

Peopletime Limited – Privacy Policy relating to the use of the PeopleManager Application

A. What is the Policy purpose?

This policy provides information about how Peopletime Limited (“Peopletime”) collects and processes personal data of those using its PeopleManager Application. It also includes details of your privacy rights along with contact information if you need further information.

Please take the time to read this privacy policy so that you can understand how and why we collect and process your data.

B. What is the purpose of the PeopleManager Application?

Peopletime is a data processor of payroll, HR and personal data relating to its clients’ employees. It helps make it easier for you and your employer if you can submit data in a simple and easy way via, for example, your phone. It also minimises the risk of data being incorrectly recorded about you if you provide it directly to us as the Data Processor. When employees provide such data to Peopletime via the PeopleManager Application or otherwise, the respective employer of those employees remains the data controller with responsibility for such data. Peopletime, as the Data Processor, processes such personal data in accordance with our service agreement with our clients and this privacy policy.

C. What data do we collect about you?

The Data Stored section of the Peopletime Data Retention and Archiving Policy at Appendix A sets out details of the data that we may collect about you as an employee:

If you provide personal data about someone else – for example details of your next of kin, then you are responsible for ensuring that you comply with all relevant data protection legislation including letting them know that you are sharing their personal data and the reasons for that.

When you use the PeopleManager Application, it will also collect some technical information such as:

- Your IP address (the name and internet address your device uses to connect to the Application)
- What parts of the Application you used and what you did in the Application including the time of your visit.

D. What do we use your data for?

Peopletime Limited is a provider of outsourced payroll and HR services. In that capacity it is required to process personal data about its clients' employees in order to be able to provide such services for its clients. Our aim is to hold and process only such personal data as is reasonable in order to provide such services. These services include:

- The processing of payroll including the calculation of net pay, tax, National Insurance contributions and pension contributions;
- Arranging the transmission of net pay to employee bank accounts;
- Reporting relevant data to HMRC, Pension providers and the employer;
- Recording Employees' Holiday and Absence;
- Recording and processing data relating to the employment of individuals – including the generation of employment contracts and other employment related documentation;
- Providing HR and/or Payroll advice to your employer.
- Provide software support to you in relation to using the PeopleManager Application
- Comply with the law including the requirements of HMRC

We do not use your information other than to provide services to your employer and to comply with the law. If we wish to use your data for any other purpose, we would not do so without first notifying you in writing.

No automated decision making processes are used in relation to the processing of your personal data.

Your information is held for as long as reasonably required or permitted as more particularly detailed in Appendix A.

E. How do we keep your Personal Data secure?

It is, of course, vital that your Personal Data is kept securely and only able to be accessed by those who have a legitimate reason for accessing it. We take this very seriously and accordingly take appropriate technical and organisational measures to prevent unauthorised access to your personal data. These precautions include:

- The servers upon which PeopleManager data is held are located in a secure data centre with suitable physical and electronic security measures in place to reduce the risk of unauthorised access;
- Access to Personal data within Peopletime is restricted to those who need to have such access to provide our services to employers
- Undertaking periodic penetration testing of our servers;
- Having appropriate back up procedures in place to ensure data is not permanently lost or corrupted;
- Not processing your data outside the UK or Ireland

F. Who can see your Personal Data?

The main users of your personal data will be your employer and those employees of Peopletime who are responsible for providing HR or Payroll services to your employer. In addition, we may provide your personal data to others when:

- You have agreed to share the data - e.g. to your landlord or mortgage provider;
- We need to share your personal data to provide payroll and/or HR services to your employer e.g. we use a third party BACS bureau to facilitate salary payments to employees and they will need to know the identity and bank details of those receiving payments, we may also use a third party reference checking agency to conduct reference checks on behalf of your employer;
- We need to send the information to third parties who are providing services to you or your employer – for example pension providers, providers of Medical and other insurance services to you
- The business of Peopletime is acquired by a third party in which case the information will be provided to the new owners to use the information in substantially the same way as used previously i.e. to provide payroll and/or HR services.
- We are required to comply with a court order or other legitimate request by a body with which we must lawfully comply.

G. What rights do you have in relation to the processing of your Personal Data?

You have rights under data protection law in relation to your personal data. You have the right to:

- Request access to your personal data
- Request that your personal data be corrected or deleted
- Object to the processing of your personal data
- Request restrictions on the processing of your personal data
- Request a transfer of your personal data
- Withdraw consent to the processing of your personal data

Please note that exercising some of these rights will adversely impact upon our ability to provide services to your employer.

If you wish to raise a complaint on how we have handled your personal data, please contact us at:

Data Compliance Officer

Peopletime Ltd

13 Castle Street

Buckingham

MK18 1BP

and we will investigate the matter.

Data Protection legislation allows us up to one month to respond to data requests. If it would reasonably take longer than a month to respond to your request, we may take up to an extra two months to respond. In such circumstances we will advise you and keep you updated.

If you are not satisfied with our response or believe our processing of your personal data is not in accordance with the law you can complain to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF – telephone 03031231113. www.ico.org.uk.

H. What are your responsibilities?

Peopletime cannot control what, when or how you submit data via the Application or otherwise. Please therefore make sure that you take care when providing your data. If you do find that you have provided incorrect data or your data changes (e.g. you change your address or bank details) you can normally amend these via the PeopleManager Application.

Please also make sure that you keep your Application log in details confidential. If you are at all concerned that your password has been compromised please make sure that you change it immediately to help secure your data.

I. Updating this Policy

We reserve the right to update this Privacy Policy from time to time as we reasonably determine. We will post any updated Policy on our website so that you can make yourself aware of the current policy at any time.

This version issued 22 April 2021

Appendix A - Peopletime Ltd Data Retention & Archiving Policy

Peopletime Limited has a responsibility to look after the personal data we collect, including information about our employees, clients, client employees and delegates. As outlined in our Data Protection Policy, personal data will only be retained for as long as is necessary and destroyed or anonymised when no longer required. Therefore, it is vital we maintain clear and specific policies and procedures with regards to the retention, archiving and destruction of personal data.

Personal data can only be retained beyond the retention period outlined in this policy with the written approval of our Data Protection Officer (DPO) in line with the General Data Protection Regulation (GDPR).

All documents will be kept in line with current legislative requirements.

For many types of HR records, there is no definitive retention period: it is up to the employer to decide how long to keep them. Different organisations make widely differing decisions about the retention periods to adopt. Employers must consider what a necessary retention period is for them, depending on the type of record.

Peopletime Limited has decided to keep historical records based on the time limits for potential UK tribunal or civil claims and to comply with HMRC guidance.

The UK Limitation Act 1980 contains a 6-year time limit for starting many legal proceedings. So, where documents may be relevant to a contractual claim, it is recommended that these are kept for at least a corresponding 6-year period. These documents may be retained by us in either hard copy or electronic format depending on the situation.

If an employee of Peopletime Limited is found to have breached this policy, they may be subject to our disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this document and how it may apply to you, seek advice from the Peopletime Limited DPO.

Definitions

Archiving

A process of moving data that is no longer actively used to a separate storage device for long-term retention.

Data subject

Any living person who is the subject of personal data (see below for the definition of personal data) held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, mental, economic or social.

Destruction

The process of destroying data, either in hard copy or electronic format, so that it is completely unreadable and can no longer be accessed or used.

Personal data

Any information relating to a data subject.

Retention

The continued storage of data for compliance or operational reasons.

Retention Policy

The DPO will determine how long data is required and define the time periods for which personal data records should be retained, deleted or archived within the Retention Schedule of this document. **If a category of personal data is not specified within this policy, the retention period will be deemed to be 3 years from the date of creation or acquisition.** The DPO will annually review the data we hold and update the Retention Schedule as appropriate.

Archiving Policy

Under GDPR, we can process personal data for archiving purposes beyond the stated retention period if doing so is in the public interest, or for historical, scientific or statistical purposes. We ensure that archiving does not contravene the rights and freedoms of data subjects and that appropriate technical and organisational safeguards are in place, such as data minimisation, pseudonymisation or encryption.

Destruction Policy

The DPO oversees and documents the destruction of personal data in accordance with the Retention Schedule. (see below)

Litigation

We may be legally required to retain personal data beyond stated retention periods to comply with ongoing investigations, litigation or other legal proceedings until any dispute is fully resolved and no longer open to appeal. If you are aware of any anticipated or existing litigation, you should notify our DPO, so they can suspend any deletion or minimisation of personal data.

Data Stored

Peopletime stores the following information about its employees and client employees for the purposes of HR services, HR software, Time and Attendance and Payroll services:

HR Service and PeopleManager

Data fields – Data Subject personal information:

- Data Subject ID number
- First name
- middle name
- surname
- email
- gender
- date of birth

- national insurance number
- address
- home telephone
- business telephone
- mobile number
- job title
- right to work in the UK details
- nationality
- disability status
- professional registrations
- identity verification
- DBS outcome – dates and confirmation only
- Pre-employment health screening – dates and confirmation only
- qualifications
- department
- working hours
- working days
- work pattern
- job start date
- length of service
- first manager id
- second manager id
- holiday approver id
- NI category
- Reference details including name and contact details of referee and previous employment

Data fields – Data Subject personal information – *special category data*

(Limited number of clients require this)

- religion
- ethnic origin
- marital status
- sexual orientation

Data fields – Benefit records

- Details of benefits awarded to Data Subject
- Start date of benefit
- End date of benefit
- Value of benefit

Data fields – Pensions

- Name of scheme
- Date of joining scheme
- Contribution details

- Opt-out confirmation

Data fields – Driver information

- Type of licence held
- Licence number
- Date of licence
- Penalty information
- Confirmation of MOT and Insurance if using own car

Data fields – Absence data:

- absence entitlement
- start date of absence
- expected end date of absence
- confirmed return date
- medical fit to work note received
- sickness category

Data fields – Pay data:

- Pay rates – including salary and hourly paid values
- Shift premiums
- Commission agreements
- Bonus values

Data fields – Time and Attendance data:

- Employee Rota
- Employee clocking data (start, break and finish times)
- Overtime
- TOIL time
- Break times
- Device identifying data
- GPS location (remote mobile clocking only)

Data fields – HR activities

- Details of the HR Activity recorded
- Start date of Activity
- End date of Activity
- Recurrence if applicable
- Notes if required

Data fields – Training Records

- Details of training undertaken by the Data Subject
- Date of the training
- Recurrence if applicable
- Value of training

Data fields – Next of Kin details

- Name of Next of Kin
- Address of Next of Kin
- Telephone Number of Next of Kin
- Mobile Number of Next of Kin
- Relationship of Next of Kin to the Data Subject
- Email address of Next of Kin

Data fields – Bank details

- Name of Bank
- Branch Name
- Account Name
- Sort Code
- Account Number
- Building Society Number

Data fields – e-signed documents

- Details of any document e-signed by the Data Subject via the Employee Self Service Portal
- Date of signature of any document e-signed by the Data Subject via the Employee Self Service Portal

Data fields - Payment Records

- Details of any additional payments made to the Data Subject
- Date of any additional payments made to the Data Subject

Documents

- Copies of any uploaded documents relating to the Data Subject e.g. contracts, right to work documents, HR letters, sick or fit notes, copy right to work documents, copy driving licence details.

Data fields - Emergency Communication Details

- Primary and Secondary telephone number
- Primary and Secondary email address

Expenses Forms

- Copies of any expense forms submitted electronically by the Data Subject via the Employee Self Service Portal

Appraisals

- Copies of any appraisal forms submitted electronically by the Data Subject via the Employee Self Service Portal
- Copies of any appraisal forms submitted electronically by the Manager via the Employee Self Service Portal

Email notifications

As a part of Peopletime service, alerts are delivered via email to nominated users. These alerts include the following personal information:

- Name of Data Subject
- Data Subject ID
- Company
- Absence Type
- Start date of Absence
- End date of Absence
- Data Subject Message
- Indication of Changes to the Data Subjects personal information
- Expiry date of Right to Work documents
- Expiry date of driving licences
- Leave date
- Start date
- Significant ages e.g. 22
- Professional Registration expiry date
- HR activities types
- HR activity due date
- Contract Expiry dates

Payroll Data fields – Data Subject payroll information:

- Data Subject ID
- First name
- middle name
- surname
- email
- gender
- date of birth
- national insurance number
- address
- home telephone
- business telephone
- mobile number

- job title
- National Insurance category
- Department
- Student Loan status
- Benefit Type
- Value of Benefit

Data fields – Pay data:

- Pay rates – including salary and hourly paid values
- Payment values
- Deduction values

Data fields – Pensions

- Name of scheme
- Date of joining scheme
- Contribution details
- Opt-out confirmation

Data fields – Bank details

- Name of Bank
- Branch Name
- Account Name
- Sort Code
- Account Number
- Building Society Number

Anti-Money Laundering

For the purposes of compliance with our obligations regarding Anti-Money Laundering regulations we must undertake customer due diligence and as a result hold the following data on the directors/owners of our payroll clients.

- Name
- Start date of Directorship.

Emails

From time-to-time information about individuals is contained in emails between our employees and our clients. Whilst we encourage all users to ensure that data is not included in the body of emails and is either sent as a password protected attachment or as a preference use the Secure File Transfer Protocol facility which is available to each client.

All documents then are treated as detailed below.

As occasional data or instruction is included in email correspondence emails are retained for 7 years in line with the other HR and payroll information as they relate to these functions.

Company Details

Peopletime keeps information on its client contacts for the purposes of delivering its service. The data it holds in this respect is as follows: -

- Name
- Email Address

Retention Schedule

Data	Retention Period after leaving employment or end of service	PPM	SAGE	e-FILES	WorkManager
Data Subject personal information	7 Years	X	X	X	
Data Subject personal information (special category)	1 year	X			
Benefit records	7 Years	X	X	X	
Pension details	12 years		X	X	
Driver details	7 years	X		X	
Absence Data	7 years	X			
Pay Data	7 years	X	X		
Time and Attendance Data	7 years	X		X	
HR Activities	7 years	X		X	
Training Records	7 years	X		X	
Next of Kin Data	3 months	X			
Bank Details	3 months	X	X		
e-signed document data	7 years	X			
Payment Records	7 years	X	X		
Documents (HR e.g., contracts, letters etc.)	7 years	X		X	
Emergency Communication Details	3 months	X			
Expense Forms	7 years	X	X		
Client contact data	3 years				X
Emails	7 years			X	