

Privacy Policy & Data Breach Response Plan

# Privacy Policy

Privacy Policy for Ro Beauty Ltd
Effective Date: 10 June 2025
Data Controller: Ro Beauty Ltd, 2 Picture House Buildings, Mill Lane, Billingham, UK, TS23 1HE
Website: www.robeauty.co.uk
Contact: robeautyltd@gmail.com |

1. Who We Are
We are Ro Beauty Ltd, a UK-based beauty salon providing in-person and online services.
This policy explains how we collect, store, and use personal information.
We are committed to protecting your privacy and handling your information in compliance with the UK General Data Protection Regulation (UK GDPR).

2. What Personal Data We Collect
General Personal Data:
- Name
- Email address
- Phone number
- Date of birth
- Billing and shipping address
- Appointment history
- Payment details (processed securely via third-party services like Stripe or Wix Payments)

Special Category Data:
- Medical history and conditions (e.g., allergies, skin conditions)
- Treatment notes

3. How We Collect Data
We collect data when you:
- Book an appointment (online or in person)
- Fill in our consultation or consent forms
- Purchase products or services through our website
- Subscribe to newsletters or marketing
- Contact us via phone, email, or social media

4. Why We Collect Your Data (Legal Basis)
Purpose: Booking and delivering treatments | Legal Basis: Contract
Purpose: Medical history for treatments | Legal Basis: Explicit consent (Special Category Data)
Purpose: Order fulfilment and payment | Legal Basis: Contract
Purpose: Marketing and offers | Legal Basis: Consent
Purpose: Regulatory compliance | Legal Basis: Legal obligation
Purpose: Record-keeping and insurance | Legal Basis: Legitimate interest / Legal obligation

5. How We Protect Your Data
Your data is stored securely using:
- SSL encryption (Wix)
- Secure cloud-based systems
- Password-protected devices
- Role-based access controls

6. Sharing Your Data
We do not sell your data. We may share your data with:
- Payment providers (Stripe, Wix Payments)
- IT and website providers (Wix)
- Insurance providers or legal advisors (as required)
- Regulatory authorities (if legally necessary)

7. How Long We Keep Your Data
- Client records: up to 6 years after your last appointment
- Medical records: up to 7 years (or until age 25 for minors)
- Financial records: 6 years (tax purposes)
- Marketing preferences: until unsubscribed

8. Your Rights Under UK GDPR
You have the right to:
- Access, correct, or delete your data
- Withdraw consent
- Restrict or object to processing
- Port data
- Lodge a complaint with the ICO: https://ico.org.uk

9. Cookies and Tracking
We use cookies for:
- Website functionality
- Analytics
- Marketing (with consent)
Cookie preferences can be managed via our cookie banner.

10. Changes to This Policy

This policy is reviewed annually and updates will be published on our website.

# Appendix 1: Data Breach Response Plan

Data Breach Response Plan Ro Beauty Ltd 2025

Purpose:
To ensure a swift, responsible, and compliant response to any data breach involving personal or special category data.

1. What is a Personal Data Breach?
Includes loss/theft of data, unauthorised access, accidental deletion, malware, or sending data to the wrong person.

2. Detection
Breaches may be identified via:
- Suspicious activity on website
- Wix or payment system alerts
- Client reports
- Internal reporting

3. Containment and Assessment (within 24 hours)
- Secure affected systems
- Identify compromised data and affected individuals
- Assess risk to individuals’ rights, especially with medical data

4. Notification (within 72 hours)
- Notify the ICO if required (https://ico.org.uk)
- Notify individuals if there's a high risk (especially medical/payment info)
- Communicate what happened, data affected, our response, and contact info

5. Documentation and Review
- Record details of the breach: what, when, who, how
- Review and update policies or training to prevent recurrence