enforcement and regulatory bodies, CGS's insurers, bankers, IT administrators, lawyers, accountants, data center providers, doctors or other healthcare providers, auditors, notaries, investors, lenders, training providers, landlords, office access providers, social media and marketing suppliers, consultants and other professional advisors, payroll/tax providers, and administrators of CGS's benefits programs. Your personal data is also accessed by third parties whom we work together with in connection with IT services, such as hosting, supporting and maintaining the framework of our information systems.

- e) CGS expects such third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security. Where these third parties act as a "data processor" (for example, a payroll provider), they carry out their tasks on our behalf and upon our instructions for the above-mentioned purposes. In this case your personal data will only be disclosed to these parties to the extent necessary to provide the required services.
- f) We may also share limited information with clients where you are part of a client team or proposed team in a tender process.
- g) We use several third-party suppliers to help us provide WORKFORCE services. These third parties may have access to or merely host your personal data but will always do so under our instruction and subject to a contractual relationship.
- h) Some third parties to whom we may provide personal data, for instance private health insurance or occupational health providers or professional advisers or regulators, are data controllers, and you should refer to their own privacy notices and policies in respect of how they use your personal data.
- i) We may also be required to disclose your personal data to third parties in response to orders or requests from a court, regulators, government agencies, parties to a legal proceeding or public authorities, or to comply with regulatory requirements or as part of a dialogue with a regulator.
- j) Your personal data may also be disclosed to advisors, potential transaction partners or interested third parties in connection with the consideration, negotiation or completion of a corporate transaction or restructuring of the business or assets of any part of the CGS group.

Please contact us if you have any questions regarding recipients of your personal data or would like more detail than is set out in this Notice.

14. Children's Privacy

Our Service does not address anyone under the age of 13. We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us. If We become aware that We have collected Personal Data from anyone under the age of 13 without verification of parental consent, we take steps to remove that information from Our servers.

If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, we may require Your parent's consent before We collect and use that information.

15. Notice of Changes

CGS may change or update this Privacy Notice at any time.

Should we change our approach to data protection, you will be informed of these changes or made aware that we have updated this Notice so that you know which information we process and how we use this information. This Notice was last updated and reviewed in October 2019