

Privacy policy

1. Introduction

1.1 We are committed to safeguarding the privacy of the Wexford Ultrasound website visitors and its clients in accordance to General Data Protection Regulation (GDPR).

This policy sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it

1.2 This policy applies where we are acting as a data controller with respect to the personal data of the Wexford Ultrasound website visitors and customers; in other words, where we determine the purposes and means of the processing of that personal data.

1.3 We use cookies on our website. Insofar as those cookies are not strictly necessary for visitors to view our website, we will ask you to consent to our use of cookies when you first visit our website.

1.4 In this policy, "we", "us" and "our" refer to Wexford Ultrasound For more information about Wexford Ultrasound, see Section 12.

2. Credit

2.1 This document was created using a template from SEQ Legal (<https://seqlegal.com>).

3. How we use your personal data

3.1 In this Section 3 we have set out:

- (a) the general categories of personal data that we may process;
- (b) in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
- (c) the purposes for which we may process personal data; and
- (d) the legal bases of the processing.

3.2 We may process data about your use of our website and services ("usage data"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the

usage data is Google Analytics. This usage data may be processed for the purposes of analysing the use of the website and services. The legal basis for this processing is for our legitimate interests, namely monitoring and improving our website and services.

3.3 We may process information contained in any enquiry you submit to us regarding goods and/or services ("enquiry data"). The enquiry data may be processed for the purposes of offering, marketing and selling relevant goods and/or services to you. The legal basis for this processing is consent.

3.4 We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("notification data"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is consent.

3.5 We may process information contained in, or relating to, any communication that you send to us ("correspondence data"). The correspondence data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website contact forms. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is for our legitimate interests, namely the proper administration of our website and business and communications with users.

3.6 We may process any of your personal data identified in this policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

3.7 We may process any of your personal data identified in this

policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

3.8 In addition to the specific purposes for which we may process your personal data set out in this Section 3, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

3.9 Please do not supply any other person's personal data to us, unless we prompt you to do so.

4. Providing your personal data to others

4.1 We may disclose cookie data to Google analytics identified at <https://analytics.google.com/> insofar as reasonably necessary for analysis - we use cookies to help us to analyse the use and performance of our website and services (cookies used for this purpose are: Google analytics - `_ga` and `_gid` and

5. Retaining and deleting personal data

5.1 This Section 5 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

5.2 Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

5.3 We will retain your personal data as follows:

- (a) personal data [email address] will be retained for a minimum period of 12 months following use of the web contact form, and for a maximum period of 24 months following the sign-up date.

5.4 In some cases it is not possible for us to specify in advance the periods for which your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria:

- (a) the period of retention of your email address will be determined based on consent and legitimate interest for the purposes of offering, marketing and selling relevant goods and/or services to you.

5.5 Notwithstanding the other provisions of this Section 5, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

6. Amendments

6.1 We may update this policy from time to time by publishing a new version on our website.

6.2 You should check this page occasionally to ensure you are happy with any changes to this policy.

6.3 We may notify you of significant changes to this policy by email.

7. Your rights

7.1 In this Section 7, we have summarised the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

7.2 Your principal rights under data protection law are:

- (a) the right to access;
- (b) the right to rectification;
- (c) the right to erasure;
- (d) the right to restrict processing;
- (e) the right to object to processing;
- (f) the right to data portability;
- (g) the right to complain to a supervisory authority; and
- (h) the right to withdraw consent.

7.3 You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.

7.4 In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to

the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.

7.5 In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.

7.6 You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

7.7 You have the right to object to our processing of your

personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.

7.8 You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

7.9 To the extent that the legal basis for our processing of your personal data is:

- (a) consent; or
- (b) that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract, and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

7.10 If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.

7.11 To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.

7.12 You may exercise any of your rights in relation to your

personal data by written notice to us OR in addition to the other methods specified in this Section 7.

8. About cookies

8.1 A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.

8.2 Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

8.3 Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

9. Cookies that we use

9.1 We use cookies for the following purposes:

- (a) authentication - we use cookies to identify you when you visit our website and as you navigate our website (cookies used for this purpose are: Google analytics - `_ga` and `_gid`).
- (f) analysis - we use cookies to help us to analyse the use and performance of our website and services (cookies used for this purpose are: Google analytics - `_ga` and `_gid` and

- (g) cookie consent - we use cookies [to store your preferences in relation to the use of cookies more generally (cookies used for this purpose are: Google analytics

10. Cookies used by our service providers

10.1 Our service providers use cookies and those cookies may be stored on your computer when you visit our website.

10.2 We use Google Analytics to analyse the use of our website. Google Analytics gathers information about our website use by means of cookies. The information gathered is used to create reports about the use of our website. Google's privacy policy is available at: <https://www.google.com/policies/privacy/>. The relevant cookies are: `_ga` and `_gid`

11. Managing cookies

11.1 Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

- (a) <https://support.google.com/chrome/answer/95647?hl=en> (Chrome);
- (b) <https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences> (Firefox);
- (c) <http://www.opera.com/help/tutorials/security/cookies/> (Opera);

- (d) <https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies> (Internet Explorer);
- (e) <https://support.apple.com/kb/PH21411> (Safari); and
- (f) <https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy> (Edge).

11.2 Blocking all cookies will have a negative impact upon the usability of many websites.

11.3 If you block cookies, you will not be able to use all the features on our website.

12. Our details

12.1 This website is owned and operated by Wexford Ultrasound Ltd.

12.2 We are registered in The Republic of Ireland under Company registration number 432166 and our registered office is at Suite 8, Redmond Medical Centre, Redmond Square, Wexford.

12.3 Our principal place of business is at Suite 8, redmond Medical Centre, Redmond Square, Wexford.

12.4 You can contact us:

- (a) by post, using the postal address given above;
- (b) using our website contact form;
- (c) by telephone, on 087 3626777; or
- (d) by email, using info@wexfordultrasound.ie.

13. Data protection officer

13.1 Our data protection officer's contact details are:

Dr. Tadhg Gleeson - Wexford Ultrasound, 087 3626777

GDPR Compliance Wexford Ultrasound 2018-05-29

GDPR became active on 25th May 2018. Prior to its implementation, a data controller was appointed by the group partners to review and enhance their organisation's risk management processes, and ensure compliance. Data Protection Impact Assessment (DPIA) An inventory of all personal data held was examined The following data is stored on password and Firewall secured PC's in Suite 8, Redmond Medical Centre and backup storage on an external optical disk Hard Drive:

- Patient name, date of birth, date of ultrasound scan
- Official radiologist report of ultrasound examination in write-protected word document.
- DICOM and JPEG copies of images acquired which are archived for reference and comparison for follow up or if imaging is requested by the patient for use in another health institution
- Data was obtained following receipt of request from qualified medical doctor to perform the scan, and following appointment being made directly with the patient, either by telephone or standard mail.
- Consent has always been implied, once the patient consents to the examination being ordered, it is presumed they agree to the images and report being forwarded to the referring doctor, and being securely stored to allow the patient themselves, or their designated consultant or doctor to access same at a later date, but only with the patient's consent
- Data is stored indefinitely to facilitate access to their medical records for their lifespan
- PCs are password protected with up-to-date antivirus and firewall software. Referral and reports are electronically received and sent on secure encrypted Healthlink and healthmail platforms, or by confidential standard mail
- Images and reports are occasionally burnt at the direct request of the patient when requiring same for referrals to

other health service providers, and only given directly to the patient themselves.

- Credit card slips are temporarily stored in locked filing cabinet for accounting and taxation purposes before being shredded at the end of the financial year.

Communicating with Staff and Service Users

Wexford Ultrasound webpage is being updated to reflect privacy policy and current consent practices as well as how and why patient data is recorded. Patient's attention is drawn to this at the time of consultation. All staff have been made aware of company policy in this regard and the necessity to protect individual service users data.

As per current legislation requires we notify our customers of our identity, our reasons for gathering the data, the uses it will be put to, who it will be disclosed to, and that it will not be transferred outside the EU if specifically requested by the patient.

Under GDPR, our website is updated to reflect the fact that we are required on medicolegal basis to store personal data relating only to the relevant medical ultrasound examination, the reasons for requiring a potentially indefinite retention period, and the fact that the service user has the right of complaint if they are unhappy with our implementation of any of these criteria, whether their data will be subject to automated decision making and their individual rights under the GDPR.

Personal Privacy Rights

We acknowledge the patient's rights to:

- Access their imaging report and copies of ultrasound scan if required
- have inaccuracies corrected
- have information erased
- to restrict the processing of their information
- a copy of their personal data (data portability)

Any request from a data subject wishing to exercise their rights under the GDPR will be dealt with by the Data Controller who will locate, access (and correct or delete) the data from all locations where it is stored upon written request by the patient (identity to be confirmed by state photo ID). Data can be saved on CD to allow data portability or sent via encrypted email if required electronically by the patient. Reports are saved as write-protected Microsoft Word documents, and images in DICOM and JPEG format to allow ease of access. Request will be dealt with promptly and well within the calendar month.

Legal Basis

To defend the practice Radiologists from future medicolegal proceedings, and to protect the service users rights to their data for health or medicolegal purposes, personal data processes will be designated as having a legal basis and not just reliant on consumer consent as justification. This is outlined in our privacy notice on the company webpage.

Amount of personal data gathered is kept to an absolute minimum.

Using customer consent as a grounds to process data

Customer consent is implied when the patient agrees to undergo the imaging procedure. Formally seeking, obtaining and recording that consent in every individual case is not practical and not routinely performed. Patients are directed to the privacy policy on the website www.wexfordultrasound.ie when appointment is being made. and whether you need to make any changes.

Consent must be 'freely given, specific, informed and unambiguous'. Essentially, your customer cannot be forced into consent, or be unaware that they are consenting to processing of their personal data. They must know exactly what they are consenting to, and there can be no doubt that they are consenting. Obtaining consent requires A positive indication of agreement is implied when the patient attends for their scan appointment and is not inferred from silence, pre-ticked boxes or inactivity.

Processing Children's Data

Minors are always accompanied by a parent or guardian who verify individual ages and give verbal consent.

Reporting data breaches

Procedures are in place to detect, report and investigate a personal data breach. Any potential data breach is reported to the Data Controller who notifies the Data Protection Commissioners office immediately, and coordinates appropriate steps to mitigate or resolve. All breaches will be reported to the DPC, typically within 72 hours, and will also be reported to the individuals concerned.

Data Protection Officers

Dr Tadhg Gleeson has been appointed on an interim basis as designate Data Controller and Data Protection Officer (DPO).