Intelligent compliance | Unique combination of smart people and smart tech

HR Privacy Statement Momenta Employees

June 25 | V4.0

Introduction

Momenta Interim Management Limited (Momenta) replaces the following: Momenta Operations (London employees), Momenta People (employees on assignment) and in addition Momenta Resourcing Pty (employees in Sydney), and Momenta Associates Pty Ltd (contractors on assignment in Australia), as controller of personal data for their employees, prospective employees and contractors, for the purposes of managing the employment, prospective employment or contracting relationship. The company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

Momenta is part of TCC Holdings group which encompasses The Consulting Consortium (TCC), Recordsure and Momenta. Employee data is controlled by HR, which is a central support function for all three companies.

This privacy statement explains:

- What personal data we collect from you directly or passively from you, or which we obtain indirectly from other sources.
- How we use that data and for what purpose.
- Who we share your data with.
- How the company protects any personal data.
- Your rights as an individual.

You can be assured that your data will only be used in accordance with this privacy statement. This privacy notice complies with data protection requirements under GDPR, Data Protection Act 2018 and the Australian Privacy Principles (APPs) under the Privacy Act 1988.

Data Controller

HR, TCC, Recordsure and Momenta
10 Lower Thames Street
London
EC3R 6EN
United Kingdom

Email: hr@tcc.group

Telephone: 020 7374 6600

How do we collect your data?

Momenta collects your personal data in a variety of ways directly from you, or indirectly for the purposes of recruitment and employment.

What information do we collect?

Momenta collects and processes a range of information about you. This may include:

- 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 within the company) and documents relating to gaps in employment.
- Professional membership of organisations.
- Previous remuneration, including entitlement to benefits such as pensions or insurance

cover.
- Credit inconsistencies, for example county court judgements.
- Previously committed fraudulent acts.
- Sanction checks where applicable.
- Criminal record where applicable.
- Nationality and entitlement to work in the UK and Australia.
- Bank account and national insurance number.
- Marital status, next of kin, dependents and emergency contacts.
- Details of your schedule (days of work and working hours) and attendance at work.
- Periods of leave taken by you, including holiday, sickness absence, family leave and the reasons for the leave.
- 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.
- Information about medical or health conditions, including whether or not you have a disability for which the company needs to make reasonable adjustments.
  Information about why you left the company, for example exit interview and resignation confirmation letter.
  Photographs, filming and any other type of image for marketing purposes, for example hard copy brochures or for the website.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Results of HMRC employment status check, details of your interest in and connection with the intermediary through which your services are supplied.

Data is stored in your personnel file within the HR system and in other IT systems, including your company email.

How is your personal information collected??

We collect personal information about candidates from the following sources:

- You, the candidate.
- Recruitment agency, from which we collect categories of data that commonly appear on CVs.
- 3rd party companies such as Disclosure and Barring Service in respect of criminal convictions and CIFAS – fraud check.
- Your named referees.
- Data from third parties is from a publicly accessible source such as LinkedIn
- Trustees or managers of pension arrangements operated by a group company.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

Why and how does Momenta process your personal data?

Our basis for processing your personal data may rely upon our legitimate interest, legal obligation, contractual obligation or consent.

The company needs to process your data to complete the recruitment process with the objective of entering into an employment contract. The data is collected on the basis of consent so that we can ascertain whether you are the most appropriate individual for the position. This will involve pre-vetting checks in accordance with the company's Recruitment Policy. Processing this data allows the company to provide you with an offer of employment.

The company has a contractual requirement to process data to enter into an employment contract with you and to meet its obligations under this contract. For example, to pay you in accordance with your employment contract and to administer employee benefits, including your pension.

In addition, the company needs to process data to ensure 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, the company has a legitimate interest in processing personal data in respect of employees before, during and after the end of the employment relationship. Processing employee data allows the company to:

- Making a decision about your recruitment or appointment
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency) including employee contractual and statutory rights.
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK/Australia
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs)
- Operate and keep a record of disciplinary and grievance processes, or a change in your criminal record, to ensure acceptable conduct within the workplace.
- Operate and keep a record of employee performance and related processes, to plan career development and for succession planning and workforce management purposes.
- Run recruitment and client promotion processes.
- Operate and keep a record of absence and absence management procedures, to allow effective workforce management, for example fitness to work and ensure that employees are receiving the pay or other benefits to which they are entitled.
- Making decisions about salary reviews and compensation***.
- Assessing qualifications for a particular job or task, including decisions about promotions*.
- Obtain occupational health advice, to ensure it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law and ensure employees are receiving the pay or other benefits to which they are entitled.
- 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 the company complies with its duties in relation to leave entitlement and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- Inviting you to participate in any share plans operated by a group company.
- Granting awards under any share plans operated by a group company.
- Administering your participation in any share plans operated by a group company, including communicating with you about your participation and collecting any tax and NICs due on any share awards
- Enrolling you Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Providing benefits to you and liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits.
- Education, training and development requirements.
- Complying with health and safety obligations.
- To prevent fraud.
- Ensure effective general HR and business administration including accounting and auditing.
- Provide references on request for current or former employees.
- Respond to and defend against legal claims.
- Making decisions about your continued employment or engagement and making arrangements for the termination of our working relationship.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution

- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.

Where the company relies on legitimate interest as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded they are not.

We will always gain your freely given, specific, unambiguous explicit and informed consent for any sharing of photographs or images on marketing materials (hard copies, soft copies or on the website) or for sharing your personal data with any third-party clients for the purposes of marketing or proposals.

Special Category Data

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance.
- If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This

will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about Community members or former members of our Community and former employees in the course of legitimate business activities with the appropriate safeguards.

We envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences for security reasons and checking suitability for certain posts, for example IT posts which come with full administrative privileges.

We are allowed to use your personal information in this way to this end. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Your rights

Whenever we process your personal data, we take reasonable steps to ensure your data is kept accurate and up-to date for the purposes for which it was collected. As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request.
- Require the company to change incorrect or incomplete data.
- Require the company to delete or stop processing your data where the data is no longer necessary for the purposes of processing.
- Object to the processing of your data where the company is relying on its legitimate interests as the legal ground for processing.
- Withdraw consent on which the processing is based, and where there is no other legal ground for processing.
- Ask the company to stop processing data for a period if the data is inaccurate or there is a dispute about whether or not your interests override the company’s legitimate grounds for processing data.

Should you wish to obtain a copy (free of charge) of the personal data being processed, the company is required to respond to your request within one month from receipt of the request. For added security, we may ask you to provide proof of your identity before releasing any data. All requests can be sent via email dpo@momentagroup.com or to the following address:

Momenta Interim Management Limited
10 Lower Thames Street
London
EC3R 6EN
Telephone: 020 7374 6600

What if you do not provide personal data?

You have some obligations under your employment contract to provide the company 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 the company with data in order to exercise your statutory rights (statutory leave entitlements, for example). Failing to provide the data may mean you are unable to exercise your statutory rights.

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

Who has access to your data?

We will only share your personal information with the following third parties for the purposes of processing your application including:

Employment agencies, for the purpose of explaining outcomes and/or progressing your application.

Ex-employers for pre-employment references from other employers and providers.

Fraud check. Cifas will use the data to prevent fraud, other unlawful or dishonest conduct, malpractice and other seriously improper conduct. If any of these are detected, you could be refused certain services or employment. Your personal information will also be used to verify your identity. Further details of how your information will be used by us and Cifas, and your data protection rights, can be found in the company's Fraud Policy.

Vetting and onboarding processing including a Disclosure and Barring Service check (Criminal Record check) and credit check.

Other group companies if we think that you may wish to know or progress opportunities with them or if we are processing data as part of your employment contract. In the majority of cases your data will be stored and processed by employees working in a different group company to the one you are applying to work within.

As an employee, Momenta may use the following third-party providers, in conjunction with TCC to process your data on our behalf:

- HR Information System and payroll processing
- Benefit providers: Pension Provider, Death in Service benefits, Private Medical Insurance, Income Protection Scheme and Health Cash Plan
- Vetting check providers on Fraud, right to work and credit check
- Backup systems provider
- Purchasing, invoicing, timesheets and payroll processing
- Accounting and banking:
- Email and file storage:
- Expenses: Hotel and travel bookings and expense management
- Lawyers: Employment legal advice
- Company clients: for fulfilling the contractual requirement including billing, workflow systems, systems, access and laptop builds where required.
- Third party auditors: Company accountants or auditing for ISO certificates.
- Occupational health consultant(s), GPs and other medical experts: if your health needs to be managed in the context of a return to work or where we need to consider reasonable adjustments to your role.
- The UK's Fit for Work programme, in the event that you become unwell and your health needs to be managed in the context of a return to work.

Where necessary, your information will be shared internally with Finance, your line manager, managers in the business area in which you work and IT staff, if access to the data is necessary for performance of their roles. The information shared is limited to that required for the purposes of the processing.

Momenta may also share limited data about you on the company's website and with prospective

clients for the purposes of tendering for new contracts and marketing.

The company will ensure that any third-party processor has adequate data protection measures in place that align with GDPR requirements by conducting periodic due diligence.

The company will not use any third-party processor outside of the UK and EU. The data storage and processing systems are protected by access controls, to minimise any risk to the integrity or security of your personal data, and the data is stored in servers in the UK and EU.

The company does not sell your personal data or other information to any third party.

Employees working on contracts whereby they are seconded to a client to perform work on behalf of a client

These employees will be working on site on behalf of another Momenta Group Company (usually Momenta Customer Services Limited). In this case, Momenta will need to share some of your personal data with its client. This is because day to day supervision of your work and management of you on site is undertaken by Momenta's client. In turn, Momenta's client will need to regularly manage the following; and therefore may share the following data with Momenta.

- Your arrival and departure times.
- Your performance on site.
- Any issues with your performance or conduct on site and management of the same.
- Any absenteeism and the reason for it.
- Holiday requests and dates.
- Management of any health conditions that may require reasonable adjustments to be put in place.
- Reasons for offboarding.
- Reference information.
- Momenta Interim Management Limited

The above is necessary in order to give effect to the contract you have with Momenta.

Momenta has however reviewed the sharing of this information with data protection principles in mind. Specifically, it has made an arrangement to allow its client very limited access to your identity data (name, address), your contact data (name, email), your holiday entitlement and your sickness absence record. It only allows access to its client's managers and only for the purpose of managing your placement.

If you have any questions or queries about the extent to which data is shared, please raise them with our Data Protection Officer.

Retention period

Momenta will only keep your personal data for as long as necessary for the purposes for which it was collected. This varies depending on the nature of your relationship with the company:

- Prospective employees. The company will hold your personal data for the purposes of the recruitment process, and where this does not result in employment your data will be held for up to 121 months for future employment in line with the company's Data Controls Policy. At the 12-month period your data will be deleted.
- Employees: The company will hold your personal data for six years after the end of your employment contract in line with the Retention Policy unless a variation is required for legal reasons for example health and safety.

If the personal data is no longer necessary, or where we no longer have the legal basis for processing,

we will delete or fully anonymise the data we hold on you, in line with our Data Protection Policy. If during your employment we become aware your data has become inaccurate, we will update it accordingly.

Exception for Australian employees or UK employees working in Australia

In the case of Australian employees or UK employees working in Australia, we do transfer personal information we collect about you to Australia in order to perform our contract with you.

However, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with, and which respects the EU and UK laws on data protection:

We have put in place binding corporate rules for data transfers affecting our Australian staff members.

If you require further information about these protective measures, you can request it from our Data Protection Officer at dpo@momentagroup.com

How do we protect your data?

The company takes the security of your data seriously. The company has internal policies and controls in place to try to ensure your data is kept securely to protect against accidental or unlawful destruction, loss, alteration, disclosure or access and is not accessed except by its employees in the performance of their duties.

The policies and controls include:

- IT Security Policy
- Access Control policy
- Anti-virus controls and firewalls
- Risk Management Framework.
- Data Loss Prevention.

Where the company 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 the data.

Automated decision making

Employment and recruitment decisions may incorporate, but are not based solely on automated decision making.

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request reconsideration.
- Where it is necessary to fulfil the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified, in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Your duty to inform us

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

If you wish to complain

The company will be more than happy to help you should you have any complaints about the processing of your personal data. If you have any queries about this privacy notice, or should you wish to make a complaint, please email dpo@momentagroup.com. In addition, you have the right to lodge a complaint with the Information Commissioner's Office (ICO), which is the national authority responsible for the protection of personal data. A complaint can be made to the ICO via its website: ico.org.uk or through its helpline: 0303 123 1113.

Do you use the company website and/or receive email communications from the company?

If so, you should read our website Privacy Statement, which sets out how we will process your data in order to effectively communicate with you and enable you to use our website.

Changes to this Privacy Notice

We reserve the right to change this Privacy Notice. The up-to-date version will be on the company website. We recommend that you check this notice regularly so that you are informed of any changes.

Head Office
TCC Group and Recordsure
6th Floor, 10 Lower Thames Street
London, EC3R 6EN

T_+44 (0)203 772 7230
E_ hello@tcc.group | info@recordsure.com
W_ tcc.group | recordsure.com