Data Protection Policy
for Job Applicants, Employees, Workers and Consultants

PRIVACY NOTICE

CONFEDERATION OF PASSENGER TRANSPORT

MAY 2018

Confederation of Passenger Transport
22 Greencoat Place, London SW1P 1PR
020 7240 3131 admin@cpt-uk.org www.cpt-uk.org
A company limited by guarantee no. 1182437 England

Data Protection Policy and Privacy Notices
for Job Applicants, Employees, Workers and Consultants

1 Overview

1.1 The Confederation of Passenger Transport (CPT) takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our service to our membership and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to job applicants, current and former employees, workers, volunteers, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.3 CPT has separate policies and privacy notices in place in respect of members and prospective members, suppliers and other categories of data subject. A copy of these can be obtained from the Finance Director.

1.4 CPT has measures in place to protect the security of your data in accordance with our Data Security Policy. A copy of this can be obtained from Finance Director.

1.5 CPT will hold data in accordance with our Data Retention criteria as detailed in this policy. We will only hold data for as long as necessary for the purposes for which we collected it.

1.6 CPT is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.7 This policy explains how CPT will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, CPT.

1.8 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by CPT at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, CPT intends to comply with the 2018 Act and the GDPR.

1.9 CPT has carried out an audit and produced a register of all personal data held, the reasons for collecting, processing and storing it. A copy of the audit may be viewed at: Y/CPTNET. The Manager Chief Executive's Office will regularly review and update the personal data register.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;

- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, or someone else (such as a former employer or your doctor), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

3.4 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, references, qualifications and details of any pre-employment assessments;
- your contact details and date of birth;
- the contact details for your emergency contacts;
- your gender;
- your marital status and family details;
- information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement;
- your bank details and information in relation to your tax status including your national insurance number;
- your identification documents including passport and information in relation to your immigration status and right to work for us;
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings);
- information relating to your performance and behaviour at work;
- training records;

- electronic information in relation to your use of IT systems/swipe cards/telephone systems;
- your images (whether captured by photograph or video);
- information relating to your attendance including sickness absence, attendance records, maternity and paternity leave, parental leave, shared parental leave, emergency dependants leave, compassionate/discretionary leave; and
- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 '**Special categories of personal data**' are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 CPT will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing. See details of your rights in section 13 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

7 Examples of when we might process your personal data

7.1 We have to process your personal data in various situations during your recruitment, employment (or engagement) and even following termination of your employment (or engagement).

7.2 For example (and see section 7.5 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you;
- to decide how much to pay you, and the other terms of your contract with us;
- to check you have the legal right to work for us;
- to carry out the contract between us including where relevant, its termination;
- training you and reviewing your performance*;
- to decide whether to promote you;
- to decide whether and how to manage your performance, absence or conduct*;
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else;
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*;

- to monitor and protect the security (including network security) of the Company, of you, our other staff, members and others;
- to monitor and protect the health and safety of you, our other staff, members and third parties*;
- to pay you and provide pension and other benefits in accordance with the contract between us*;
- paying tax and national insurance;
- to provide a reference upon request from another employer;
- monitoring compliance by you, us and others with our policies and our contractual obligations*;
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*;
- to answer questions from insurers in respect of any insurance policies which relate to you*;
- running our business and planning for the future;
- the prevention and detection of fraud or other criminal offences;
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*;
- to reimburse expenses incurred on CPT business; and
- for any other reason which we may notify you of from time to time.

7.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Manager Chief Executive's Office.

7.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

7.5 We might process special categories of your personal data for the purposes in paragraph 7.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety.

7.6 We do not take automated decisions about you using your personal data or use profiling in relation to you.

8 Job Applicants

8.1 The personal data of job applicants will be collected, processed, retained and disposed of in accordance with the principles laid down in this policy.

8.2 Job Applicants will be notified of their rights in respect of personal data by way of a Privacy Notice. (Appendix 1).

9 Access to your personal data

9.1 Authorised members of staff will have access to some or all of your data in order to carry out the terms of your contract or in order to fulfil legal obligations or legitimate business interests.

9.2 Internally the following Directors and Managers have access to your personal data and where relevant access to personal sensitive data (for example if there is a need to access health data in respect of making reasonable adjustments). Access to personal and sensitive personal data is normally limited to:

- Your Director/Line Manager in respect of the terms of employment;
- Finance Director in respect of salary payments and setting up benefits;
- Manager Chief Executive's Office in respect of administering HR policies and maintaining records;
- Chief Executive in respect of management of the organisation
- CPT Chairman (where appropriate for example when hearing a Grievance or Disciplinary appeal)

10 Sharing your personal data

10.1 We share some items of your personal data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

10.2 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

10.3 We may share relevant data in order to carry out legitimate activities with the following third parties:

- Moorepay in respect of payroll
- Royal London insurance in respect of pension provision
- Unum in respect of Life Assurance provision
- Prudential (Vitality) in respect of private health insurance provision
- Canada Life in respect of Income Protection provision (Directors)
- Gallaghers Brokers in respect of sourcing employee insured benefits
- Predictive Proactive Solutions Ltd in respect of IT support and processing
- Vodafone in respect of mobile phone provision
- Barclaycard in respect of CPT credit cards
- Amanda Edge HRM in respect of HR Support
- The Kings Mill Partnership our Auditors in respect of auditing our financial records and processes
- And any other legitimate agencies such as HRMC

10.4 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

11 How should you process personal data for CPT?

11.1 Everyone who works for, or on behalf of, CPT has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Security policy.

11.2 CPT's Finance Director is our nominated Data Protection Manager and is responsible for reviewing this policy and updating CPT's Executive Management Team on the CPT's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

11.3 You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of CPT and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

11.4 You should not share personal data informally.

11.5 You should keep personal data secure and not share it with unauthorised people.

11.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

11.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

11.8 You should use strong passwords.

11.9 You should lock your computer screens when not at your desk.

11.10 Personal data should be password protected in a Word Documents before being transferred electronically to authorised external contacts.

11.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

11.12 Do not save personal data to your own personal computers or other devices.

11.13 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Finance Director.

11.14 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

11.15 You should not take personal data away from CPT's premises without authorisation from your line manager or the Finance Director (Data Protection Manager).

11.16 Personal data should be shredded and disposed of securely when you have finished with it.

11.17 You should ask for help from the Finance Director if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

11.18 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

11.19 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

12 How to deal with data breaches

12.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

12.2 If you are aware of a data breach you must contact the Finance Director immediately and keep any evidence you have in relation to the breach.

13 Subject access requests

13.1 Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Finance Director who will coordinate a response.

13.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to the Finance Director. We must respond within one month unless the

request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

13.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

14 Your data subject rights

14.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

14.2 You have the right to access your own personal data by way of a subject access request (see above).

14.3 You can correct any inaccuracies in your personal data. To do you should contact the Manager Chief Executive's Office.

14.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the Manager Chief Executive's Office.

14.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the Manager Chief Executive's Office.

14.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

14.7 You have the right to object if we process your personal data for the purposes of direct marketing.

14.8 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

14.9 With some exceptions, you have the right not to be subjected to automated decision-making.

14.10 You have the right to be notified of a data security breach concerning your personal data.

14.11 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the Manager Chief Executive's Office.

14.12 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

15 How long will we keep your data?

15.1 CPT will keep your data whilst we are entitled under law to process it, there are legitimate business interests for doing so or where it is necessary for the establishment, exercise or defence of legal claims.

15.2 The following criteria are used to determine data retention periods of personal data:

- Retention in Case of Queries

  CPT will retain your personal data for as long as necessary to deal with any queries (for example a query about your holiday entitlement)
- Retention in Case of ensuring your Health & Wellbeing

  CPT will retain health related personal data for as long as necessary to ensure your Health, Safety and Wellbeing (for example where it is necessary to make reasonable adjustments in respect of any disability)
- Retention in case of Claims

  CPT will retain your personal data for as long as you might legally be able to bring claims against the organisation; and
- Retention in accordance with legal and regulatory requirements.

  CPT will retain your personal data during and after your employment has ended however this comes about based on legal and regulatory requirements.

15.3 All personal data will be disposed of confidentially and securely.

Employee/Worker (Consultant) Signature

I have received, read, understand and will comply with the requirements of the Data Protection Policy.
I am aware of my rights under the policy.
I will draw to the attention of the Finance Director any breaches of this Policy.

Signed: _____ Date: _____

Appendix 1

PRIVACY NOTICE

JOB APPLICANTS

As part of any recruitment process, the Confederation of Passenger Transport (CPT) collects and processes personal data relating to job applicants. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information do we collect?

CPT collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process; and
- information about your entitlement to work in the UK.

CPT may collect this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment. We may also collect personal data about you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why does CPT process personal data?

We need to process data to take steps at your request prior to entering into a contract with you. We may also need to process your data to enter into a contract with you.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, it is mandatory to check a successful applicant's eligibility to work in the UK before employment starts.

CPT has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

CPT may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. We may also collect information about whether or not applicants are disabled to make reasonable adjustments for candidates who have a disability. We process such information to carry out our obligations and exercise specific rights in relation to employment.

Who has access to data?

Your information may be shared for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process including our external HR Consultant and Committee Members, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

We will not share your data with other third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you.

How does CPT protect data?

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by authorised personnel in the proper performance of their duties.

For how long does CPT keep data?

If your application for employment is unsuccessful, the organisation will hold your data on file for 6 (six) months after the end of the relevant recruitment process. At the end of that period, or once you withdraw your consent, your data is deleted or destroyed.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your Human Resources file (electronic and paper based) and retained during your employment. A copy of our Data Protection Policy will be provided to you which details the periods for which your data will be held.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the organisation to change incorrect or incomplete data;
- require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- object to the processing of your data where CPT is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact the Manager Chief Executive's Office.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to CPT during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.