

DirectMed Imaging
Privacy Notice for UK, EEA and California Staff and Third Parties
Last Updated: February 12, 2025

DirectMed Imaging, LLC together with their subsidiaries and affiliates (“DirectMed”, “we” “us” “our”) is committed to protecting the privacy and security of your personal information.

It is important that you read this policy, together with any privacy notice we may provide on specific occasions when we are collecting or processing your personal information.

What is the purpose of this document?

This policy describes how we process personal information of our past, current and/or prospective employees, workers, applicants, candidates, interns, agency workers, consultants, individual contractors, or directors (together, “**staff**” or “**you**”) and any third parties whose information staff provide to us in connection therewith (for example, in respect of dependents, partners, dependants, beneficiaries or emergency contacts) (together, “**Third Parties**”).

This policy applies to staff and Third Parties who are residents of the UK, EEA, or California. We are providing this privacy policy because we are required to do so by law, and because the laws in the UK, EEA, and California provide specific privacy rights to staff and Third Parties. Please note that for California residents, this policy does not apply to information excluded from the scope of the law mandating this disclosure. This includes information subject to California and federal laws governing the privacy of health, financial and consumer report information, such as HIPAA, GLBA and FCRA.

DirectMed will collect and process personal information relating to staff and Third Parties prior to your commencement as a staff member and throughout your employment or engagement with us as set out in this policy.

Where we refer to “**employment**” or “**engagement**” in this policy, we do so for convenience only, and this should in no way be interpreted as purporting to confer employment status on non-employees to whom this policy also applies. This policy does not form part of any contract of employment or engagement, does not confer any employment status on you and does not confer any contractual right on staff or Third Parties, or place any contractual obligation on us.

This policy applies to all personal information collected, maintained, transmitted, stored, retained, or otherwise used (i.e., processed) by us regardless of the media on which that personal information is stored. We may update this policy from time to time. If we make material changes to this policy, we will post it to, as applicable, our employee handbook and applicable sections of our website at the time of the change becoming effective.

The Company is a “**data controller**” or “**business**”. This means that we are responsible for deciding how we hold and use personal information about staff and Third Parties.

The types of personal information we process

Personal information, or personal information, means any information about an individual from which that person can directly or indirectly be identified. It does not include data where the person is no longer identifiable (anonymous data).

We will collect, store, and use the following categories of personal information about you:

Personal details: Name, title, employee identification number, work and home contact details (email, phone numbers, physical address), languages(s) spoken, gender, date of birth, National Identification Number, Social Security Number or local equivalent, marital/civil partnership status and dependants, domestic partners, disability status, emergency contact information (for you and any next of kin) and photographs.

Recruitment: Recruitment information (including copies of right to work documentation, references and other information included in a résumé, CV or cover letter or as part of the application process), previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates, information necessary to complete a background check.

Documentation required under immigration laws: Citizenship, passport data, details of residency or work permit.

Compensation and payroll: Base salary, annual leave, pension, benefits, bonus, compensation type, commission plan, salary step within assigned grade, details on stock options, stock grants and other awards, currency, pay frequency, effective date of current compensation, salary reviews, bank account details, payroll records and tax status information, National Insurance number, Social Security number or local equivalent, working time records (including annual leave and other absence records, leave status, hours worked and department standard hours), pay data and termination date.

Position: Employment records (including job titles, work history, working hours, training records and professional memberships), description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, job functions, company name and code (legal employer entity), branch/unit/department, location of employment or workplace, employment status and type, full-time/part-time, terms of employment, employment contract, work history, start, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, date of transfers, and reporting manager(s) information.

Talent management information: Compensation history, performance information and history, development programs planned and attended, e-learning programs, performance and development reviews, disciplinary and grievance information, and information used to populate employee biographies.

Management records: Details of any shares of common stock or directorships.

System and application access data: CCTV footage and other information obtained through electronic means such as swipecard records, information about your use of our information and communications systems, information required to access company systems and applications such as System ID, LAN ID, email account, instant messaging, mainframe ID, previous employee ID, previous manager employee ID, system passwords, employee status reason, branch state, country code, previous company details, previous branch details, previous department details, and electronic content produced by you using company systems.

Family information: Next of kin and emergency contact information (which is only held for the purposes of contact such as in the event of a medical emergency or in the context of absence).

Sensitive information:

Please note that we may process more sensitive personal information, such as:

Social Security number and other forms of government identification;

Information about gender, race or ethnicity; and

Information about health, including any medical condition, health and sickness records.

We collect this information for specific purposes, such as health/medical information in order to accommodate a disability or illness and to provide benefits, and demographic personal information (such as age, gender, race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination. Please be assured that we will process such sensitive information only for the purposes set out in this policy and as provided by law.

How do we collect personal information?

We collect personal information about staff through our application, recruitment and on-boarding processes, either directly from you or from an employment agency or background check provider. We may sometimes collect additional information from others, including former employers.

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

How we will use information about you

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with our legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of others, provided your interests and fundamental rights do not override those interests. The situations in which we will process personal information are listed below.

Recruitment: Making a decision about whether or not to recruit or employ you. Determining the terms on which you work for us. Checking that you are legally entitled to perform work for us. Performing background checks.

Managing workforce: Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning. Conducting performance reviews, managing performance and determining performance requirements. Making decisions about salary reviews and compensation. Assessing qualifications for a particular job or task, including decisions about promotions. Education, training and development requirements, planning and monitoring of training requirements and career development activities and skills. Managing promotions, transfers, and secondments. To conduct data analytics studies to review and better understand employee retention and attrition rates.

Staff relations and safety: Gathering evidence for possible grievance or disciplinary hearings. Making decisions about your continued employment or engagement. Making arrangements for the termination of our working relationship. Conducting investigations and reviewing employment or engagement decisions. Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work. Ascertaining your fitness to work. Managing sickness absence. Complying with health and safety obligations. Providing references on request. Performing staff surveys.

Payments and benefits: Paying you and, if you are an employee, deducting tax and National Insurance, Social Security or local equivalent contributions, and deducting pay for elected benefits. Providing the benefits to which you are entitled. Liaising with your pension provider. Administering the contract we have entered into with you. Administering awards such as stock options, stock grants and bonuses. Making business travel arrangements and managing business expenses and reimbursements.

Communications and emergencies: Facilitating communication with you, protecting the health and safety of staff and others, safeguarding IT infrastructure, office equipment and other property, facilitating communication with your nominated contacts in an emergency.

Business operations: Business management and planning, including accounting and auditing. Operating and managing the IT and communications systems. Managing product and service development, and improving products and services. Managing our assets, selling or buying business assets, allocating our assets and human resources. Strategic planning. Project management. Business continuity.

Compliance: Compliance with legal and other requirements, such as income tax and National Insurance, Social Security, or local equivalent deductions, record-keeping and reporting obligations. Conducting audits, and compiling audit trails and other reporting tools. Maintaining records relating to business activities. Budgeting, financial management and reporting. Managing mergers, acquisitions, sales, re-organizations or disposals and corporate transactions. To prevent fraud. Equal opportunities monitoring. Compliance with government inspections and other requests from government or other public authorities. Responding to legal process such as subpoenas, and pursuing legal rights and remedies.

Data protection: 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 unauthorized access to our computer and electronic communications systems and preventing malicious software distribution.

Some of the above reasons will overlap and there may be several legal bases for processing which justify our use of your personal information.

If you fail to provide information

If you fail to provide certain personal information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an incompatible purpose, we will notify you and we will explain the legal basis which allows us to do so.

Legal basis and purposes of processing

We will only process your personal information where legally permitted. Sometimes more than one legal basis applies to the processing of the same piece of personal information, depending on the processing activity taking place. We will process your personal information on the following legal grounds:

Performance of our contract with you. Usually, your personal information is processed for the performance of your contract, for purposes such as payroll, accounting, financial bookkeeping, providing retirement or pensions, vacation planning, promotions and succession planning, travel and expenses, sick or parental leave, insurances, and training. In this context, you are obliged to provide us with your personal information, otherwise we will not be able to execute the duties under the contract of employment / engagement.

Our legitimate interest. Another legal basis for processing your personal information is the legitimate interest of the data controller, i.e., DirectMed, which will be the case for intra-group reports and financial planning such as budget, effectivity and cost efficiency of personnel planning, labor management, travel and expenses, providing references, loans, training, defending DirectMed's legal rights, investigating incidents or workplace accidents, documenting and utilizing your work product, operating and protecting our IT and communications systems, managing devices used for work, monitoring compliance with our policies, securing our premises and equipment, managing disciplinary matters, grievances and terminations, building and providing products and services, managing our assets and human resources, planning, project management, maintaining records and reports relating to business activities, financial management and reporting, communications, staff surveys and managing corporate activities such as fundraising, financings, mergers, acquisitions, sales, re-organizations or disposals. Please note that where this basis applies, we will consider the risk to you as an individual as against the legitimate interest of the data controller.

Legitimate interest of other entities. This can also provide the basis of processing your personal information, e.g., customers, affiliated companies or other stakeholders for example in cases of fraud prevention, the enforcement of legal entitlements or the accounting for stock options.

Compliance with a legal obligation. Processing can in some cases be necessary for compliance with a legal obligation, such as answering requests from legal authorities or defending DirectMed against legal claims or disputes. We process your personal information for the legal obligations of paying income taxes and social contributions, paying pensions and retirement plans if applicable, compliance with audits and other government inspections, record overtime, incidents, working conditions and legal files, maintaining compliance with policies by the workforce as well as documentation of details of transports.

Staff consent. While we do not need your consent if the relevant processing is based on one of the grounds (a) to (d) above, if we require your consent for processing your personal information, 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 and you may refuse to give your consent.

Sensitive personal information

Sensitive personal information requires higher levels of protection. Depending on your jurisdiction, we need to have further justification for collecting, storing and using this type of data.

We will only process sensitive personal information where the law allows us to do so. Below, we describe specific uses for certain sensitive personal information we collect.

We will use information relating to leaves of absence, which may include sickness absence or family related leaves, for carrying out obligations or specific rights with regard to employment, social security and social protection 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, subject to appropriate confidentiality safeguards.

We will use information about your gender, race, and ethnicity, to ensure meaningful equal opportunity monitoring and reporting or to comply with legal and/or regulatory requirements. Staff members are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

Less commonly, we may process this type of information where it is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity or where it is needed to protect your interests (or someone else's interests) and you or a third party are not capable of giving your consent, where you have already made the information public, or for reasons of substantial public interest.

Automated decision-making

We do not envisage that any decisions will be made about you using automated means, however we will inform you by posting an update to this policy or informing you in writing (including via email) if this position changes.

Data sharing

We may share personal information with other entities, including service providers and other entities in the Group. We require service providers to respect the security of personal information and to treat it in accordance with the law. We may transfer personal information outside of the jurisdiction in which we collect it, including, for EEA and UK employees, to the United States and other countries. We will only transfer personal information to another country in accordance with applicable data protection laws and provided there is adequate protection in place for the data.

We may also share personal information with other entities at your direction, such as with benefit providers with which you have a direct relationship. These entities are “controllers” or “businesses” in handling your personal information, and their processing of your personal information is subject to their own privacy policies, which you should review carefully prior to directing us to share your information with them.

Why might you share my personal information with other entities?

We will share your personal information with other entities where required by law, where it is necessary to administer the working relationship with you, where you direct us to do so, or where we have another legitimate interest in doing so.

Which third-party entities process personal information?

Professional advisors: Accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors.

Benefits and Human Resources Service Providers: Benefits, payroll and equity management providers and administrators, training program operators and systems, background check providers, recruiting and hiring service providers and systems, and human resource service providers and systems.

Other entities: Other third party service providers or systems that DirectMed utilizes in order to operate its business in the normal course, such as internal and customer-facing collaboration tools, word processing and business tools, security tools, education tools, and compliance systems.

Public, governmental and regulatory authorities: Entities that regulate or have jurisdiction over DirectMed such as regulatory authorities, law enforcement, public bodies, and judicial bodies.

We may share personal information with other entities, for example with our customers or in the context of the possible sale or restructuring of the business. We may share personal information with a regulator or to otherwise comply with the law.

We do not sell personal information or disclose personal information to third parties for targeted advertising. We do not sell your personal information as we understand the term sale to be defined by the California Consumer Privacy Act.

How secure is personal information with third-party service providers?

All our professional advisors and third-party service providers are required to take appropriate security measures to protect personal information in line with our policies, as are any parties to corporate transactions. We only permit them to process personal information for specified purposes and as appropriate, in accordance with our instructions.

The transfers set out above may involve transfers overseas among the following countries: the USA, Denmark and countries in the European Economic Area. To help provide an adequate level of protection for personal information, we have put in place appropriate measures to require those entities to treat personal information in a way that is consistent with and which respects applicable data protection law. These include agreements and commercial terms which contain relevant protections and place appropriate obligations on entities which have access to or receive personal information.

When might we share personal information with other entities in DirectMed?

DirectMed currently operates in the USA, Denmark and countries in the European Economic Area.


We will share personal information with other entities in our Group based on our legitimate interests (i) as part of our regular reporting activities related to performance, (ii) in the context of a business reorganization or group restructuring exercise, (iii) for system maintenance support and hosting of data, and (iv) in order to perform our contract with you. We may share personal information with a group at a regulator's instruction or to otherwise comply with the law.

We may transfer the personal information with Group entities in the following countries:

USA, Denmark; and Countries in the European Economic Area.

How secure is personal information with other entities in DirectMed?

All entities in DirectMed are required to take appropriate security measures to protect personal information in line with our policies, as are any parties to corporate transactions. We only permit them to process personal information for specified purposes and as appropriate, in accordance with our instructions.

There is no adequacy decision by the European Commission in respect of the USA and . This means that these countries to which we transfer your data are not deemed to provide an adequate level of protection for personal information under the GDPR. There is an adequacy decision by

the European Commission in respect of Canada. This means that Canada is deemed to provide an adequate level of protection for personal information under the GDPR.

Data security

DirectMed takes the security of HR-related personal information seriously. We have put in place appropriate security measures designed to protect personal information from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed.

HR-related personal information held in personnel files, HR systems, and HR files are stored securely, and we limit access to personal information to those staff members, agents, contractors and others who have a business need to access this data in the proper performance of their duties. We require everyone to only process personal information on our instructions and subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security incident and will notify you and any applicable regulator of a suspected breach where we are legally required or it is appropriate to do so.

Data retention

We will only retain personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements, after which it will be deleted or archived except to the extent that it is necessary for us to continue to process it for the purpose of compliance with our legal obligations or for another legitimate and lawful purpose. To determine the appropriate retention period for personal information, we take a number of factors into account.

In some circumstances, we may anonymize personal information so that it is no longer identifiable, in which case we may freely use such information for any purpose without further notice to you.

Candidate personal information will be retained to the extent necessary to enable DirectMed to comply with any legal obligations or for the exercise or defense of legal claims following the application process. Unsuccessful candidates' personal information will be stored for up to six years then destroyed securely and safely in accordance with our legal obligations.

We will normally keep your personnel file throughout the time that you work for us and for up to six years after you leave, after which it will be destroyed unless there is a good reason to keep it (or any part of it) for longer (for example, for the purposes of compliance with our obligations relating to audits or tax or as required in connection with potential litigation or per applicable law).

Staff monitoring

DirectMed may carry out monitoring of its employees, in accordance with its employee monitoring policy in the Employee Handbook. DirectMed will ensure that any personal information generated by this monitoring is treated in accordance with this privacy policy.

Your obligations

Your obligation to inform us of changes

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.

Your obligation to inform Third Parties

You must also inform your dependents whose data you provide to DirectMed about the content of this notice and provide them with a copy of this notice and any relevant policies.

Your Privacy Rights

Your rights in connection with your personal information

You may be entitled to exercise certain data subject rights available under the General Data Protection Regulation, the United Kingdom General Data Protection Regulation, the California Consumer Privacy Act or other privacy laws. Under certain circumstances and depending on your jurisdiction, by law you may have the right to:

- Request information about how we have collected and used your personal information. We have made this information available to you without having to request it by including it in this privacy policy.
- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below);
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and the circumstances of your particular situation mean you wish to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes (including profiling);
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it; and
- Request the transfer of your provided personal information to another party.

Please note, however, that certain personal information may be exempt from such access, correction and deletion requests pursuant to applicable data protection laws or other laws and regulations.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you may have the right to withdraw your consent for that specific processing at any time, depending on your jurisdiction.

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. If we have another legitimate basis in law for processing information, we may still process the same data and we will not require your consent to do so.

Non-Discrimination

You are entitled to exercise the rights described above free from discrimination.

No fee usually required

You will not ordinarily be required to pay a fee to access your personal information (or to exercise any of the other rights), but we may charge a reasonable fee for any additional copies of the materials we provide. Where your request is manifestly unfounded or excessive, we may also charge a reasonable fee or alternatively, we may refuse to comply with the request.

Authorized Agents

If you live in California, you may empower an authorized agent to submit requests on your behalf. We will require authorized agents to confirm their identity and authority, in accordance with applicable laws.

What we may need from you

We may request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Limitations

In some instances, your choices may be limited, such as where fulfilling your request would impair the rights of others, our ability to provide a service you have requested, or our ability to comply with our legal obligations and enforce our legal rights.

Alternative formats for employees with disabilities

Upon request, this notice is available in alternative formats, such as large print, braille, or audio. Please contact sales@directmedimaging.com, and an alternative format will be provided to you so you can access the information in this notice.

How to exercise your right of access or other rights relating to your personal information

If you want to make a request in respect of your rights relating to your personal information, please contact us in writing by emailing us at sales@directmedimaging.com.

Please note that we may be required to ask you for further information in order to confirm your identity before we provide the information requested.

If your request or concern is not satisfactorily resolved by us, UK individuals can contact the [Information Commissioner](#) and EEA individuals can contact their applicable data protection authority.

For Swiss individuals with concerns about our processing of your personal information, you have the right to make a complaint to a data protection supervisory authority. If you are in Switzerland, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner (“FDPIC”). You can visit their webpage at <https://www.edoeb.admin.ch/edoeb/en/home.html>.

Our contact details

DirectMed Imaging, LLC
12525 Stowe Dr,
Poway, CA 92064

Changes to this privacy policy

We reserve the right to update this privacy policy at any time, and we will inform you and provide you with access to the new policy when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy policy, please contact us at sales@directmedimaging.com.