This privacy notice explains the processing of personal data of prospective employees, current employees and former employees of Assurity Consulting Ltd (including the entity of Assurity Consulting Holdings Ltd).

Topics:

Why do we process your personal data?

Assurity Consulting Ltd need to collect and process information about you (personal data) as a prospective employee, an employee, or a former employee for many reasons including but not limited to:

- selection and recruitment of job applicants;
- staying in contact with prospective employees who have signed up to our mailing list;
- obtaining references;
- checking the right to work in the UK;
- checking driving licence information for drivers of company vehicles;
- undertaking DBS checks to satisfy our customer requirements;
- setting up the employment contract;
- paying our employees;
- providing an auto enrolment pension scheme;
- providing benefits to our employees;
- providing references for employees;
- booking work travel;
- providing HMRC and other government agencies with information required by law;
- providing our customers and suppliers with business transaction documents including quotes, orders, invoices, credit notes, reports, letters, details of who will undertake work, training and competency records, risk assessments, etc;
- keeping our employees safe by recording accidents and incidents, investigating causative factors to make improvements going forward, and undertaking risk assessments and providing personal emergency evacuation plans (PEEPs);
- making or defending insurance claims or court cases relating to personal injury, liability or professional indemnity;
- recording of images when entering and leaving our offices using your pass fob or when an alarm is activated for the purposes of theft prevention and fire security only;

- and marketing our products in print, and also in video and other formats through our website, social media and through trade press and media.

What are the principles we apply when processing your personal data?

As a responsible business we apply and are able to demonstrate compliance with the following principles for the control and processing of personal data relating to you as a prospective employee, an employee, or a former employee:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- processed in a way that is adequate, relevant and limited to what is necessary;
- maintained to ensure it is accurate and where necessary kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- 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.

We take reasonable steps to ensure that third parties who process data on our behalf also apply and are able to demonstrate compliance with the above principles.

What types of data do we process?

The following list is not exhaustive, but will give you an idea of the kinds of data we may process relating to you. This list will be reviewed regularly as part of the review of this privacy notice to make sure it is as complete as possible:

Your job application – CV, covering letter, qualification certificates
Copy of right to work documents
Your name
Your signature
Your salutation
Your gender
Your date of birth
National insurance number
Home address
Personal phone number
Company phone number
Personal email address
Company email address
Pay and tax data, including pay slips, P60s, P45s, and P11D
Contract letters
Accident and incident records, sickness and absence records, doctors certificates, medical letters, maternity and paternity and shared parental information, adoption

information, return to work meeting notes, risk assessments, PEEPs (these may contain medical information that is treated as special category data)
A record that you have undertaken a DBS check with an indication of the outcome of the check (this may contain criminal offence data only if you have disclosed this information to us)
Disciplinary and grievance evidence, investigations, and hearing minutes
Written warnings, final written warnings, and performance management letters.
Bonus letters and details of targets and objectives and remuneration and benefits.
Review meeting notes and personal development notes and actions
Emails that you send or receive or are copied or blind copied in
In Case of Emergency (ICE) details of next of kin etc.
Driving licence details and licence checks – for those who drive or have driven on company business
Passport details – for those who may travel on company business
Communications from external authorities relating to the individual – such as speeding offence letters from the police, parking fine letters from local authorities, request for information from Child Support Agency.
Communications from 3rd party suppliers of benefits in relation to the benefits you are being provided or possibly cannot be provided due to circumstances.
Your image when entering and leaving our offices using your pass fob or when an alarm is activated for the purposes of theft prevention and fire security only.

What lawful bases do we have for processing your data?

For prospective employees the act of you applying for a job is your consent for us to process your data purely for the purposes of the recruitment and selection of the job role you have applied for. If you are not successful in your application and we want to process you for another job role or a potential future job role we will ask for your permission to do this.

For employees we process your data to perform the contract of employment between you and us. Some processing of data is directly related to performing our contract of employment as well as to meet legal obligations such as submitting pay data to HMRC. Some processing of data, such as providing information to police about a company car speeding offence or providing the Child Benefit Agency with your data is required for us to meet our legal obligations.

Where we hold criminal offence data we do so with your explicit consent. You may choose not to disclose criminal record data from a DBS check to us. Records of conducting DBS checks and whether or not the certificates contain any information is retained to perform the contract or employment between you and us and also in many instances is then required for us to perform contracts between us and third parties that require such checks such as Schools, financial institutions and charities that require safeguarding of vulnerable individuals.

Where we hold special category data (medical information disclosed as part of accident, incident, sickness, etc. records) we do so under the 'employment, social security and social protection law' condition of processing. There are many laws that

require this processing of data. The Social Security (Claims and Payments) Regulations requires that we keep accident records. The Health and Safety at Work, etc. Act 1974 requires employees to co-operate with employers to enable them to fulfil their statutory duties, including reporting all dangerous occurrences, near misses and accidents whether or not they resulted in injury, damage or disease. The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations requires us as an employer to report certain defined work-related events to the enforcing authority.

We may hold maternity, paternity, shared parental and adoption related records in order to establish eligibility of benefits and leave – this is covered by various laws and information of eligibility and records that employers should obtain can be found on the gov.uk information pages.

For former employees we may need to process your data to perform duties in closing the contract of employment, such as notifying benefit providers that you no longer work for us. Some processing will be necessary to meet legal obligations such as retention of tax and pay records. Much of the longer term retention of data will be on the grounds of legitimate interests to defend legal and insurance claims both on behalf of us and our suppliers and customers.

How long will we retain your personal data?

N.B. Where there is an outstanding dispute, court proceedings, legal claim, insurance claim, or similar we may extend the retention periods stated below of data relevant to the case until the case is closed and the window of opportunity to appeal any decision is considered to be closed.

Prospective employees: We will keep your data for the duration of the recruitment campaign that you have applied for and unless you are unsuccessful or specifically give us permission to keep your data for longer we will delete all of your personal data within 7 months of the completion of the recruitment campaign. Our processing of your data will be limited to the sole purpose of recruitment and selection for vacancies at Assurity Consulting Ltd.
Current employees: We will keep relevant data throughout the duration of your employment. You have a duty to inform us of changes, such as changes to your address or other contact details, and we will ensure that we keep your records up to date based on the updates you have provided.

Former employees:
Within 6 months
We will inform relevant third parties such as suppliers, customers, benefit providers that you are no longer an employee as soon as possible after your termination of employment and within 6 months of your last day of employment.

Work email addresses and phone numbers will remain active for up to 6 months after your last day of employment to allow customers and suppliers the opportunity to be redirected to someone who can support them or provided with a message that redirects them.

Within 12 months
To allow for data to be available for any immediate tribunal cases relating to your employment or termination of employment most of the personnel files will remain largely intact for up to one year after the end of employment. Within this year the file will be reviewed, and information that is no longer required will be deleted. This will include the deletion of next of kin data, grievance and disciplinary information (except where it may be required in evidence to support a legal claim – e.g. a disciplinary 'for fighting' may be needed to defend a personal injury claim and therefore will be kept for up to 7 years), holiday requests, CV and references obtained for original employment.

Within 24 months
Marketing videos, brochures etc. are very expensive to produce. If you were mentioned or appeared in a photo or video marketing campaign we will ensure that this is no longer used in active marketing within 2 years of your last day of employment.

Within 7 years
Sickness records and details of any accidents will be kept for up to 7 years in case a personal injury claim should be brought against the company that requires defending.

Employee pay data, including pay rise letters, bonus letters and tax data will be kept for up to 7 years to meet the requirements of tax and pay audits.

Training records will be kept for up to 7 years to help our customers show that work was completed by competent individuals.

Right to work check data will be kept for up to 7 years to defend any illegal working court cases.

Within 40 years
On the advice of our liability and professional indemnity insurers, customer reports will be retained for up to 40 years. These reports can contain your name if you were the person who undertook the work. This will also include letters and emails that you have sent to customers or been copied in on that provide customers with advice, scope of works, quotations for work etc. Such correspondence may be deleted as required as per our customer or supplier privacy notice guidelines.

Asbestos related data will also be kept for up to 40 years. This includes your training records if you undertook asbestos services, and any information that relates to any potential exposure of you to airborne asbestos fibres.

We will also keep your name, last job title, employment start date and employment end date for up to 40 years after you cease to be an employee. This will allow us to confirm to a potential new employer if you ever worked for us, and could also be used to confirm when you worked for us in the case of a long term employer liability claim.

Data back-ups.

To protect our business interests we undertake secure back-ups of our data. As these back-ups are formed of disc images it is not realistic for us to delete or search for individual data items in these back-ups. However, we limit our back up retention to 12 months so within 13 months after the retention guidelines given above, the data will also have been removed from our back-up systems.

Who is the data controller and who processes your data?

Assurity Consulting Limited is the data controller.
We have our own in house HR and Finance functions and so we also process much of the required personal data for the purposes of maintaining the contract of employment, and processing payroll.

However, there are many third parties that we need to send your data to and from for processing, these include but are not limited to:

For prospective employees

- Job boards may be used as a portal for your application
- A specialist consultancy can be used to host and provide reports on selection tests for personality, preference or mental ability.
- Current employer, previous employers, academic referees and personal referees may be contacted to provide references (you will have provided the details of these third parties for this purpose).
- Depending on the job role applied for then prior to or during initial employment we may request credit or criminal record checks through a third party. DBS certificates will only ever be sent to a home address you provide and you can then decide if you wish to disclose this information to us.

For employees and former employees

- Bank – for payment of wages.
- Inland Revenue, Companies House, Child Support Agency, and other government and pseudo government agencies – to meet legal requirements we need to provide details about your employment, your salary, benefits, tax and national insurance contributions.
- Payroll software support – when supporting our software, temporary access to process data may be required to fix any issues.
- Accountancy firm – as part of our annual audit they need access to payroll records, contracts of employment, pay rise letters etc. to make sure we are meeting legal and best practice standards.
- Commercial and employment lawyers and interested parties – where there is a possible or actual employee dispute, or where due diligence is required relating to ownership of the business or any transfer or undertakings, employee data will need to be shared with our lawyers and where relevant the lawyers of the interested party and the interested party themselves.
- Police, local government, toll and parking operators – details requested relating to whom a company vehicle was assigned to when an alleged offence or alleged contravention of use contract etc. took place.
- Credit card provider – for those who have a company credit card

- Mobile data operators – for those who have company phones, company broadband, or company mobile enabled devices
- Car fleet operator, accident management company, vehicle hire operator, driving licence checking operator, car insurer and broker, and their third parties, – for those who are assigned or need to drive a company vehicle, or a vehicle hired or leased to the company.
- Travel agents, and the transport and hotel companies themselves – for employees who travel on company business, information about the employee including passport details will need to be shared.
- Private medical insurance provider, cash plan provider, medical insurance broker – for employees who benefit from private medical insurance.
- Pension provider, pension advisor and brokers – for employees who benefit from the pension scheme and also employees who must be automatically enrolled irrespective of if they elect to opt-out.
- Childcare voucher provider - for those who elect to receive this benefit.
- Life assurance provider – for all employees who may be eligible to receive this benefit we provide details so that they can receive the benefit once they have completed 1 year of service.
- Permanent Health Insurance provider – for those who are members of this scheme (this scheme closed to new members in 2010).
- Commercial insurers and commercial insurance brokers – to process a claim personal information about those involved and witnesses if applicable may need to be provided.
- Suppliers in general – to maintain our contract and service with them they will need contact information for finance, main and secondary contacts.
- Customers in general – to maintain our contract and service with them they will need contact information for finance, main and secondary contacts. They may also need training and competency data and may also need further information such as date of birth or NI number for security purposes to enable access to their property. If they request to see a copy of a criminal record check you will need to decide if you are happy to disclose this information.
- Customers 3rd party invoice and health and safety portals – to maintain contracts with some customers we need to upload some information to portals provided by their third parties. This will usually be limited to name, job title and contact details if you are assigned to undertake the work for the customer.
- Auditing companies to maintain our certifications and accreditations – training records, and other information such as who processed a customer report may need to be accessed as part of these audits.

It may sometimes be necessary to transfer your personal information overseas. When this is needed information is normally only shared within the European Economic Area (EEA). Our main data servers are located in the UK and maintained by a UK based data storage company. Data may be transferred outside of the EEA by the data storage company as part of their support provision to ensure continuity of service. We have a contract in place with the data storage company to ensure that the highest data security standards are maintained. Any transfers made will be in full compliance with all aspects of the data protection act.

What are your rights as a data subject?

If you would like to realise any of these rights please contact us using the contact details provided in the 'how to contact us' section of this document. Please make it clear what right you want to realise and be as specific as possible with what you want so that we can prioritise your request.

Right to be informed – you have the right to be informed about how and why we process your personal data. This privacy notice is designed to meet this requirement.

Right of access – you have the right to access your personal data that we hold on you. If you make a request please try and be as specific as possible about the type of data you would like to have access to and the time frames you would like us to look at. We may contact you to discuss your request to help meet your needs.

Right to rectification – you have the right to request that we rectify your personal data. We also want to make sure that your personal data is accurate and up to date. Please let us know if there is data about you that you believe is incorrect and needs to be rectified.

Right to erasure (to be forgotten) – you have the right to request the deletion or removal of personal data. We believe that we have set out clearly the data we hold, the legal basis for processing the data and a realistic retention period which balances the rights of you as an individual against the interests of us and third parties. However, if you believe that we have data on you that should be deleted, please let us know, so that we can investigate.

Right to restrict processing – you have the right to request that we 'block' or suppress processing of data (including deletion of data). If you wish to exercise this right please let us know the reasons for this.

Right to object – you have a right to object to our processing of your personal data. If you wish to exercise this right please give clear details of the grounds of your objection.

Right to data portability – We do not believe that we hold data on our prospective employees, employees or ex-employees that falls into the definition of this right within the GDPR regulations. However if you believe we are incorrect please let us know why and what data you believe we should enable for portability. When you leave our employment we will create a P45 to transfer required employment data to a new employer. We may also decide to provide a reference if requested by a new employer.

Rights related to automated decision making including profiling – you have a right to be informed that profiling or automatic decision making will be performed, right of access to things like the logic involved in automatic decision making, and the right not to be subject to a decision based solely on automated decision making. If we

wish to profile your data or automate decisions based on your data we will let you know as soon as possible.

Right to lodge a complaint with a supervisory authority – you have the right to raise a complaint with the supervisory authority in the country where you live, where you work, or where the infringement took place. In the UK the supervisory authority is the ICO (ico.org.uk).

Changes to this privacy notice

We regularly review our privacy notices. The most up to date privacy notices are available on our website. The date of issue of this privacy notice is indicated in the footer of the document.

How to contact us?

Please contact us if you have any questions about this privacy notice or the personal data we hold about you:

Email: DataProtection@assurityconsulting.co.uk
Write: Data Protection Compliance Coordinator
Assurity Consulting Ltd
26 Redkiln Way
Horsham
West Sussex
RH13 5QH