

GROUP DATA PROTECTION STATEMENT FOR HEALTHCARE 21

CONTACT DETAILS

If you have any questions about this Data Protection Statement or the way in which your Personal Data is being used by us please contact:

Data Protection Officer
C/O Healthcare 21 HQ
Unit 13000 Blarney Business Park,
Blarney, Cork
T23 HV1N
Ireland

Email: gdpr@hc21.group
Telephone: 0810 21 21 21

“Personal Data” means any information relating to an identified or identifiable natural person (**‘data subject’**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1. ABOUT THE HEALTHCARE 21 GROUP

This Data Protection Statement applies to the following companies in the Healthcare 21 Group:

Primacy Healthcare 21 Ltd
Tools for Living (Ireland) Ltd
Healthcare 21 (UK) Ltd
Primary Healthcare 21 (International) Ltd
O’Flynn Medical
Aquilant Medical (ROI) Ltd
Aquilant Scientific (ROI) Ltd
Aquilant Northern Ireland Ltd
Aquilant Ltd
Aquilant Endoscopy Ltd
Xograph Group Holdings Ltd
Xograph Healthcare Ltd
Xograph Healthcare Ireland Ltd

References to **“We”**, **“Us”** the **“Company”** and **“HC21”** shall apply to the company in the group that is processing your Personal Data.

Established in 2003, Healthcare 21 is one of Northern Europe’s largest privately-owned healthcare companies with operations across Ireland, the UK, and Germany. We are a leading provider of sales, marketing, customer service, engineering service and logistics for a variety of market leading global medtech manufacturers.

In order to provide our services, we need to process Personal Data. We are committed to protecting the rights and privacy of individuals in accordance with data protection legislation including the General Data Protection Regulation in Europe (the “GDPR”).

2. THE PURPOSE OF THIS DATA PROTECTION STATEMENT

This Data Protection Statement describes our approach to data protection and sets out the basis on which any Personal Data we collect from you, or that you provide to us, will be used by us where we are controllers of that Personal Data for the purposes of the GDPR. Please read this Data Protection Statement carefully to understand our views and practices regarding the Personal Data we collect and how we will treat it.

The protection of your Personal Data is important to us, and we are committed to protecting and safeguarding your rights.

3. WHO THIS DATA PROTECTION STATEMENT APPLIES TO

This Data Protection Statement provides specific information relating to the following individuals whose Personal Data we process:

- (i) business contact data including our customers, suppliers, partners, shareholders and business prospects “**Business Contacts**”; and
- (ii) prospective employees/those applying for jobs at the Company, “**Candidates**”; and
- (iii) users/guests of our Website “**Website Users**”.

Personal Data of employees of the Company is dealt with in a separate internal data protection notice.

4. CATEGORIES OF PERSONAL DATA

We process the following categories of Personal Data. For each category we have included an example of the type of Personal Data that may be part of that category:

Personal Data Category	Description
Identification Data	may include a person’s name, photograph, date of birth, driver’s license and passport information.
Contact Data	may include a person’s email address, phone number, postal address, other communication details (e.g. Skype)
Communication Data	may include phone calls, email correspondence and hard copy correspondence.
Marketing Data	may include your Contact Data and any preferences in receiving marketing from us and your communication preferences.
Recruitment Data	may include recruitment related data such as Identification Data, Contact Data, Communication Data, CV and job application data. When processing CV data, we may process certain Personal Data including the following: employment history, skills/ experience, languages, educational history, qualifications, membership of professional associations, contact details of employer references/character references, licenses held, interests and hobbies, languages, locations, nationality, passport, eligibility to work in certain jurisdictions, salary expectations,

	interview/screening answers and notes and usernames and passwords for access to our recruitment portal.
Financial Data	may include payment related information or bank account details and financial data received as part of the services that we provide.
Special Category Data	If we interact with you for the purposes of a job with the Company or as part of provision of products and services to you we may collect Special Category Data: this can include diversity data such as gender, religion, racial or ethnic origin, sexual orientation, trade union membership or data relating to health. We will only source this data with your explicit consent.
Web Data	When you interact with us online we will automatically collect data about your use of our services, including data on the type of device you're using, its IP address, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of Website use. Where possible, this information is collected at an aggregate level and your identity data is not stored as part of this technical data. Web Data includes cookies and web beacons. Further information about how we use cookies is available in our cookie notice.

5. OUR LEGAL BASIS FOR PROCESSING PERSONAL DATA

We process all Personal Data lawfully and in accordance with the requirements of the law. The GDPR sets out the legal grounds for processing Personal Data.

When the Company processes Personal Data it is generally on one of the following legal basis:

CONTRACT

We will process Personal Data where necessary to perform our obligations relating to or in accordance with any contract that we may have with you or to take steps at your request prior to entering into that contract (e.g. our Terms of Sale);

CONSENT

For certain processing activities we may rely on your consent.

Where we are unable to collect consent for a particular processing activity, we will only process the Personal Data if we have another lawful basis for doing so.

You can withdraw consent provided by you at any time by contacting us at gdpr@hc21.group

LEGITIMATE INTEREST

At times we will need to process your Personal Data to pursue our legitimate business interests, for example for administrative purposes, to collect debts owing to us, to provide information to you, to operate, evaluate, maintain, develop and improve our websites and services or to maintain their security and protect intellectual property rights.

We will not process your Personal Data on a legitimate interest basis where the impact of the processing on your interests or fundamental rights and freedoms outweighs our legitimate interests. You may object to any processing we undertake on this basis. If you do not want us to process your Personal Data on the basis of our legitimate interests, contact us at gdpr@hc21.group and we will review our processing activities.

LEGAL OBLIGATION

If we have a legal obligation to process Personal Data, such as the payment of taxes, we will process Personal Data on this legal ground.

6. OUR PROCESSING ACTIVITIES

We use your Personal Data to provide you with our services and to assist us in the operation of our company. Under data protection law, we must ensure that the purpose of processing is clear.

We have set out below the general purpose of processing, the categories of Personal Data processed and the related lawful basis for processing.

Purpose of Processing	Categories of Personal Data	Lawful Basis
<u>Service Delivery activities</u> <ul style="list-style-type: none"> to contact you re payments to and from you; for customer relationship management and support; to send notifications about changes/updates to our products and services; to provide you with the right products and services and appropriate training to fulfil our legal and contractual obligations 	<ul style="list-style-type: none"> Identification Data Contact Data Communications Data Special Category Data 	<ul style="list-style-type: none"> Contract Legitimate Interest Consent
<u>Marketing & Promotion activities</u> <ul style="list-style-type: none"> to respond to any requests from you to send newsletters and other information that maybe of interest to contact you as part of our business relationship or for lead generation and general administration to inform you of events or webinars that might be of interest to deliver and organise our conferences, seminars, events, and training programmes to create shareable educational content, including photographs and videos from the above events 	<ul style="list-style-type: none"> Marketing Data Contact Data Web Data Identification Data 	<ul style="list-style-type: none"> Consent Legitimate Interest
<u>Recruitment Activities</u> <ul style="list-style-type: none"> as part of agency shortlisting to select the right Candidate to interview the Candidate 	<ul style="list-style-type: none"> Identification Data Contact Data Communication Data 	<ul style="list-style-type: none"> Consent Legitimate Interest Contract

<ul style="list-style-type: none"> to hire and seek to onboard the Candidate (pre contract) to manage our database of prospective Candidates 	<ul style="list-style-type: none"> Recruitment Data Web Data Marketing Data Special Category Data 	<ul style="list-style-type: none"> Legal Obligation
<u>Website Delivery</u> <ul style="list-style-type: none"> to respond to web forms completed by you; to promote our products and services; to administer the Website; and for internal operations, including support, troubleshooting, data analysis, testing, research, statistical and survey purposes to ensure the safety and security of our website and our services. 	<ul style="list-style-type: none"> Web Data 	<ul style="list-style-type: none"> Consent Legitimate Interest
<u>Administration of Client Relationship</u> <ul style="list-style-type: none"> to manage/respond to a complaint/appeal to notify you of updates to this Data Protection Statement 	<ul style="list-style-type: none"> Identification Data Contact Data Communication Data Financial Data 	<ul style="list-style-type: none"> Contract Legitimate Interest
<u>Managing payments and administration of the contract</u> <ul style="list-style-type: none"> to process payments to and from our business. 	<ul style="list-style-type: none"> Identification Data Contact Data Communication Data Financial Data 	<ul style="list-style-type: none"> Contract Legitimate Interest
<u>Management of Corporate Affairs</u> <ul style="list-style-type: none"> to take minutes at board meetings to contact shareholders/investors to enter partnerships and other commercial relations to undertake appropriate due diligence to keep our premises secure (CCTV) 	<ul style="list-style-type: none"> Identification Data Contact Data Communication Data Financial Data 	<ul style="list-style-type: none"> Contract Legitimate Interest Legal Obligation

7. SOURCES OF PERSONAL DATA

BUSINESS CONTACT PERSONAL DATA

We collect Business Contact Personal Data from our business contacts including – customers, suppliers, partners, shareholders and business prospects.

We source Business Contact Personal Data to serve the business relationship. We will only ever source Personal Data that is necessary and in a way that would be generally expected.

We receive Personal Data about Business Contacts from a variety of sources, as follows:

- the Personal Data is often provided by the Business Contact as part of the business relationship;
- the Personal Data may be collected from public sources;

- the Personal Data may be collected indirectly from another person within the company of the Business Contact;
- the Personal Data may be collected through our website;
- the Personal Data may be collected indirectly from a website or from a third party.

CANDIDATE PERSONAL DATA

We will only ever source Personal Data in a way that would be generally expected.

We receive Personal Data relating to Candidates from a variety of sources. The primary source is from Candidates directly. Examples of the sources of Personal Data of Candidates are as follows:

- the Candidate may send their CV to us with the intention of registering with us to be informed of potential job vacancies;
- the Candidate may apply directly to a position advertised on our website;
- the Candidate may apply to a position advertised on a third-party jobs' website;

WEB DATA

We may collect Website User Personal Data from all visitors to our website to improve our services and develop the Website. Click the cookie settings icon on the webpage to access the cookie notice and further details about cookies.

8. DISCLOSURE OF PERSONAL DATA

In certain circumstances, we may disclose Personal Data to third parties as follows:

- to business partners and subcontractors for the performance of any contract relating to our services, including email, Skype, Customer Relationship Management systems, Marketing Management & Social Media scheduling platforms, payment processors, data aggregators, hosting service providers, external consultants, auditors, IT consultants and lawyers.
- to any recruitment agency who is helping us to recruit candidates;
- to analytics and search engine providers that assist us in the improvement and optimisation of the Website.
- if we or substantially all our company is merged with another company or acquired by a third party, in which case Personal Data held by us will be one of the transferred assets.
- if we are under a duty to disclose or share Personal Data to comply with any legal obligation (including tax, audit or other authorities), or in order to enforce or apply any contracts that we have.
- to protect our rights, property, or safety, or that of our Candidates or Business Contacts or others. This may include exchanging Personal Data with other companies and organisations for the purpose of fraud protection.

When we engage other organisations to perform services for us, we may provide them with information including Personal Data, in connection with the performance of those functions. We do not allow third parties to use Personal Data except for the purpose of providing these services.

9. SECURITY MEASURES

We will take all steps reasonably necessary to ensure that all Personal Data is treated securely in accordance with this Data Protection Statement and the relevant law, including the GDPR.

In particular, we have put in place appropriate technical and organisational procedures to safeguard and secure the Personal Data we process.

We monitor for and do everything we can to prevent security breaches of the Personal Data that we process.

Once we have received your Personal Data, we will use strict procedures and security features for the purpose of preventing unauthorised access and ensuring that only those who need to have access to your Personal Data can access it.

We also use secure connections to protect Personal Data during its transmission. Where you have been given (or where you have chosen) a password which enables you to access services, you are responsible for keeping this password confidential. Please do not share your password with anyone.

If you think that there has been any loss or unauthorised access to Personal Data of any individual, please let us know immediately.

10. TRANSFERS OUTSIDE THE EEA

In order to provide our products and services we may need to transfer Personal Data outside the European Economic Area (EEA). We ensure that any transfer of Personal Data outside the EEA is undertaken using legally compliant transfer mechanisms and in accordance with the GDPR.

If we transfer Personal Data outside of the EEA, we generally rely on the Standard Contractual Clauses under Article 46.2 of the GDPR adopted by the EU Commission. For US transfers we rely on the EU-US (+/- UK Extension) Data Privacy Framework. We may also rely on some of the other legally compliant transfer mechanisms provided under the GDPR.

11. COOKIES

Cookies are small text files placed on your computer or mobile device by websites that you visit, and they help us improve the products and services that we offer you. They are used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Cookies may allow a website to remember your activity over a period of time. Cookies are optional and you do not have to accept them.

Click the cookie settings icon on the webpage to access the cookie notice and further details about cookies



12. THIRD PARTY WEBSITES

Our Website may contain links to and from third party websites. If you follow a link to any of these websites, please note that these websites have their own data protection settings, and these are not endorsed by us. We do not accept any responsibility or liability for these third-party websites. Please undertake the appropriate due diligence before submitting any Personal Data to these websites.

13. RETENTION

In some circumstances it is not possible for us to specify in advance the period for which we will retain your Personal Data. In such cases we will determine the appropriate retention period based on balancing your rights against our legitimate business interests. We may also retain certain Personal Data beyond the periods specified herein in some circumstances such as where required for the purposes of legal claims.

Further information about our retention practices are set out below:

Purpose of Processing	Retention Period
Service Delivery Activities	24 months after completion of service delivery activities in the case where there is no further meaningful engagement.
Marketing and Promotion Activities	12 months in the case where no meaningful engagement or earlier in the case you unsubscribe.
Recruitment Activity	12 months for Candidates who are not hired. Candidates who have consented will remain on the database for other positions with the company until consent is withdrawn or there is no meaningful engagement over a period of time. A separate retention policy applies to employees
Website Delivery	12 months
Managing Payments and administration of the contract	7 years
Management of Corporate Affairs	7 years unless required to retain indefinitely

In certain cases, we may retain Personal Data for longer than specified here if required under relevant laws or in the event of any legal claim.

14. YOUR RIGHTS

You have various rights relating to how your Personal Data is used.

Right of access to the Personal Data we hold on you

You have the right to ask for all the Personal Data we have about you. When we receive a request from you in writing, we must give you access to everything we've recorded about you as well as details of the processing, the categories of Personal Data concerned and the recipients of the Personal Data.

We will provide the first copy of your Personal Data free of charge, but we may charge you a reasonable fee for any additional copies.

We cannot give you access to a copy of your Personal Data in some limited cases including where this might adversely affect the rights and freedoms of others.

Right of rectification of Personal Data

You should let us know if there is something inaccurate in your Personal Data.

We may not always be able to change or remove that Personal Data, but we'll correct factual inaccuracies and may include your comments in the record to show that you disagree with it.

Right of erasure of Personal Data (right to be forgotten)

In some circumstances you can ask for your Personal Data to be deleted, for example, where:

- your Personal Data is no longer needed for the reason that it was collected in the first place
- you have removed your consent for us to use your Personal Data (where there is no other lawful basis for us to use it)
- there is no lawful basis for the use of your Personal Data
- deleting the Personal Data is a legal requirement

Where your Personal Data has been shared with others, we will do what we can to make sure those using your Personal Data comply with your request for erasure.

Please note that we can't delete your Personal Data where:

- we are required to have it by law
- it is used for freedom of expression
- it is used for public health purposes
- it is used for scientific or historical research or statistical purposes where deleting the Personal Data would make it difficult or impossible to achieve the objectives of the processing
- it is necessary for legal claims.

Right to restrict what we use your Personal Data for

You have the right to ask us to restrict what we use your Personal Data for where:

- you have identified inaccurate Personal Data, and have told us of it
- where we have no legal reason to use the Personal Data, but you want us to restrict what we use it for rather than erase the Personal Data altogether

When Personal Data is restricted, it can't be used other than to securely store the Personal Data and with your consent to handle legal claims and protect others, or where it's for important public interests.

Right to have your Personal Data moved to another provider (data portability)

You have the right to ask for your Personal Data to be given back to you or another service provider of your choice in a commonly used format. This is called data portability.

This right only applies if we're using your Personal Data with consent and if decisions were made by a computer and not a human being. It does not apply where it would adversely affect the rights and freedoms of others.

Right to object

You have the right to object to processing of your Personal Data which is based on public interest or legitimate interest processing. We will no longer process the Personal Data unless we can demonstrate a compelling ground for the processing.

Right not to be subject to automated decision-making

You have the right not to be subject to a decision based solely on automated processing. This right shall not apply where the processing is necessary for a contract with you, or the processing is undertaken with your explicit consent or the processing is authorised by law.

You can make a complaint

You have the right to lodge a complaint with the local supervisory authority for data protection in the EU member state where you usually reside, where you work or where you think an infringement of data protection law took place.

15. AMENDMENTS TO THIS DATA PROTECTION STATEMENT

We will post any changes on the Website and when doing so will change the effective date at the top of this Data Protection Statement. Please make sure to check the date when you use our services to see if there have been any changes since you last used those services.

In some cases, we may provide you with additional notice of changes to this Data Protection Statement, such as via email. We will always provide you with any notice in advance of the changes taking effect where we consider the changes to be material.

Thank you for reading our Data Protection Statement. Please contact us at gdpr@hc21.eu if you have any questions. If we are unable to resolve your concerns, you have the right to contact the supervisory authority in the country where you live or work, or where you consider that the data protection rules have been breached

Contact Details for the relevant Supervisory Authorities are set out below for your information:

Country	Supervisory Authority	Contact Details
Ireland	Data Protection Commission	Online Form: https://forms.dataprotection.ie/contact Address: 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland Tel: +353 578 684 800 or +353 761 104 800
UK	Information Commissioner Office	Online: https://ico.org.uk/global/contact-us/ Live Chat: ico.org.uk/livechat Helpline: 0303 123 1113

