Data controller: Ypeople

Data protection compliance representative: Jennifer Allan, Head of People

Ypeople collects and processes personal data relating its employees to manage the employment relationship. Ypeople is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

Data we process in relation to casual workers and volunteers is also covered by this notice.

What information does Ypeople collect?

Ypeople collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- 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 Ypeople;
- information about your remuneration, including entitlement to benefits such as pensions or life assurance scheme;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your working pattern (days of work and working hours) and attendance at work;
- For those who are undertaking lone working appointments, details of personal appearance, contact details, emergency contract details, safety device tracking number and any other relevant information;
- details of periods of leave taken by you, including holiday, sickness absence, compassionate leave and unpaid leave 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, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which Ypeople needs to make reasonable adjustments; and
- equal opportunities monitoring information including information about your ethnic origin, sexual orientation, disability, and religion or belief;
- information on training sessions attended, results of e-learning training and evaluation feedback forms;
- Vehicle insurance, MOT and details of your driving licence, where you use your own vehicle in the course of your duties.

Ypeople may collect this information in a variety of ways. For example, data might be collected through application forms; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, Ypeople may collect personal data about you from third parties, such as references supplied by former employers, occupational health practitioners or the employee's own medical practitioner, and information from criminal records checks permitted by law.

Ypeople seeks information from third parties with your consent only.

Data will be stored in a range of different places, including in your personnel file, in Ypeople's online HR management systems and in other IT systems on Ypeople's server (including Ypeople's email system).

Why does Ypeople process personal data?

Ypeople needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer pension and entitlements.

In some cases, Ypeople needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled.

In other cases, Ypeople has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows Ypeople to:

- run recruitment and promotion processes;
- to fulfil our statutory reporting duties;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, to provide support for employee's to effectively manage long and short term absence, and ensure that employees are receiving the pay to which they are entitled;
- to maintain the safety of staff undertaking lone working appointments;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that Ypeople complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- to monitor learning and development and measure the effectiveness of training courses;

- provide references on request for current or former employees; and
- respond to and defend against legal claims.

Special categories of personal data or Criminal records data

Special categories of personal data such as information about health or medical conditions, is processed to carry out employment law obligations such as those in relation to employees with disabilities. Ypeople may obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law and to provides support for employees to effectively manage long and short-term absence.

Absence data is held securely on the HR Management system and is confidentially destroyed or deleted after 2 rolling years. The employee's manager and the HR Department have access to this information on the system, through a secure log in.

Medical or Occupational Health reports are retained in the employees personal file for a rolling 2 year period from the date it was obtained or the duration of employment if the organisation has a duty to make reasonable adjustments. Access to this information is restricted to the HR Department. Where appropriate, medical information will be shared with management to implement reasonable adjustments or support relating to medical conditions or to manage health and safety. Information relating to employee's health condition will be shared with our Occupational Health provider should a medical referral be requested. In this instance, Ypeople will also seek explicit consent to process this data.

Where Ypeople processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that Ypeople uses for these purposes is collected with the express consent of employees, which can be withdrawn at any time by notifying the HR Department in writing. Equal opportunities data is anonymised for reporting purposes. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so. Results will be recorded by the HR department in a secure format and retained for 5 years for trend analysis. Data on gender is gathered on the Vacancy Filled form when the employee commences employment for the purposes of anonymised monthly reports and statutory reporting on gender pay gaps. This information is only accessed for this purpose. This data is held securely on the HR management system for the duration of employment and 7 years after employment ends.

Ypeople is obliged to seek information about criminal convictions and offences for successful job applicants and do 3 yearly update checks for current employees. This information is processed by Disclosure Scotland, which is an Executive Agency of the Scottish Government and runs on behalf of Scottish Ministers. Where Ypeople seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to statutory legal obligations and the requirements of our regulatory bodies. Membership or certificate number, date the check was carried out, and expiry date are all recorded on the password protected HR Management System. Certificates are stored in a secure filing system and destroyed and replaced after any update has been carried out. The certificates of those leaving the organisation will be destroyed one month after the leaving date.

If a relevant conviction is declared a Risk Assessment exercise is undertaken by the line manager, which is then authorised by a senior manager. The risk assessment

documentation will be retained with the certificate in a secure storage system, separate from the employee file for 3 years until the next scheduled update is carried out.

If the outcome of a risk assessment results in the termination of employment, the Risk Assessment paperwork will be retained for 7 years after employment has ended. Ypeople may also be legally required to share details of dismissal or termination of employment with Disclosure Scotland, Care Inspectorate and Scottish Social Services Council.

Ypeople will not use any personal data for any purpose other than those outlined above.

Who has access to data?

Your information may be shared internally, including with members of the HR Department and Finance Department your line manager or senior managers in the area in which you work if access to the data is necessary for performance of their roles.

Ypeople shares your data with third parties in order to obtain and provide pre-employment references from other employers, obtain necessary criminal records checks from the Disclosure Scotland Service. The organisation may also be required to share your details with the Scottish Social Services Council when you apply for or renew your registration with them. The organisation may also be obliged to make a referral to SSSC or Disclosure Scotland as part of the Discipline, Performance or Absence Management process.

Ypeople also shares your data with third parties that process data on its behalf in connection with payroll, IT and telecommunications, regulatory bodies, the provision of benefits, training, health and safety and the provision of occupational health services.

Ypeople Management Accounting and Payroll systems
Ypeople Banking system
HMRC
You Manage HR System
Safeshores Monitoring Limited
Amalgamate Occupational Health Providers
Scottish Widows Pension Provider
The People's Pension Provider
YMCA Group Life Assurance
CRISIS Counselling Service
Click Networks IT support service
Scottish Social Services Council
Disclosure Scotland
Care Inspectorate
Scottish Qualifications Authority
Yellow Com
Charity Learning Consortium E-learning Platform

Ypeople will not transfer your data to countries outside the European Economic Area.

How does Ypeople protect data?

Ypeople takes the security of your data seriously. Ypeople has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

The steps taken to ensure data is protected are:

- Restricted Permission Access to electronic folders on the shared drive.
- Personal password protection on HR Management System, Finance and Payroll Systems, and Operational Management Systems.
- Locked filing cabinets to store personal data, special categories of data and criminal record information.
- Local Restrictions on making copies, printing and transporting hard copies of personal data and confidential files.
- Local Restrictions on what information is appropriate to send electronically.
- Password Protection on emailed documents, which is disclosed separately to the intended recipient.
- Retention and cleansing timescales for data.
- Secure destruction of personal data information.
- Redacting any information regarding the identity of the individual where appropriate.

Where Ypeople engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

For how long does Ypeople keep data?

Ypeople will hold your personal data during and after the end of employment as set out in the relevant retention periods, outlined in the Data Protection Policy.

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 Ypeople to change incorrect or incomplete data;
- require Ypeople 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 Ypeople is relying on its legitimate interests as the legal ground for processing.

If you would like to exercise any of these rights, please contact Jennifer Allan, Head of People, who has been appointed as the person with responsibility for data protection compliance within Ypeople. **They can be contacted at dp@ypeople.org.uk. Questions about this policy, or requests for further information, should be directed to them.**

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

What if you do not provide personal data?

You have some obligations under your employment contract to provide Ypeople with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide Ypeople with data in order to exercise your statutory rights, such as in

relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable Ypeople to enter a contract of employment with you. If you do not provide other information, this will hinder Ypeople's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated decision-making

Employment decisions are not based solely on automated decision-making.