1. PURPOSE

This Privacy Notice explains how EMR Group Limited and its group companies ("EMR Group", "we", "us", "our") collect, use, store and share ("process") personal data relating to employees, workers, contractors, agency staff, volunteers, directors and applicants.

We are committed to processing personal data fairly, lawfully and transparently in accordance with data protection law including, in the UK, the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2. WHO WE ARE

2.1 EMR Group

The employing EMR Group entity is the data controller of your personal data.

For UK employees, this will typically be:

EMR Group Limited
Sirius House
Delta Crescent
Westbrook
Warrington
WA5 7NS
United Kingdom

Email: dpo@emrgroup.com

Its holding company Ausurus Group Ltd, and all of its subsidiaries, including (but not limited to):

- EMR BV
- EMR GmbH
- EMR Polymers Limited
- Innovative Environmental Solutions UK Limited
- EMR SRL
- EMR Switzerland GmbH

Each EMR Group company acts as a data controller in respect of personal data it processes.

3. WHO THIS NOTICE APPLIES TO

This notice applies to:

- Employees (permanent and fixed-term)
- Workers, contractors, consultants and associates
- Agency staff, casual workers, temporary staff and volunteers
- Directors and officers
- Job Applicants and Candidates
- Former workers, where relevant

4. ABOUT THIS DOCUMENT

Where relevant, parts of this notice may also apply to prospective applicants and former workers, although separate or additional privacy information may be provided to those individuals when their personal data is collected.

We also maintain related policies and notices that provide additional information about how personal data is used in specific contexts (for example, monitoring, IT systems, and record keeping).

This Privacy Notice is the primary document explaining how EMR Group processes your personal data. It does not form part of your contract of employment.

We may also provide additional privacy information at the point we collect personal data where appropriate.

5. HOW WE COLLECT YOUR PERSONAL DATA

We collect personal data in a variety of ways, including:

- directly from you (for example through applications, interviews, correspondence)
- from third parties (such as recruitment agencies, the Disclosure and Barring Service (DBS), other background check providers, referees, pension and benefits providers, occupational health services, insurers, public sources (such as LinkedIn or other websites and regulators) through the provision and updating of personal details within HR systems
- during recruitment activities, including applications submitted through our careers website, recruitment systems, recruitment agencies, interviews, assessments and pre-employment screening processes
- during your employment or engagement, including by filing reports, note taking, completion of paperwork regarding performance reviews, ongoing training, and day-to-day use of EMR systems (for example IT systems, access controls, and CCTV)
- through your interactions with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below
- from customers, suppliers or other third parties where relevant to your role

6. THE TYPES OF PERSONAL DATA WE COLLECT

6.1 Ordinary personal data

This may include:

- Identity data: name, title, date of birth, gender, nationality, photographs (such as staff ID card), Copies of passports or other photo ID, copies of proof of address documents (such as bank statements or utility bills),
- Contact data: home address, telephone numbers, email addresses and emergency contacts
- Family data: next of kin and dependents information
- Recruitment data: CVs, application forms, interview notes, assessment results, psychometric test results (where used), references, right-to-work documentation, recruitment correspondence, salary expectations and pre-employment screening information
- Employment data and operational data: job title, role, start date, work location, working arrangements, performance records, training records, certifications, disciplinary and grievance records, leaving details
- Financial and tax data: bank account details, payroll records, tax status, National Insurance number, pension and benefits information
- IT and monitoring data: system usage logs, access records, CCTV footage, swipe card data

6.2 Special category data

Where necessary, we may process special category personal data in accordance with applicable data protection law and only where there is a valid legal basis to do so. This will typically be where the processing is necessary for employment law obligations, health and safety requirements, equality monitoring, or the establishment, exercise or defence of legal claims.

Special category data may include:

- Health and medical information (including sickness absence)
- Racial or ethnic origin
- Religious or philosophical beliefs
- Sexual orientation

- Trade union membership

Provision of equality, diversity and inclusion information is voluntary unless required by law, and individuals may choose not to provide this information.

In limited circumstances, we may also process additional sensitive personal data where this is necessary for specific purposes, such as internal investigations, grievance or disciplinary processes, safeguarding, or legal claims. Any such processing will be limited to what is relevant and necessary for the purpose, subject to appropriate safeguards, and carried out in accordance with applicable data protection law.

Where appropriate, this data will be anonymised or used in aggregated form, particularly in relation to equality monitoring.

6.3 Criminal offence data

Where required for your role or by law, we may process information relating to criminal convictions, allegations or background checks (for example DBS checks).

7. HOW AND WHY WE USE YOUR PERSONAL DATA

We only process your personal data where we have a lawful basis to do so.

7.1 Lawful Bases

- Contract – to perform your employment or engagement contract
- Legal obligation – to comply with applicable laws and regulations
- Legitimate interests – to operate and protect our business
- Recognised legitimate interests – for certain processing activities specified in law (such as disclosures to public authorities and regulators, crime and fraud prevention, and safeguarding), where the legitimate-interests balancing test does not apply
- Vital interests – in emergency situations
- Consent – where required and appropriate (such as optional use of employee images or participation in voluntary initiatives)

7.2. Purpose of Processing

We use your data for:

- Recruitment, onboarding and right-to-work checks
- Payroll, benefits, pensions and expenses
- Performance management, training and development
- Managing attendance, absence and working arrangements
- Health and safety compliance
- Disciplinary, grievance and investigation processes
- IT, network and physical security
- Workforce planning, reporting and analytics
- Legal compliance, dispute resolution and regulatory reporting
- Business continuity and emergency contact purposes

7.2.1 Recruitment and Candidate Data

Where you apply for a role with EMR Group, we may process your personal data to:

- assess your suitability for employment or engagement
- communicate with you regarding recruitment opportunities
- verify qualifications, experience and references
- undertake right to work checks and other pre-employment checks where appropriate

- maintain records relating to recruitment decisions
- establish, exercise or defend legal claims arising from recruitment activities

Where we would like to retain your personal data for future employment opportunities beyond the conclusion of a recruitment process, we will seek your consent to include your details within a candidate talent pool.

Providing consent is entirely voluntary and will not affect your application. You may withdraw your consent at any time by contacting us. Where consent is withdrawn, your personal data will be removed from the talent pool unless we are required to retain it for another lawful purpose.

7.3. Legitimate Interests

Our legitimate interests include:

- Ensuring effective business operations
- Maintaining security of systems and premises
- Preventing fraud and misconduct
- Managing workforce performance and planning

Where we rely on legitimate interests, we consider and balance those interests against your rights. Where we rely on a recognised legitimate interest specified in law, that balancing exercise is not required, but the processing must still be necessary for the relevant purpose.

8. SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA – ADDITIONAL GROUNDS

We only process special category and criminal offence data where an additional legal condition applies, including:

- Employment and health & safety obligations
- Assessing working capacity
- Equal opportunities monitoring
- Preventing or detecting unlawful acts
- Establishing, exercising or defending legal claims
- Substantial public interest
- Protecting vital interests where consent cannot be given

Where we process special category or criminal offence data in reliance on a condition in Schedule 1 to the Data Protection Act 2018, we maintain an Appropriate Policy Document setting out our compliance and retention measures, which is available on request.

9. MONITORING

We carry out proportionate monitoring where necessary for legitimate business purposes, including:

- CCTV at EMR premises (security and safety)
- Access control systems
- Monitoring use of IT and communications systems in accordance with EMR policies

The lawful basis for monitoring is our legitimate interests in protecting our business, employees and assets, and compliance with legal obligations and EMR Group Policies.

10. AUTOMATED DECISION-MAKING

We do not make decisions based solely on automated processing that have legal or similarly significant effects, including profiling.

11. DATA SHARING

We may share your personal data with:

- Payroll, pension, benefits and expenses management providers
- IT service providers and system administrators
- Professional advisers (legal, audit, insurance)
- Regulators and public authorities (e.g. HMRC)
- Occupational health providers
- Group companies where necessary
- Training providers

All third parties are required to respect the security of your data and process it lawfully under contractual controls.

11.1 Joint data controllers

EMR Group companies may act as joint data controllers where they jointly determine the purposes and means of processing personal data, including through shared HR, payroll, benefits, information technology and other group-wide services.

Where joint controller arrangements exist, the relevant organisations will work together to ensure compliance with applicable data protection laws and to facilitate the exercise of individuals' rights.

Individuals may exercise their data protection rights through the contact details provided in this Privacy Notice, regardless of which EMR Group company is responsible for the processing activity.

Further information regarding the processing of personal data within EMR Group is available from the Data Protection Officer upon request.

12. INTERNATIONAL TRANSFERS

Where personal data is transferred outside the UK, EMR Group ensures appropriate safeguards are in place, including:

- UK adequacy regulations
- The UK International Data Transfer Agreement (IDTA)
- The UK Addendum to EU Standard Contractual Clauses
- Intra-group data transfer agreements

Further details are available on request.

13. HOW WE STORE YOUR DATA

Personal data is stored on secure IT systems (including cloud-based systems and internal servers) and access is restricted to authorised personnel on a role-based basis. We apply appropriate technical and organisational security measures, including access controls, logging and monitoring, encryption where appropriate, and security controls designed to protect personal data from unauthorised access, loss, alteration or disclosure.

14. DATA RETENTION AND DISPOSAL

We retain personal data only for as long as necessary for the purposes for which it was collected, including to meet legal, regulatory and business requirements.

Retention periods are determined based on the type of data, the purpose for which it is processed, applicable legal obligations, and the need to retain information for the establishment, exercise or defence of legal claims.

Typical retention periods include:

- **Recruitment data** (such as CVs, application forms, interview notes and assessment outcomes): generally retained for up to 2 years from the end of the recruitment process

- **Candidate data retained for future opportunities** (talent pooling): retained for up to 2 years where the individual has provided consent
- **Equality and diversity data collected during recruitment:** retained for a limited period and, where possible, anonymised or aggregated for reporting purposes
- **Employment records:** generally 7 years after termination, unless a longer period is required by law or for legal claims
- **Health and safety or exposure records:** up to 40–50 years where legally required (e.g. in relation to industrial disease or injury or exposure risks)

Where specific retention periods cannot be defined, we apply retention criteria based on the nature, sensitivity and purpose of the data, and any applicable legal or regulatory requirements.

When personal data is no longer required, it is securely deleted, anonymised or destroyed in accordance with our Records Retention Policy. This includes applying appropriate deletion methods across relevant systems and ensuring that data held in backups is retained only in line with defined retention cycles and is not restored unless required.

15. CONSEQUENCES OF NOT PROVIDING DATA

If you do not provide certain personal data when requested, we may not be able to progress your application, perform your employment contract, comply with legal obligations, or provide certain benefits or services.

16. YOUR RIGHTS

You have the following rights under UK data protection law:

- Right of access to your personal data
- Right to rectification of inaccurate data
- Right to erasure (in certain circumstances)
- Right to restrict processing
- Right to object to processing
- Right to data portability
- Right to withdraw consent (where applicable)

You are not required to pay any charge for exercising your rights. We will respond within one month of receiving your request. Where requests are complex or numerous, we may extend this period by up to two further months and will let you know if this is the case. Where we reasonably require further information to confirm your identity or to clarify your request, the one-month period will not begin until we have received that information.

To exercise your rights, contact Data Protection Officer: dpo@emrgroup.com

17. COMPLAINTS

If you have concerns about how we handle your personal data, you may raise them with us by contacting our Data Protection Officer at dpo@emrgroup.com. We will acknowledge your complaint within 30 days of receiving it and will keep you informed of the outcome without undue delay. We encourage you to contact us first so that we can try to resolve your concern.

In the UK you also have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Textphone: 18001 0303 123 1113
www.ico.org.uk

18. UPDATES TO THIS NOTICE

We may update this Privacy Notice from time to time. Where appropriate, we will notify you of any significant changes.

19. CONTACT

For any questions about this notice or your personal data:
Email: dpo@emrgroup.com

20. APPROPRIATE POLICY DOCUMENT (SPECIAL CATEGORY AND CRIMINAL OFFENCE DATA)

This section is EMR Group's Appropriate Policy Document (APD) for the purposes of Schedule 1 to the Data Protection Act 2018 (DPA 2018). It explains how EMR Group complies with the principles in Article 5 of the UK GDPR, and sets out our retention and erasure policies, when we process special category data (Article 9 UK GDPR) and criminal offence data (Article 10 UK GDPR) in reliance on the Schedule 1 conditions that require an APD to be in place. It is maintained as an accountability record under Schedule 1, Part 4 of the DPA 2018 and is available to the Information Commissioner on request.

20.1 Scope

This APD applies to EMR Group's processing of special category data (described in Section 6.2) and criminal offence data (described in Section 6.3) relating to the individuals identified in Section 3 — employees, workers, contractors, agency staff, volunteers, directors, applicants and, where relevant, former workers. We process such data only where we have an Article 6 lawful basis, a condition under Article 9 or Article 10 of the UK GDPR, and (where required) a condition in Schedule 1 to the DPA 2018.

20.2 Conditions for processing relied upon

The table below sets out the principal purposes for which EMR Group processes special category and criminal offence data, the relevant condition under Article 9 or Article 10 of the UK GDPR, and the corresponding condition in Schedule 1 to the DPA 2018. Where the Schedule 1 condition relied upon requires an Appropriate Policy Document, this document satisfies that requirement.

Processing purpose	Category of data	UK GDPR condition	DPA 2018 Schedule 1 condition
Administration of the employment relationship — sickness absence, occupational health, reasonable adjustments, pensions and statutory/family leave	Health data; trade union membership (where applicable)	Article 9(2)(b)	Part 1, para 1 — employment, social security and social protection
Equality, diversity and inclusion monitoring	Racial or ethnic origin; religion or belief; health/disability; sexual orientation	Article 9(2)(g)	Part 2, para 8 — equality of opportunity or treatment
Investigations, disciplinary and grievance processes, and the prevention or detection of unlawful acts	Special category data; criminal offence data	Article 9(2)(g); Article 10	Part 2, para 10 — preventing or detecting unlawful acts
Prevention of fraud	Special category data	Article 9(2)(g)	Part 2, para 14 — preventing fraud
Safeguarding of young people on placements/ apprenticeships and other individuals at risk	Health and other special category data	Article 9(2)(g)	Part 2, para 18 — safeguarding of children and of individuals at risk
Criminal record / DBS checks for eligible roles	Criminal offence data	Article 10	Part 1, para 1 (employment), and/or processing under official authority
Establishing, exercising or defending legal claims	Special category and criminal offence data	Article 9(2)(f); Article 10	Article 9(2)(f) requires no APD; criminal offence data under Schedule 1, Part 3

20.3 Compliance with the data protection principles

EMR Group secures compliance with the principles in Article 5 of the UK GDPR in relation to special category and criminal offence data as follows:

- Lawfulness, fairness and transparency — we identify an Article 6 lawful basis, an Article 9 or Article 10 condition and (where required) a Schedule 1 condition before the processing begins, and we explain our processing to individuals in this Privacy Notice.
- Purpose limitation — we process special category and criminal offence data only for the specified purposes set out in paragraph 20.2, and not in any manner incompatible with those purposes.
- Data minimisation — we limit such data to what is relevant and necessary for the purpose; equality and diversity data is anonymised or aggregated wherever possible.
- Accuracy — we take reasonable steps to keep this data accurate and up to date, and we rectify or erase inaccurate data without undue delay.
- Storage limitation — we retain this data only for as long as necessary, in accordance with Section 14 and paragraph 20.4 below.
- Integrity and confidentiality (security) — we apply appropriate technical and organisational measures, restrict access to authorised personnel, and impose confidentiality obligations on those who handle the data.
- Accountability — we maintain records of processing under Article 30, carry out data protection impact assessments where processing is likely to be high risk, keep this APD under review, and our Data Protection Officer oversees compliance.

20.4 Retention and erasure

EMR Group retains special category and criminal offence data only for as long as necessary for the purposes for which it is processed, in accordance with the retention periods and criteria set out in Section 14 (Data Retention and Disposal). In particular:

- Health, occupational health and exposure records are retained in line with statutory requirements, including the long retention periods for health, safety and exposure records described in Section 14.
- Equality and diversity monitoring data is retained for a limited period only and is anonymised or aggregated wherever possible.
- Criminal record and DBS check information is retained only for as long as necessary to make the relevant suitability decision and is then securely deleted unless a legal obligation requires it to be retained.

When this data is no longer required, it is securely deleted, anonymised or destroyed in accordance with our Records Retention Policy, including in respect of data held in backups.

20.5 Review, retention of this document and availability

This APD is kept under review and updated as necessary to ensure it remains accurate and current. In accordance with Schedule 1, Part 4 of the DPA 2018, EMR Group will retain this document until at least six months after the relevant processing ceases, will review it during that period, and will make it available to the Information Commissioner on request without charge. Our records of processing under Article 30 of the UK GDPR record the Schedule 1 condition relied upon, how the processing satisfies Article 6, and whether the data is retained and erased in accordance with the policies described above.