

Employee/Contractor Privacy Notice

Cornerstone Document Reference - CS-IS-PR-01

Contents

Key summary	2
About us.....	2
How to contact us	3
Useful words and phrases.....	4
What information do we collect?	4
Why we process your personal data	6
How long do we keep your data?	9
How is processing your personal data lawful?	11
How we keep your data secure	13
Who will have access to your Personal Data?.....	14
Your rights	15
Other information	18

Key Summary

We process your personal information as your employer and for no other purpose.

We share your information with suppliers who act on our behalf for services such as on-site security in order to support you during the course of your employment.

In addition, we share your personal information to set up your account with providers of services such as pensions, insurance, and life assurance. They provide these services to you directly and not on our behalf.

This notice explains what data we process, why, how it is legal and your rights.



About Us

This Privacy Notice applies to employees and contractors of Cornerstone Telecommunications Infrastructure Limited ("Cornerstone").

Your employer is the company named on your contract of employment or consultancy agreement. In this Privacy Notice, "we" means whichever company is your employer.

Cornerstone is for the purposes of the General Data Protection Regulation (EU) 2016/679 and the Data Protection Act 2018, your Data Controller. This means that we are responsible for, and control the processing of, your personal information.

As your employer, we take your privacy very seriously and we ask that you read this Privacy Notice carefully as it contains important information about:

- Your rights;
- The Personal Data we collect about you and why we collect the data;
- What we do with your data, and;
- Who your information will be shared with.

If you need extra help

We have appointed the following Information Security Officer:

- Name: Sean Sadler
- Address: Hive 02, Arlington Business Park, Theale, Berkshire, United Kingdom, RG7 4SA

- Email: gdpr@ctil.co.uk



How to Contact Us

Please contact us or the Information Security Officer if you have any questions about this Privacy Notice, or the information we hold about you.

If you wish to contact us, please send an email to gdpr@ctil.co.uk or write to us at Hive 02, Building 1530, Arlington Business Park, Theale, Berkshire, RG7 4SA.



Useful Words and Phrases

Please familiarise yourself with the following words and phrases as they have particular meaning in Data Protection Laws and are used throughout this Privacy Notice:

GDPR	General Data Protection Regulation (EU) 2016/679. This legislation, along with the Data Protection Act 2018, sets out the principles and rules about how companies can process Personal Data and your rights in relation to your data.
Personal Data	Any information from which a <u>living individual</u> can be identified. This will include information such as telephone numbers, names, addresses, e-mail addresses, photographs, voice recordings. It will also include expressions of opinion and indications of intentions about Data Subjects (and their own expressions of opinion/intentions). It will also cover information which on its own does not identify someone, but which would identify them if put together with other information which we have or are likely to have in the future.
Special Categories of Personal Data	Any information relating to: rRacial or ethnic origin; Political opinions; Religious beliefs or beliefs of a similar nature; Trade union membership; Physical or mental health or condition;

	Sex life; or Genetic data or biometric data for the purpose of uniquely identifying you.
Processing	This covers virtually anything anyone can do with Personal Data, including: Obtaining, recording, retrieving, consulting, holding, organising, adapting or alter, disclosing, disseminating or otherwise making it available; and aligning, blocking, erasing or destroying it.
Data Subject	The person whom the data is about.
Information Commissioner	The UK Information Commissioner who is responsible for implementing, overseeing and enforcing the Data Protection laws.
Data Controller	The person who determines the purposes for which, and the manner in which, any Personal Data is processed.
Data Processor	The person who processes the data on behalf of the Data Controller.
Information Security Officer	This is the designated person within Cornerstone who is responsible for ensuring that the Data Protection laws are adhered to.
Data Protection Laws	The laws which govern the handling of data. This includes the GDPR and the Data Protection Act 2018.



What Information Do We Collect?

- **Personal information provided by you**

To employ you or enable you to work for us as a contractor, we collect and hold the following information about you:

Personal Data	Special Categories of Data
Name Contact details (address, phone number, email address) Date of birth Country of birth Bank account details UK National Insurance Number Passport information Photograph Marital status Sickness and absence records Employment history and references Professional qualifications Appraisals Training records Spouse/family and next of kin details (where relevant for PMI, maternity, parental leave)	Medical health information for the purpose of sickness absence management or occupational health advice. Right to work information for the purpose of preventing illegal working. Disability information to enable us to provide reasonable adjustments where required.

- **Personal information provided by third parties**

We also receive information about you from other sources, such as your previous employer, HMRC or Data Processors or Data Controllers who provide elements of our recruitment service for us. Further details are set out in the table below:

Personal Data	Special Categories of Personal Data
Identity and document verification Right to work verification Five-year employment history	Information about your health, from your GP, other treating clinician or an occupational health practitioner to enable us to more effectively cater for disabilities, sickness or

<p>Credit check and address verification</p> <p>Professional membership check (if applicable)</p> <p>Higher education check</p> <p>Tax information from the government</p> <p>Information from your previous employers, such as references</p> <p>Information about your health, from your GP, other treating clinician or an occupational health practitioner</p>	<p>injury when providing reasonable adjustments</p>
--	---

▪ **Personal information about other individuals**

If you provide us with information about other individuals (e.g. your next of kin), you confirm that you have informed the relevant individuals accordingly.

Why We Process Your Personal Data



We use your Personal Data for the following purposes listed in this section and table below. As an employer, we are required to use your data on certain legal bases - please go to the section below in this Privacy Notice which provides more detail on how processing your Personal Data is lawful.

Payroll Pension and Accounts	To calculate and pay your salary and pension contributions and to keep business accounts.
Benefits	To calculate, pay and provide benefits such as employer pension contributions, life assurance, private medical cover, and cycle to work schemes.
Security	To keep your Personal Data and that of others secure and prevent unauthorised access, loss, damage, destruction or corruption.

Business Development	To develop our business generally (i.e. we may provide your name, work contact details and/or experience to potential and existing suppliers or landlords).
Employee Administration	To administer your employment with us. For example, this will include, complying with employment contracts, legal obligations, our policies and to administer medical and sickness records, sick pay/leave information, holiday/absence, appraisals, promotions, disciplinary and grievance matters, maternity, parental leave and time off for dependants.
Business Travel	To administer any travel and/or accommodation arrangements where you are required to travel within or outside of the UK for work.
Company and Group Company Administration	To carry out administration tasks within Cornerstone, Vodafone and Telefonica (our shareholders).
Equal Opportunities and Trade Unions	To promote and monitor equal opportunities and trade union membership. This might include the processing of Special Categories of Personal data including, religious or similar beliefs, ethnic origin and trade union membership.
Restructuring	To carry out group company restructuring or acquire or merge with other businesses. We may disclose your Personal Data, including Special Categories of Personal Data for any of the above purposes, including at negotiation stage.
Regulatory Requirements	To comply with regulations governing Cornerstone or its shareholders.
Administration of Membership Records	To administer your membership with clubs, associations and other organisations for business and/or professional purposes.
Tax	To administer our revenue and tax obligations.
Training and Career Development	To administer and supervise your training and career development.

Health and Safety	To comply with health and safety laws and our policies. This may include us processing Special Categories of Personal Data, such as details of your mental and physical health.
Monitoring	To monitor your use of our IT resources. More information has been provided about this in the section headed ' Monitoring ' below.
Credit Reference Checks	To check your credit status, when required by your role and responsibilities. This will involve obtaining information about you from credit reference organisations such as Experian. If we carry out a credit check, a record of this will be kept on the credit reference organisation's files.
Visa information	To ensure we fulfil our obligations to employ only people with a right to work in the UK. This may involve obtaining Personal Data from the Home Office or other governments or bodies responsible for visas or migration globally.
References	Before you join us, we will obtain reference(s) about you from previous employers or character referees. We use this as part of our recruitment process, to determine whether you are offered employment with us.

- **Monitoring and recording communications**

We sometimes monitor and record communications with you (such as telephone conversations and emails), in accordance with our Acceptable Use Policy for the purpose of quality assurance, training, fraud prevention and compliance with our confidentiality obligations because our shareholders are subject to strict competition law requirements. We might also monitor and record in the following circumstances:

IT Maintenance	To maintain and update IT resources and to monitor for viruses and other disruptive programmes.
Unauthorised use of IT resources	To determine whether any IT resources are being used without authorisation either by employees or external hackers.

Information Gathering	To establish the existence of business-related facts and/or to determine whether communications are relevant to our business. For example, if you are away from work, to establish whether incoming e-mails are from shareholders, landlords or suppliers and to ensure that they are properly dealt with during your absence.
Legal and Policy Compliance	To determine whether Cornerstone and/or you are complying with legal requirements, our policies and rules and any other requirements which Cornerstone and/or you should comply with.
Quality Standards	To determine whether you are attaining standards which you ought to be achieving.



How Long Do We Keep Your Data?

The table below provides details of how long we will retain your data.

Data we process	How long this will be held for
Personnel and training records, including: <ul style="list-style-type: none"> • Recruitment records, qualifications and references • Annual/assessment reports • Job history • Resignation, termination and/or retirement letters • Travel and subsistence claims • Disciplinary/grievance matters • Any leave taken 	While employment continues and for six years after employment ceases
Written particulars of employment, contracts of employment, and notices of changes to terms and conditions	While employment continues and for six years after employment ceases
Opt-out forms signed in connection with the Working Time Regulations 1998	Two years from the date on which they were entered into

Records to show compliance with the Working Time Regulations 1998, including: <ul style="list-style-type: none"> • Timesheets for opted-out workers; • Health assessments for night workers; • Records of working hours for young workers 	Two years after the date they were made
Annual leave records	During employment: six years, or longer if leave can be carried over from year to year After employment ceases: for six years
Collective workforce agreements and past agreements that could affect present employees	Permanently
Works Council minutes	Permanently
Maternity records	Three years after the end of the tax year in which the maternity pay period ends
Adoption and paternity records	Three years after the end of the tax year in which the adoption pay, ordinary paternity pay, or additional paternity pay period ends
Shared parental leave records	Three years after the end of the tax year in which the shared parental leave pay period ends
Sickness records required for the purposes of statutory sick pay	Three years after the end of the tax year in which payments are made
Current bank details	During employment and for six months following the final salary payment
Record of advances and loans to employees	While employment continues and up to six years after repayment
Immigration checks	Two years after termination of employment
Death Benefit Nomination and Revocation forms	While employment continues or up to six years after payment of benefit Note that member data may also be held by the trustees of the relevant scheme as well as by us

Records in relation to hours worked and payments made to workers	Three years beginning with the day upon which the pay reference period immediately following that to which they relate ends
Payroll and wage records	Six years from the financial year-end in which payments were made
PAYE	Six years after the end of the tax years to which they relate
Any reportable accident, death or injury in connection with work	For at least three years from the date the report was made



How Is Processing Your Personal Data Lawful?

We are allowed to process your Personal Data for the following reasons and on the following legal bases:

- **Legitimate interest**

We have a legitimate interest in processing your data, having considered the impact of processing on your interests and rights, and having ensured appropriate safeguards are in place to minimise any intrusion on your privacy. The table below explains the Personal Data processed on this basis

Personal Data	Legitimate Interests
<ul style="list-style-type: none"> • Appraisal information • Training records • Professional qualifications 	To maintain and develop the efficiency and competence of our staff. This captures information about you in the context of your role and is therefore not intrusive. It is also beneficial to you and helps you develop your skills and qualifications
<ul style="list-style-type: none"> • Email content • Internet activity information • Phone usage 	To protect our network and ensure that our IT resources are being used in a safe and secure manner

<ul style="list-style-type: none">• Photos• Contact details	To promote us at events or on our web site
--	--

▪ **Contract**

It is necessary for the performance of your employment contract with Cornerstone. For example, we require your bank details in order to comply with our obligation to pay your salary

▪ **Legal Obligations**

It is necessary for the purpose of compliance with a legal obligation. For example, we are required under the Working Time Regulations to process certain data about your working hours and annual leave.

▪ **Vital interest**

It is necessary for the protection of your vital interests, such as your life. For example, in an emergency we may need to disclose data relating to your health to a medical professional without your consent.

▪ **Special Categories of Personal Data**

We will only process Special Categories of Personal Data for the following reasons and subject to the following exceptions.

Consent

We will process Special Categories of Personal Data where you have given us your consent to do so. For example, if you have given us explicit consent to process details relating to your ethnic or religious background for diversity monitoring or you wish to have an optional occupational health assessment.

Employment

We may be required to process Special Categories of Personal Data for compliance with our obligations under employment law.

Vital Interests

Processing Special Categories of Personal Data may be necessary for us to protect your vital interest. For example, it may be necessary for us to process your medical or health information in an emergency without your consent, in order to protect your life.

Manifestly Public Personal Data

We may process Special Categories of Personal Data if you have made it public, for example, information made public on a public social media platform.

Legal claims

We may process Special Categories of Personal Data in order to defend or establish a legal claim. For example, we may need to process such data in defending a discrimination claim brought under the Equality Act 2010.

Health purposes

We may process Special Categories of Personal Data for health-related purposes, including in connection with occupational health advice.

Criminal convictions

We are required to process such data for the purposes of compliance with regulatory obligations and criminal reporting requirements that we are subject to. This may include compliance with police procedures in connection with various investigations.

How We Keep Your Data Secure



We use technical and organisational measures to safeguard your Personal Data, for example we use secure connections on the Core, to ensure data residing on it is encrypted. This means that we convert your data into a computer code, which will make it harder for hackers to access your data when stored on the Core or your OneDrive.

We have up-to-date technical security measures and security policies. These ensure that we follow good practices across our business, and we require the same of our suppliers. We aim to keep your information safe from external threats such as hackers and malicious software and internal threats such as applying patches to laptops and servers. However, you also need to play your part by ensuring all patches are installed as soon as you receive the appropriate notification.

Whilst we will use all reasonable efforts to safeguard your Personal Data, you acknowledge that the use of the internet is not entirely secure and for this reason we cannot guarantee the security or integrity of any Personal Data that are transferred from you or to you via the

internet. If you have any particular concerns about your information, please contact us (see 'How you can contact us?' above).

Who Will Have Access to Your Personal Data?

We may disclose your Personal Data to third parties who provide certain employment and recruitment services for us, including:

Personal Data	Who information is shared with
Payroll information, including your salary, age, national insurance number, benefits information and bank details	Our outsourced payroll provider (currently CGI, Octopus and Cascade HR)
Personnel records	Our online HR records system, which is used for internal purposes (currently Octopus and Cascade HR)
Information necessary for administering your pension entitlement, including your salary, contact details, national insurance number and pension contribution information	Our pension scheme provider (currently Standard Life)
Information necessary for administering your life and health insurance benefits, including your name, date of birth, address, contact details and details of any dependants named by you	Our life and health insurance provider (currently Vitality)
Information necessary to allow you to have access to our online benefits platform, including your name, contact information, date of birth, employee ID and bank details	Our online rewards platform provider (currently Reward Gateway)

Your name and contact details for the purpose of access to online assessments used as part of our onward development and recruitment process	Our online assessments provider (currently Talent Q)
If you were placed with us by a recruitment firm, your name, CV and contact information may be contained on a cloud-based system	Recruitment agencies (including preferred suppliers such as Project People)
or shared over email, for the purpose of managing our relationship with them	Stored in Applicant Tracker System (currently Bullhorn)
Pre-employment information including your CV, employment history, a copy of your passport or other identification documents, right to work information, training history, credit check information, professional membership details and bank statements	Our pre-employment verification provider (currently Agenda)



Your Rights

As a Data Subject, you have the following rights under the Data Protection Laws:

- the right of access to Personal Data relating to you;
- the right to correct any mistakes in your information;
- the right to restrict or prevent your Personal Data being processed in some circumstances;
- the right to have your Personal Data ported to another Data Controller;
- the right to erasure of your Personal Data; and
- the right to withdraw consent to receive our newsletter.

These rights are explained in more detail below, but if you have any comments, concerns or complaints about our use of your Personal Data, please contact us using the contact details above. We will respond to any rights that you exercise within a month of receiving your request, unless the request is particularly complex, in which case we will respond within three months. There are exemptions to many of these rights which we will apply in accordance with the law.

▪ **Right to access Personal Data relating to you**

You may ask to see what Personal Data we hold about you and be provided with:

- A copy;
- Details of the purpose for which it is being or is to be processed;
- Details of the recipients or classes of recipients to whom it is or may be disclosed, including if they are overseas and what protections are used for those overseas transfers;
- The period for which it is held (or the criteria we use to determine how long it is held);
- Any information available about the source of that data; and
- Whether we carry out any automated decision-making, or profiling, and where we do information about the logic involved and the envisaged outcome or consequences of that decision or profiling.

Requests for your Personal Data must be made to gdpr@ctil.co.uk in writing and a copy will be retained on your personnel file.

To help us find the information easily, please give us as much information as possible about the type of information you would like to see.

If, to comply with your request, we would have to disclose information relating to or identifying another person, we may need to obtain the consent of that person if possible. If we cannot obtain consent, we may need to withhold that information or edit the data to remove the identity of that person if possible.

There are certain types of data which we are not obliged to disclose to you, which include Personal Data which records our intentions in relation to any negotiations with you where disclosure would be likely to prejudice those negotiations.

▪ **Right to correct any mistakes in your information**

You can require us to correct any mistakes in your information which we hold, free of charge. If you would like to do this, please:

- Email, call or write to us (see 'How can you contact us?' above)
- Let us have enough information to identify you (e.g. account number, username, registration details), and
- Let us know the information that is incorrect and what it should be replaced with.

▪ **Right to prevent processing of Personal Data**

You may request that we stop Processing your Personal Data temporarily if:

- You do not think that your data is accurate. We will start processing again once we have checked whether or not it is accurate;
- The processing is unlawful, but you do not want us to erase your data;
- We no longer need the Personal Data for our processing, but you need the data to establish, exercise or defend legal claims; or
- You have objected to processing because you believe that your interests should override Cornerstone's legitimate interests.

▪ **Right to erasure**

You can ask us to erase your Personal Data where:

- You do not believe that we need your data in order to process it for the purposes set out in this Privacy Notice;
- You had given us consent to process your data, you withdraw that consent and we cannot otherwise legally process your data;
- You object to our Processing and we do not have any legitimate interests that mean we can continue to process your data; or
- Your data has been processed unlawfully or has not been erased when it should have been.

▪ **Right to withdraw consent**

We will not process your Personal Data until you have given your consent for one or more specific purposes as listed above. As well as clearly expressing consent, you also have the right to withdraw consent you have given us at any point. This is a vital and necessary aspect of consent, and at Cornerstone we are aware that you may wish to withdraw consent at any time.

▪ **Copies of your Personal Data (Data portability)**

You may ask for an electronic copy of your Personal Data which we hold electronically and which we process when we have entered into a contract with you.

▪ **What will happen if your rights are breached?**

You may be entitled to compensation for damage caused by contravention of the Data Protection Laws.

▪ **Complaints to the regulator**

If you do not think that we have processed your data in accordance with this Privacy Notice, you should let us know as soon as possible. Similarly, you may complain to the Information

Commissioner's Office. Information about how to do this is available on the website at www.ico.org.uk.



Other Information

Changes to the Privacy Notice

We might change this Privacy Notice from time to time, and if we do, we will provide you with notice by email of the changes.