GDPR Responsibilities Checklist

For: Bramforth AI Customers

Purpose: Quick checklist of your data protection responsibilities

Applies to: All appointment-based businesses using voice AI

Time to Complete: 30-60 minutes

Before You Start Using Bramforth AI

- [ ] **1. Update Your Privacy Notice**

What to add:

- "We use AI-powered call handling for appointment booking and customer service"
- "Call recordings kept for [duration] and then automatically deleted"
- "Some data processed by US providers under legal safeguards (SCCs)"
- Link to your full privacy notice

Where to add it:

- Your website privacy page
- Reception area or waiting room (optional but good practice)
- Booking confirmation emails

Examples by business type:

💆‍♀️ **Medical/Aesthetic Clinic:**

> *"We use AI-powered call handling for appointment booking. Calls are recorded for quality and training purposes. During calls, you may share health-related information which is processed securely under our lawful basis for healthcare provision."*

💇 **Hair Salon/Spa:**

> *"We use an AI booking assistant to handle appointment calls. Calls are recorded to improve our service. Recordings are kept for 30 days and then automatically deleted."*

💼 **Consultancy/Coaching:**

> *"Our AI assistant handles appointment scheduling. Call recordings are used for service improvement and are automatically deleted after 30 days."*

Need help? We can provide template text for your industry.

- [ ] **2. Set Your AI's Greeting Script**

Must include: AI identifies itself as an AI assistant

Examples:

Medical Clinic:

> *"Hello, you're through to [Clinic Name]. I'm [Name], your AI assistant. How can I help you today?"*

Hair Salon:

> *"Hi, this is [Salon Name]. I'm [Name], your booking assistant. I can help you schedule an appointment."*

Consultancy:

> *"Good morning, you've reached [Company Name]. I'm [Name], your virtual assistant. How may I assist you?"*

That's it. No need for "this call is being recorded" announcement.

- [ ] **3. Check Your Legal Basis**

  For ALL Businesses:

  You need a lawful basis under GDPR Article 6 to process customer data:

  - ✅ **Legitimate interests** (service delivery) - usually covers appointment booking
  - ✅ **Contract performance** (managing customer appointments)

  These two bases cover standard appointment booking for most businesses.

  For Healthcare/Medical Businesses ONLY:

  If you're a medical clinic, aesthetic clinic, or healthcare provider, you also need a legal basis for processing **health data** under GDPR Article 9:

  - ✅ **Healthcare provision** (Article 9(2)(h)) - most common for medical practices
  - ✅ **Explicit consent** from patients
  - ✅ **Legitimate interests** with appropriate safeguards

  > ⚠️ **If unsure, consult your DPO or legal advisor.** Health data has stricter rules.

  For Professional Services (Therapists, Counselors):

  If you provide therapy, counseling, or similar services where clients may disclose sensitive personal information:

  - ✅ Consider whether you're processing **health data** (mental health, therapy notes)
  - ✅ If yes, follow healthcare guidance above
  - ✅ If no (e.g., business coaching), standard legal basis applies

  For Other Businesses (Salons, Spas, General Services):

  Standard appointment booking = standard personal data. No special considerations unless you're specifically collecting health information (e.g., medical history forms for beauty treatments).

- [ ] **4. Sign the DPA**

  What happens:

  - We send you the Data Processing Addendum (DPA)
  - You review and sign
  - We countersign and send you a copy
  - Done

  Keep the signed copy for your records.

  What's in it: Legal agreement covering how we handle your customers' data, security measures, and your rights.

- [ ] **5. Designate a Data Protection Contact**

  Who: Someone in your organization who handles data protection queries

  Their job:

  - Respond to customer data requests (with our help)
  - Be main contact for DPA-related matters
  - Doesn't need to be a qualified DPO

  Tell us: Name and email of this person

  Examples:

  - **Small business:** Owner or manager
  - **Larger business:** Office manager or compliance officer
  - **Medical practice:** Practice manager or DPO if you have one

While Using Bramforth AI

- [ ] **6. Handle Customer Data Requests**

  If a customer asks for their data:

  1. Email us: info@bramforth.ai
  2. We provide their call recordings/transcripts within 2 business days
  3. You send it to the customer within 30 days (GDPR requirement)

  If a customer wants deletion:

  1. Verify it's legally okay to delete (check retention rules for your industry)
  2. Email us to delete
  3. We confirm deletion in writing

  Industry notes:

  - **Healthcare:** Check medical records retention requirements before deleting
  - **Other businesses:** Usually no special retention requirements for appointment calls

- [ ] **7. Report Any Issues**

  Tell us immediately if:

  - Customers complain about AI or recordings
  - You suspect a data breach
  - You have concerns about data handling

  Contact: info@bramforth.ai

Annual Tasks

- [ ] **8. Review This Arrangement Annually**

  Once per year, check:

  - Privacy notice still accurate
  - DPA still reflects how you're using the service
  - No changes needed to AI scripts or data handling

  We'll remind you when annual review is due.

Industry-Specific Guidance

🥼 Healthcare/Medical Businesses:

Additional considerations for clinics, medical practices, aesthetic clinics:

- Your privacy notice should explicitly mention health data processing
- Consider having patients acknowledge your privacy notice (e.g., during registration or first appointment)
- GMC/NMC/CQC guidance on confidentiality applies to your use of AI
- Medical records retention rules apply (typically 8+ years)
- If you're regulated by CQC, ensure AI use aligns with inspection standards

Legal basis: Healthcare provision (Article 9(2)(h)) typically covers appointment booking conversations where patients mention medical conditions.

💇 Beauty & Wellness Businesses (Salons, Spas, Beauty Therapists):

What's simpler for you:

- Standard privacy notice sufficient (no health data sections needed)
- No special retention requirements (30-day default is fine)
- No regulatory body considerations (no CQC equivalent)
- Same DPA applies, but compliance is more straightforward

Only exception: If you collect medical history forms (e.g., for certain treatments), mention this separately in your privacy notice.

💼 Professional Services (Consultancies, Coaching, Training):

Business consultants, coaches, trainers:

- Standard privacy notice sufficient
- No special data considerations unless you provide therapy/counseling
- Client appointment data = standard personal data
- Retention: 30-day default usually appropriate

Therapists/Counselors:

- If providing mental health therapy, consider this **health data** (Article 9)
- Follow healthcare guidance above for legal basis
- Longer retention periods may apply under professional body rules

🏢 Other Appointment-Based Businesses:

Any business with appointments (mechanics, solicitors, accountants, etc.):

- Standard privacy notice sufficient
- Follow universal sections above
- No special considerations unless processing sensitive data specific to your industry

Professional services with regulatory requirements: Check if your professional body (Law Society, ICAEW, etc.) has specific guidance on AI use.

Optional (Good Practice)

- [ ] **Register with ICO**
  Most UK businesses processing personal data need to register and pay annual fee (£40-60).
  Check: https://ico.org.uk/for-organisations/data-protection-fee/

- [ ] **Keep a Data Processor Register**
  List all your data processors (including Bramforth AI) in a simple spreadsheet.
  Useful for: Compliance audits, knowing who has your data

- [ ] **Train Your Staff**
  Brief staff on:
  - AI is handling some calls
  - How to access recordings if needed
  - Who to contact for data requests

  Examples:
  - **Salon:** "Our AI assistant handles booking calls. If a client asks about their data, contact [Name]."
  - **Clinic:** "Voice AI records calls for appointments. Medical records rules still apply. Contact [DPO] for data requests."

What You DON'T Need to Do

✅ **These apply to ALL businesses:**

- ❌ Hire a Data Protection Officer (unless you're large or high-risk)
- ❌ Conduct formal Data Protection Impact Assessment (we've done this)
- ❌ Get explicit consent before every call
- ❌ Announce "this call is being recorded" on every call
- ❌ Keep recordings forever (automatic deletion after 30 days default)
- ❌ Manage sub-processors (we handle this)
- ❌ Assume healthcare regulations apply if you're not in healthcare

Quick Reference

Your Responsibility	Our Responsibility
Privacy notice	DPA compliance
Legal basis for processing	Secure data storage
Customer data requests (respond to customer)	Customer data requests (provide data to you)
AI greeting script	AI technology
Breach notification to ICO (if required)	Breach notification to you (48 hours)

Common Questions

Q: I run a hair salon. Do I need to worry about "health data"?

A: No, unless you're collecting medical information for treatments. Standard appointment booking = standard personal data.

Q: I'm a therapist. Does this count as health data?

A: Yes, mental health therapy typically involves processing health data. Follow the healthcare guidance in this checklist.

Q: Can customers opt out of AI and speak to a human?

A: Yes, you should configure your AI to offer this option or provide a way for callers to request human handling.

Q: What if a customer complains about the AI recording them?

A: Point them to your privacy notice (which discloses the recording). If they want their recording deleted, contact us and we'll help.

Q: Do I need a lawyer to review the DPA?

A: Not required, but you can if you want. The DPA follows standard UK GDPR templates.

Need Help?

> **Email:** info@bramforth.ai
>
> **Response time:** 2 business days
>
> **Common questions answered in:** DPA Plain English Summary (separate document)

Checklist Complete? ✅

Once you've ticked all boxes in "Before You Start", you're ready to go live.

Estimated total time: 30-60 minutes (mostly updating privacy notice)

Your Business Type Quick Guide

Not sure which sections apply to you? Use this:

Business Type	Special Considerations?	Follow Healthcare Guidance?
Medical/Aesthetic Clinic	Yes - health data	✅ Yes
Hair Salon/Barber	No	❌ No
Beauty Spa/Aesthetician	Only if collecting medical history	❌ Usually no
Therapist/Counselor	Yes - mental health data	✅ Yes
Business Coach/Consultant	No	❌ No
Dentist/Optician	Yes - health data	✅ Yes
Fitness/Personal Training	Maybe - depends on health data collection	⚠️ Check
Other appointment businesses	Unlikely	❌ Probably no