ISS.4.13

Information Security Standard -

Colleague Privacy Notice

Version History

Version	Date	Author	Comments & Updates
1.00	23-May-2018	Sabiha Ali	Initial Candidate Privacy Notice document
2.00	26-Jul-2018	Sabiha Ali	Release for Public Website Update to section 3, Your rights in relation to your personal data - more details. Update to section 13, Data Protection Officer details.

Release Control

The following personnel must formally approve the document prior to assigning a non-draft version number.

Prepared by (Name & Title)	Authorised by (Name & Title)	Date Approved for Release
Sabiha Ali, HR Business Partner	Marc Sellis, Business Change Director & Acting HR Director	23-May-2018
Sabiha Ali, HR Business Partner	Marc Sellis, Business Change Director & Acting HR Director	26-Jul-2018

Distribution

Version	Distributed to	Date distributed
V1	Company Intranet	25-May-2018
V2	Public Website	26-Jul-2018

Document Review

This Data Privacy Management document will be reviewed each year by the document owner/author following the initial publication. Document to be ratified for publication by the Trenitalia c2c Executive Team.

Copyright

Table of Contents

1. Introduction

c2c is committed to protecting the privacy and security of your personal information and being transparent about how we collect and use your data. We are aware of our obligations under the General Data Protection Regulation (GDPR) and this Privacy Notice sets out, in line with GDPR, the types of data that we hold on you during and after your working relationship with c2c. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

We will process your personal data in accordance with this Privacy Notice, unless such processing conflicts with the requirements of applicable law, in which case, applicable law will prevail.

We may update this Privacy Notice from time to time and will publish updated copies of the Privacy Notice on the company intranet.

This Notice applies to all current and former c2c Employees, Community Volunteers, Consultants, Contractors, Suppliers and Vendors hereinafter to be referred to as: "Colleagues" who store, control and process data (both electronic and physical/paper based) relating to identifiable individuals - Data Subjects.

This Notice should be read in conjunction with the c2c Personal Data Protection Policy and the Acceptable User Agreement.

2. Data Protection Principles

c2c complies with its obligations under GDPR in relation to your personal data. This includes:

- Lawfulness, Fairness and Transparency
  - *The personal data shall be processed lawfully, fairly and in a transparent manner*
- Purpose Limitations
  - *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*
- Data Minimisation
  - *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*
- Data Accuracy
  - *Personal data shall be accurate and, where necessary, kept up to date*
- Storage Limitations
  - *Personal data shall be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed*
- Integrity and Confidentiality (Security)
  - *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*
- Accountability
  - *c2c and all c2c Colleagues shall be responsible for, and be able to demonstrate compliance with data protection laws*

3. Your rights in relation to your personal data

Individuals, be they current or former Colleagues, have specific rights under Data Protection Laws. You **must** notify the Data Protection Officer immediately if you get a request from an individual who wishes to exercise one of their below rights:

I. Right to be Informed

All individuals have the right to be informed of how we collect and use their data. This is typically done through the c2c Privacy and Cookies Notice and the Colleague Privacy Notice (this Notice).

II. Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. We have an obligation to correct the inaccuracies and to respond to the request within one month.

III. Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. This right enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

However, the right to erasure does not provide an absolute 'right to be forgotten'. Certain records must be kept under Statutory Law and regulations. The Data Retention, Media Destruction and Backup Policy has full details of different record types and lengths of time they will be kept for, however the following types of documents provide a brief example of records required to be kept;

- Financial Records - 7 Years
- Health Information - upto 40 years

Individuals have a right to have personal data erased and to prevent processing in some specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data has to be erased in order to comply with a legal obligation.

IV. Right to Restrict Processing

Individuals have a right to 'block' the processing of their personal data. If we receive such a request we must ensure that we retain just enough information to the restriction is respected in the future.

V. Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer their personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

VI. Right to Object

Individuals have the right to object to c2c processing their personal data based on legitimate interests and/or direct marketing (including profiling).

VII. Right of Access

All individuals who are a subject of personal data held by c2c are entitled to:

- Obtain a confirmation of the processing;
- Be informed the Personal Data we hold about them;
- Be informed of the categories of Personal Data concerned, and
- Obtain a copy (subject to certain limitations and exemptions).

VIII. Rights in relation to automated decision making

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal (or similarly significant) effects concerning the individual without any human intervention (eg automatic refusal of an online credit application or decisions on recruitment).

c2c does not make any decisions about an individual solely on the basis of automated decision making.

If an individual contacts c2c requesting the execution of any of these rights, the individual should be asked to email sar@c2crail.net to make a subject access request.

- Under Data Protection Laws we must respond to valid requests within no more than one month.
- For more info, please see the Subject Access Request Policy & Guidance, or by email at dpo@c2crail.net.

4. How we collect your personal data

We collect data about you in a variety of ways and this will usually start when we undertake a recruitment exercise where we will collect the data from you directly. This includes the information you would normally include in a CV or a recruitment cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms at the start of your employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

We will also collect data about you from third parties, such as employment agencies, former employers when gathering references or occupational health provider for a medical screening.

5. Types of data we collect

We collect and hold many types of data about you, including:

- your personal details including your name, address, gender, date of birth, email address, phone numbers
- your photograph
- marital status, dependants, next of kin and their contact numbers
- medical or health information including whether or not you have a disability
- information about your remuneration, including pay grades, salary, tax code, national insurance number, bank account, entitlement to benefits such as pensions or insurance cover
- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK including passport and visa
- driving licence
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with c2c, current and previous job titles, job descriptions, hours of work and other terms and conditions relating to your employment with us
- details of your schedule (days of work and working hours) and attendance at work
- details of your leave records including annual leave, family leave (maternity, paternity, parental, adoption, carer), sickness absence, sabbatical, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence
- details of any performance management concerns including measurements against targets, formal warnings and related documentation with regard to capability procedures
- details of any live criminal record where applicable
- details of genetic, biometric data where applicable

- competence management records

We also undertake monitoring of employees in the workplace to protect the legitimate commercial interests of the business, to ensure a safe working environment for all employees, for the prevention and detection of crimes and to comply with legal obligations (e.g. access rights or disclosure). Monitoring of employees can be carried out by:

- information captured on security systems, including closed circuit television ("CCTV")
- key card entry systems
- GPS/Geolocation tracking of c2c vehicles
- tracking of emails and websites visited
- voicemails and documents
- other work product and communications created, stored or transmitted using our networks, applications, devices, computers or communications equipment

6. Why we process your personal data

There are a number of reasons why we need to collect and process your personal data these would include:

- to perform the employment contract that you have entered into with us
- to carry out legally required duties
- to carry out our legitimate interests
- to protect your interests
- for archiving, research or statistical purposes
- where you have given consent
- where something is done in the public interest

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data in order to carry out the employment contract that we have entered into with you and ensure you are paid.

We need to collect your data to ensure we are complying with legal requirements such as:

- ensuring tax and National Insurance is paid
- carrying out checks in relation to your right to work in the UK
- making reasonable adjustments for disabled employees
- to comply with health and safety laws including drug and alcohol testing
- to meet our legal obligations on reporting on the gender pay gap
- to comply with out legal obligation on carrying out unspent criminal records checks
- to enable you to take periods of leave

We also collect data so that we can carry out activities which are in c2c's legitimate interests. Processing your data allows us to:

- make decisions about who to offer initial employment to, and subsequent internal appointments, promotions etc
- make decisions about salary and other benefits
- provide contractual benefits to you
- maintain comprehensive up to date personnel records about you to ensure, amongst other things, effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained
- effectively monitoring both your conduct and your performance and to undertake disciplinary and performance procedures with regard to both of these if the need arises
- offering a method of recourse for you against decisions made about you via a grievance procedure
- to meet our legitimate interests to carry out workplace investigations
- the reasons of preventative or assessing your training needs
- operate and keep a record of employee performance and related processes, to plan for career development, succession planning and workforce management purposes
- implement an effective absence management system including monitoring the amount of leave and subsequent actions to be taken, including unsatisfactory attendance and the making of reasonable adjustments
- gain expert medical opinion when making decisions about your fitness for work
- manage statutory leave and pay systems such as maternity leave and pay etc
- to share with you information about the company
- carryout business planning and restructuring exercises
- provide references on request for current and former employees
- maintain and promote equality in the workplace
- dealing with legal claims made against us
- preventing fraud
- to carry out surveys for service improvements
- ensure effective HR and business administration
- ensure our IT systems are secure and robust against unauthorised access

7. Special categories of data

There are a number of reasons why we need to collect special categories of data which will processed in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process your data in order to carry out our legal obligations
- we must process your data for reasons of substantial public interest
- you have already made the data public

Special categories of data we collect are:

- race
- ethnic origin
- politics
- religion
- trade union membership
- biometrics
- health
- sex
- sexual orientation

We will use your special category data:

- for the purposes of equal opportunities monitoring
- in our absence management procedures
- to determine reasonable adjustments, particularly for those with disabilities
- for health and safety purposes including random drug and alcohol testing
- to operate check-off and payment for union subscriptions
- to comply with industry fitness standards
- for gender pay gap reporting

Special categories of data that we uses for monitoring purposes is anonymised, and is collected with your express consent, which can be withdrawn at any time. The use of sensitive data for monitoring purposes helps c2c to better plan services for both our colleagues and our customers.

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time for which here will be no consequences.

8. If you do not provide your data

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties e.g. ensuring you are paid correctly.

We may also be prevented from confirming, or continuing with your employment with us, in relation to our legal obligations, e.g. if you do not provide us with documentary evidence confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

9. Sharing your data

We share your data with colleagues within c2c where it is necessary for them to undertake their duties. This includes for example:

- your line manager for their management of you
- HR for maintaining personnel records
- Payroll for administering your payment
- IT to provide you with electronic equipment and work email

We also share your data with third parties, some of whom are outside of the EEA, where it is necessary for them to undertake their duties. This includes for example:

- pre-employment references from other employers
- criminal records checks from the Disclosure and Barring Service (DBS, Disclosure Scotland)
- the provision of occupational health
- Rail Staff Travel (RTS) so you can benefit from rail staff travel facilities
- medical checks from medical doctors and consultants
- RPMI Limited for administration of the Railway Pensions Scheme
- The Pensions Regulator (TPR) if required
- HMRC for Tax deductions and NI contributions

We may also share your data with third parties as part of a Company sale or restructure, or for other reasons to comply with a legal obligation upon us.

10. Protecting your data

We take the security of your data very seriously and are aware of the requirement to ensure your data is protected against accidental loss, destruction, disclosure or abuse and is not accessed except by those authorised to do so to carry out their duties. We have implemented and use appropriate technologies and procedures to protect your data against such data breaches.

Our information security policies and procedures are reviewed regularly and updated as necessary to meet our business needs, changes in technology and regulatory requirements. For example:

- Procedures and systems
  - we have measures in place to protect against accidental loss, unauthorised access, unauthorised use, destruction or disclosure
  - we place appropriate restrictions on access to personal information
  - we implement appropriate measures and controls, including monitoring and physical measures to store and transfer data securely
  - we store your personal data in personnel files with HR, with your manager and within c2c's HR and IT systems
  - we conduct Data Privacy Impact Assessments (DPIA) in accordance with legal requirements and our business policies
- Colleagues
  - we provide privacy, information security and other applicable training on a regular basis for colleagues who have access to our colleague data
  - we take steps to ensure that our colleagues operate in accordance with our data protection procedures
- Third party
  - where we share your data though our collaboration with third parties, we request they confirm that your data is held securely and in line with GDPR
  - we require that third parties implement appropriate technical and organisational measures to ensure the security of your data

11. Retention of your data

In line with data protection principles we will retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including any legal, accounting, reporting and legitimate requirements.

12. Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

13. Data Protection Officer

c2c has appointed a Data Protection Officer to ensure we protect personal data of our customers & others and comply with data protection legislation.

If you any questions about how c2c uses your personal data that are not answered here, or if you want to exercise your rights regarding your personal data, please contact our Data Protection Officer:

Our DPO: Andy Stewart-Wright

Email: dpo@c2crail.net

Phone: 0330 109 8130

Write to: Data Protection Officer, Trenitalia c2c Limited, 2nd Floor, Cutlers Court, 115 Houndsditch, London EC3A 7BR

You have the right to lodge a complaint with the Information Commissioner's Office. Further information, including contact details, is available at https://ico.org.uk or call 0303 123 1113

14. Who to Contact About This Notice

Any questions about this policy should be directed to the Human Resources department.

Email: hr@c2crail.net
Write to: Human Resources, Trenitalia c2c Limited, 2nd Floor, Cutlers Court, 115 Houndsditch, London EC3A 7BR

Glossary

Term	Meaning
Colleagues	all c2c Employees, Community Volunteers, Consultants, Contractors, Suppliers and Vendors.
Community Volunteer	A person or organisation that freely provides a service or performs a designated role or activity.
Contractor / Supplier / Vendor / Consultant	A person or organisation that undertakes a contract to provide goods, works, services or tenancy to c2c
Controller	A person, organisation, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Classification: *CONFIDENTIAL* *INTERNAL* *PUBLIC*	 Highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorisation by the Data Owner is required for access because of legal, contractual, privacy, or other constraints. Confidential data has a very high level of sensitivity Information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorised access, modification, transmission, storage or other use. This classification applies even though there may not be a statute requiring this protection. Internal Data is information that is restricted to personnel who have a legitimate reason to access it Information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to disclosure rules, is available to all employees and all individuals or entities external to c2c
Data Subject	Is any living person who's personal data is being collected, held or processed.
Employee	A person employed by c2c under a contract of employment (for the avoidance of doubt this includes FTE's and those employed on fixed term contracts, but not those employed through consultancy

	agreements)
Information Commissioner's Office (ICO)	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.
"Need to Know" Principle	The "Need to Know" principle pertains to Protectively Marked Material that Colleagues will need to have access to, or modify in order to carry out their roles within the organisation. Colleagues who do not have "Need to Know" shall be prohibited from accessing and processing such material.
Personal Data	Any information relating to a living individual who can be identified from that information – either on its own or when put together with other information that c2c holds. This includes any expression of opinions about the individual and any intentions of any person in respect of the individual. For example, names, addresses, telephone numbers, CCTV images, photographs, etc.
Processing	Collecting, obtaining, recording or holding the information or data or carrying out an operation or set of operations on Personal Data, including, but not limited to: • Organisation, adaptation or alteration of the data • Retrieval, consultation or use of the data • Disclosure of the data by transmission, dissemination or otherwise making it available, or • Alignment, combination, blocking, erasure or destruction of the data
Role Based Access Control (RBAC)	RBAC is a method of restricting network and application access based on the roles of the individual users within the business. RBAC let's Colleagues have access rights to only the information they need to perform their job role and prevents accessing information that does not pertain to their job role.
Sensitive Personal Data	Includes Personal Data consisting of information relating to: 1. Racial or ethnic origin 2. Political Opinions 3. Religious beliefs or beliefs of a similar nature 4. Trade Union membership

	5. Physical or mental health or condition 6. Sexual life 7. Commission or alleged commission of any criminal offence 8. Proceedings for any criminal offence or alleged criminal offence, the disposal of such proceedings or the sentence of any court in such proceedings.

This page is intentionally blank to indicate the end of this document