TMC, a Unilabs Company – Global Information Notice

INFORMATION NOTICE OUR PEOPLE (EMPLOYEES AND NON-EMPLOYED STAFF)

Section 1 – Identity and contact details of controller

According to the relevant data protection laws and depending on your clinic's contract and the type of radiologists' services TMC provide, your data will be processed by one of the entities.

EUROPEAN TELEMEDICINE CLINIC, SL, whose registered office is at C/ Marina 16-18, floor 33, 08005 Barcelona, Spain, and Organisation and Tax number: ESB62799689, ("ETMC").

TELEMEDICINE CLINIC Ltd, whose registered office is at Mazars, 45 Church Street, Birmingham West Midlands B3 2RT, UK, and Registration number: 06958314, ("UKTMC").

AUSTRALIAN TELEMEDICINE CLINIC PTY LIMITED, whose registered office is at 13th floor, 25 Bligh Street, Sydney NSW 2000, Australia, and Registration number ABN: 99125092597, ("ATMC").

TELEMEDICINE CLINIC NEW ZEALAND LIMITED, with registered office at BDO Auckland, 4, Graham Street, Auckland Central, Auckland, 1010, New Zealand, Company number: 8595286, ("NZTMC").

Email address: dpo@unilabs.com

Section 2 – What personal data we collect

TMC collects the following personal data related to you:

- **Identification Data:** Name, surname, e-mail address, home address, date of birth, ID card and/or passport number.
- **Professional Data:** Contracts of employment and associated HR records, curriculum vitae, working hours, job title, function, working department, rank, starting date of the current position, seniority, current position, annual leave and public holiday records, emergency contact details.
- **Financial Data:** bank account details, pay details, salary arrangements, bonus payments, allowances, benefits, social security numbers, personal details of spouses and/or defendants which includes marital status, family details for benefits entitlement.
- **Performance Details Data:** performance review, formal notes of performance review meetings, performance improvement plan documentation.
- **Investigation Data:** Copies of any formal employee complaint, formal investigation and/or disciplinary meeting notes, formal witness statements, documented outcomes of any such investigations and/or disciplinary hearings.
- **Technical Data:** Unilabs and TMC email, internet browsing history, TMC mobile & office phone call records, IP Address, Log data.
- **Medical Data:** medical certificates, sick leave records, sick pay records, occupational health assessments.

Section 3 – Purposes of the processing and legal basis

Your personal data will be processed for the following purposes and in accordance with the legal basis as set out below:

Purpose	Legal basis
Personnel file Comply with employment and Revenue laws and to ensure that terms and conditions of employment are properly adhered to and managed as well as to manage planning and organisational structure within Unilabs and TMC.	The processing is necessary to comply with various employment and Revenue laws. The processing is also necessary for the performance of the employment contract. Emergency contact details are collected from employees to protect employees' vital interests in the event of an accident or emergency. Where the individual does not provide the requested data, the organisation may be unable to continue their employment.
Training and Development Provide training and develop our staff.	The processing is necessary for the performance of the employment contract.
Business Trips Management Organise and enable business trips	The processing is in the legitimate interests of TMC to manage trips and mobility of human resources (enable staff to travel safely and be reimbursed)

Whistleblowing schemes Management Manage whistleblowing schemes	The processing is in the legitimate interests of TMC to enable employees to raise concerns regarding suspected conduct or practices that are illegal or in violation of corporate policy and correct inappropriate conduct and actions
Conference call and remote trainings Run internal web-shops through our third parties	The processing is in the legitimate interests of TMC to develop its brand.
Payroll Ensure employees are paid in line with their contractual entitlements and that any regulatory and statutory deductions are paid under our obligations to Revenue as an employer.	The processing is necessary to comply with various employment and Revenue laws. The processing is also necessary for the performance of the employment contract. Where an employee does not provide the requested data, the organisation may be unable to pay employees their contractual entitlements.
Illness Benefit Refund Allocate state illness benefit to correct staff.	The processing is necessary to comply with legal obligations.
Pension administration Properly administer the employee's pension entitlement and to comply with necessary pension rules of the State	The processing is necessary to comply with pension laws. The processing is also necessary for the performance of the employment contract. Processing of special categories of personal data is carried out for pension purposes in line with applicable data protection laws. Where the individual does not provide the requested data, the organisation may be unable to administer their pension.
Performance management Manage employee performance in accordance with relevant company policies.	The processing is necessary for the performance of the employment contract and is in the legitimate interests of the employer to manage employee performance in circumstances where such interests are not overridden by the rights and freedoms of employees.
Grievance, disciplinary and bullying & harassment investigations Ensure employee complaints and/or disciplinary matters are managed appropriately and that they are properly investigated in accordance with the principals of natural justice as well as the relevant Unilabs policies and employment legislation.	The processing is necessary to comply with an employer's legal obligations to apply fair procedures to any employee investigation, for the performance of the employment contract and in the legitimate interests of the employer to fully investigate employee complaints in circumstances where such interests are not overridden by the rights and freedoms of employees.
Manage network, security and IT assets and tools Protect against the dangers associated with e-mail and internet use and to ensure employees are using such systems in accordance with Unilabs policies. This also includes providing proper IT assets and tools.	The processing is in the legitimate interests of TMC to manage employee performance and ensure the security of e-mail and internet systems in circumstances where such interests are not overridden by the rights and freedoms of employees.
Assessment of the working capacity Manage employee absences, to manage sick pay in accordance with the contract of employment and employee handbook, to allow Unilabs to assess the fitness to work of relevant employees.	The processing is necessary to assess, subject to appropriate safeguards, the working capacity of the employee and to carry out obligations and exercise rights under employment law and health & safety legislation.
Employment termination management Adequately manage the termination of the employment relationship.	The processing is necessary to comply with the employment contract and is in the legitimate interests of the employer to manage the termination of the employment relationship in line with company policies in circumstances where such interests are not overridden by the rights and freedoms of employees.

Define and manage planning and organizational structure	The processing is necessary for the performance of the employment contract and in the legitimate interest of TMC to mobilize human resources by organizing daily work to support TMC strategy. If we use data that is sensitive to you (like health data) this is limited to what is necessary processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment (art. 9 GDPR, par. 2, point b).
Improve quality of work life and engagement	The processing is in the legitimate interests of TMC to mobilize and develop human resources to support TMC strategy in improving the work life balance quality. If we use data that is sensitive to you (like health data) this is limited to what is necessary processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment (art. 9 GDPR, par. 2, point b).
Analyse financial performance and perform planning (budget) process	The processing is in the legitimate interests of TMC to monitor and plan for company's performance.
Manage insurance contracts to protect the company and its directors against main risks	The processing is in the legitimate interests of TMC to protect its assets, employees and directors.
Perform internal and external audits to assess level of internal control and comply with regulations	The processing is in the legitimate interests of TMC to assess internal control level.
Control physical access and visitors access	The processing is in the legitimate interests of TMC to secure physical access to its premises.
Communication to employees	The processing is in the legitimate interests of TMC to communicate and inform employees.
Manage and report litigation cases	The processing is in the legitimate interests of TMC to establish, exercise or defence of legal claims.
Manage quality Quality management includes quality processes when performing medical diagnosis activities, manage quality documentation, manage quality audits, training of internal staff to quality standards, manage non-conformities and claims, and perform continuous improvement activities.	The processing is necessary to comply with a legal obligation when applicable, including maintenance of external quality certifications and is in the legitimate interests of TMC to maintain and improve operational standards, handle incidents, and improve customer satisfaction.

If you are working in Operations or as Physician:

Type of data	Purpose	Legal basis	Retention period
Identification data Work organization data	Register referrals and samples	The processing is necessary for the performance of the employment contract	Up to 10 years following last performed diagnostic procedure (depending on in which country the patient has been treated)
Identification data Work organization data	Interpret results and report	The processing is necessary for the performance of the employment contract	
Identification data Work organization data	Send report and images to referrer (and/or statutory bodies)	The processing is necessary for the performance of the employment contract	
Identification data Work organization data	Manage relationship with Health Facilities, Hospitals, Health Professionals, and Patients	The processing is necessary for the performance of the employment contract	Following termination of contract, 5 years

Identification data Work organization data	Collect and transport samples (logistics)	The processing is necessary for the performance of the employment contract	Up to 10 years following last performed diagnostic procedure (depending on in which country the patient has been treated)
Identification data Work organization data	Develop product and process	The processing is in the legitimate interests of TMC to improve its business and its customers satisfaction	

Where necessary, TMC may keep information relating to your health (provided by you), which could include reasons for absence and doctor's reports and notes. This information will be used in order to comply with TMC health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to the job might be appropriate. This information can also be used to support you in visa processes if applicable. We will also need this data to administer and manage statutory and company sick pay.

In addition, by virtue of Security and Confidentiality User Guidelines, TMC may have access to your company computer and mobile telephone use, when so required. Any such measures will be carried out according to the process defined in that guideline.

In the event of the employee's absence, TMC may access the employee´s email to recover communications and work performed in the strictly professional field, as well as allowing the redirection of the professional's email account to the account of another member of the department and/or, if applicable, business line, during a period of three (3) months in order to properly manage professional emails that could be received.

Section 4 – Profiling or Automated Decision Making

Your preferences and interests when it comes to training and development will be evaluated and analyzed in order to offer you tailored courses and information which we believe you will be interested in. We believe this will be beneficial for your development.

Section 5 – Indirect collection of data

Your personal data may also have been indirectly collected from different sources:

Categories of personal data indirectly collected	**Source**
Identification and Professional Data	Internal sources (such as the manger) External sources (recruitment agencies or training companies)

Section 6 – Categories of recipients of the personal data

Your personal data will be shared with the following recipients:

- Within TMC, Unilabs Switzerland and Unilabs Group, including other TMC companies: with authorized personnel in charge of HR, payroll, controlling and finance, IT, physical security, commercial activities. It will also be shared with your line manager. Identification data, professional data and work organization will be more widely shared internally and for specific events with the event's organisers.
- With providers acting on our behalf and assisting us in the management of our activities such as: pension providers, social declaration recipients, insurance providers.

Section 7 – Data retention period

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, tax, accounting, reporting or contractual requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

When personal data is no longer needed or has reached its retention period it is deleted.

Personal data might be kept for a longer period of time where it is necessary in accordance with legal requirements.

Please consult the specific retention periods below.

Type of data	Retention period
Record and update contracts and employee / non-employed staff files	During the validity of the contract, and after that 5 years, any relevant document for commercial purposes 6 years and for tax purposes and legal (litigation cases) purposes 10 years
IT logfiles and user information	
Communication records	6 years after end of employment
Health data for visa process	Medical records used for obtaining the visa will be kept during the application process and destroyed within a month after the application process is terminated
Whistleblowing schemes	2 months from the start of the investigation, or as long as required to complete the investigation (if longer than 2 months)
Photos	During the validity of the contract, and after that 5 years

Section 8 – Transfer of personal data

Due to the international dimension of the TMC Group, your personal data may be transferred outside of the European Union to the Australian Telemedicine Clinic located in Sydney, Australia, and Telemedicine Clinic New Zealand, located in Auckland, New Zealand. As TMC is part of the Unilabs group, the data may also be transferred to the headquarters in Switzerland, which is a country recognized as ensuring an adequate level of protection.

To provide you with the best quality services, we use service providers such as Enterprise Resource Planning (ERP) software services provider, for example to raise and manage invoices, with presence in other countries such as the United States. Some of these providers process your personal data in countries where the level of protection of your personal data requires the implementation of additional measures. To ensure the protection of personal data, TMC put in place relevant safeguards such as the signature of data transfer agreements based on the standard contractual clauses issued by the European Commission or, in the United Kingdom, the Information Commissioner's Office. If you wish to obtain more information, please write to the following address: dpo@unilabs.com.

Section 9 – Data subjects rights

In relation to your personal data, you have the following rights:

- **(a) Right to object:** You can object to our processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this basis. Please contact us, providing details of your objection.
- **(b) Access to your personal data:** You can request access to a copy of your personal data that we hold, along with information on what personal data we use, why we use it, who we share it with, how long we keep it for and whether it has been used for any automated decision making. You can make a request for access free of charge. In compliance with the GDPR, we will respond to a valid subject access request without undue delay and at the latest within one month of receiving the request. In some circumstances, we can extend the time to respond by a further two months. For example, when the request is complex. In this case, we will let you know within one month of receiving your access request and explain to you why the extension is necessary.
- **(c) Consent:** Most of the time, we won't need your consent to use your personal data as we will be using it only to fulfil our obligations and exercise our rights as an employer. There are limited circumstances where we may ask for your consent to process your information. Where you have given us your consent to use personal data, you can withdraw your consent at any time.
- **(d) Rectification:** You can ask us to change or complete any inaccurate or incomplete personal data held about you.
- **(e) Erasure:** You can ask us to delete your personal data where it is no longer necessary for us to use it, you have withdrawn consent, or where we have no lawful basis for keeping it. Please be aware that we may have legal obligations to retain employee records for a certain period after your employment.
- **(f) Portability:** You can ask us to provide you or a third party with some of the personal data that we hold about you in a structured, commonly used, electronic form, so it can be easily transferred.
- **(g) Restriction:** You can ask us to restrict the personal data we use about you where you have asked for it to be erased or where you have objected to our use of it.

- **(h) No automated-decision making:** Automated decision-making takes place when an electronic system uses personal data to make a decision without human intervention. You have the right not to be subject to automated decisions that will create legal effects or have a similar significant impact on you, unless (i) you have given us your consent (ii) it is necessary for a contract between you and us, or (iii) is otherwise permitted by law. You also have certain rights to challenge decisions made about you.

Section 10 – Means of exercising

To exercise your rights please fill out the web form available at this link.

You can also exercise your rights by sending an e-mail to the following address: dpo@unilabs.com.

The exercise of your rights is free of charge.

Section 11 – Contact details of the Data Protection Officer

If you have any comments or questions regarding this Privacy Notice or our data handling practices, please contact the Data Protection Officer.

Email: dpo@unilabs.com

Section 12 – Right to lodge a complaint with DPA

If you are unsatisfied with the way in which we have handled your personal data or any privacy query or request that you have raised to us and you didn't receive a satisfied answer by us and/or our DPO, you have the right to lodge a complaint with a Data Protection Authority (DPA).

Please consult the table below for the contact details of the DPAs of the countries where we are established.

Data Protection Authority	**Contact Details**
Data Protection Authority of Spain	Agencia Española de Protección de Datos (AEPD) C/Jorge Juan, 6 28001 Madrid Tel. +34 91 266 3517 Fax +34 91 455 5699 Email: internacional@aepd.es
Data Protection Authority of UK	The Information Commissioner's Office Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF Tel. +44 1625 545 745 E-mail: international.team@ico.org.uk
Data Protection Authority of Denmark	Datatilsynet Carl Jacobsen Vej 35 2500 Valby Tel. +33 19 32 00 Email: dt@datatilsynet.dk
Data Protection Authority of Sweden	Integritetsskyddsmyndigheten Drottninggatan 29 104 20 Stockholm Tel. +46 8 657 6100 Fax +46 8 652 8652 Email: imy@imy.se
Data Protection Authority of Australia	The Office of the Australian Information Commissioner 175 Pitt Street Sydney NSW 2000 Tel. 1300 363 992 | +61 2 9942 4099 Fax +61 2 6123 5145
Data Protection Authority of New Zealand	The Privacy Commissioner's Office

Data Protection Authority	Contact Details
Data Protection Authority of Spain	Agencia Española de Protección de Datos (AEPD) C/Jorge Juan, 6 28001 Madrid Tel. +34 91 266 3517 Fax +34 91 455 5699 Email: internacional@aepd.es
	Level 13, 15 Shortland Street, Auckland 1010 New Zealand Tel. 0800 803 909 Email: enquiries@privacy.org.nz

If you are located in the European Union, you have the right to lodge a complaint with the DPA of the Member State of your habitual residence, place of work or place of the alleged infringement.

To find the appropriate contact details of the Data Protection Authorities members of the European Data Protection Board, please visit the EU Commission's directory of DPAs.

29.04.2024