GDPR & THE EU AI ACT — THE PLAIN-ENGLISH GUIDE

What Antek Automation actually needs to do, in normal words. Not legal advice — a practical map.

THE ONE-PARAGRAPH VERSION

Two separate EU rulebooks touch AI voice agents and chatbots. **GDPR** is about personal data — names, numbers, call recordings, transcripts. **The EU AI Act** is about the AI system itself. For a normal reception bot, lead-qualifier or website chatbot, the AI Act mostly just says "tell people they're talking to a robot." GDPR is the one with real day-to-day teeth — because every call and chat is full of personal data.

PART 1: GDPR IN PLAIN ENGLISH

What it is: EU law on handling people's personal data — names, phone numbers, emails, addresses, call recordings, transcripts, CRM notes.

Why it applies to us: Every AI receptionist call and every chatbot conversation captures someone's personal data. That's GDPR's whole territory.

The key roles:

- **Controller** — the client (they decide why the data is collected).
- **Processor** — usually Antek (we handle it on the client's behalf).
- ▲ If we ever reuse a client's call/chat data for our own model training, benchmarking or analytics, we stop being a plain processor and become responsible in our own right. Don't do this without a proper legal setup.

What we need to be able to hand a client, in plain terms:

1. A **Data Processing Agreement (DPA)** — the contract that says how we handle their data.
2. A **subprocessor list** — who else touches the data (OpenAI, Twilio, ElevenLabs, etc.).
3. A **transfer mechanism** if data leaves the EU (Standard Contractual Clauses).
4. **Retention settings** — how long we keep recordings, transcripts, logs.
5. A **deletion/export process** — client can ask for their data back or gone.
6. A **security summary** — how it's protected.
7. **Privacy notice wording** they can put on their site/phone script.

Rule of thumb: minimise what you capture, delete it when you no longer need it, and never let it silently end up in a model you're training on.

PART 2: THE EU AI ACT IN PLAIN ENGLISH

What it is: EU law on the AI system itself — what it's allowed to do, and what it has to disclose.

Who it applies to: Anyone whose AI system is used in the EU, sold into the EU, or affects someone in the EU — even if Antek itself isn't based there.

The one rule that matters for us — Article 50 (transparency):

People must be told they're talking to AI. That's it, for a normal bot.

- **Kicks in: 2 August 2026** (basically now).
- Bots already live before that date get until **2 December 2026** to add the disclosure.

Suggested disclosure wording:

- Voice: "Hi, I'm the AI assistant for [Company]. I can help with bookings, messages, and common questions. I can transfer you to a person if needed."
- Chat: "You're chatting with [Company]'s AI assistant. It can answer questions, collect details, and pass you to the team."

Don't hide that it's AI behind a human-sounding name/persona.

The three risk tiers (only matters if you stray outside normal use):

Tier	What it means	Where a normal Antek bot sits
Limited / transparency	Just disclose it's AI	✓ Receptionist, chatbot FAQ, lead capture, booking, reminders — this is us
High-risk	Heavy compliance regime	✗ Only if used for HR/recruitment, credit scoring, insurance pricing, education access, emergency dispatch, law enforcement, biometrics
Prohibited	Banned outright	✗ Manipulative/deceptive AI, exploiting vulnerable people, social scoring, scraping faces into a database, emotion-reading at work/school

Bottom line: a standard AI receptionist or chatbot that answers FAQs, takes messages, qualifies leads and books appointments is **not** high-risk. It becomes a problem only if it starts making real decisions about someone's job, credit, insurance, education, or safety.

PART 3: EPRIVACY — THE QUIET THIRD RULEBOOK

Covers call recording notices and marketing consent. Two practical points:

- If calls are recorded/transcribed, **say so at the start of the call**.
- If the bot ever triggers marketing texts/emails/calls, the client needs proper consent under their local rules — the AI Act does not cover this, GDPR/ePrivacy does.

PART 4: WHAT THIS MEANS FOR ANTEK, PRACTICALLY

Build these into every deployment as default settings, not extras:

- AI disclosure line, always, at the start.
- A human handoff/escalation option, always.
- Never let the bot claim to be human.
- Never let the bot make the final call on anything legal, financial, medical, housing or employment-related.
- Don't infer emotion, health, or protected characteristics.
- Don't train shared/global models on client conversations unless separately agreed in writing.
- Keep transcripts only as long as genuinely useful.
- Keep a log of what the bot did — prompts, routing, CRM writes, handoffs.

Have a standard "compliance pack" ready to hand any EU client:

1. What the product does / doesn't do (explicit exclusion list: no HR screening, credit, insurance, emergency dispatch, biometrics).
2. AI disclosure scripts (voice + chat).
3. Human escalation design.
4. Data flow diagram (caller → bot → AI/voice provider → CRM/calendar).
5. Subprocessor list + hosting regions.
6. Retention defaults.
7. DPA + SCC reference.
8. Security summary.
9. Incident process (what happens if the bot hallucinates, misroutes, or leaks data).

Sales line that's actually true:

> "AI Act-ready voice and chat automation for small businesses: clear AI disclosure, human fallback, GDPR-aware data handling, and no risky automated decisioning."

Objection handling, if a prospect worries about "the AI Act":

> "It doesn't ban business chatbots or AI receptionists. For ordinary reception, FAQs, lead capture and booking, the only real requirement is telling people they're dealing with AI. The heavy rules are for hiring, credit, insurance, education, biometrics, law enforcement and emergency dispatch — categories we deliberately stay out of."

PART 5: UK VERSION — WHAT'S DIFFERENT

Big point: there's no UK AI Act. UK doesn't have an EU-style horizontal AI law for ordinary receptionist/chatbot use. The real UK compliance burden is **UK GDPR + PECR + Ofcom + consumer protection**, not an AI-specific statute. Don't sell "UK AI Act compliant" — it doesn't exist for this use case.

Sell instead: "UK GDPR, PECR, and telecoms-aware AI receptionist implementation."

Still disclose AI at the start — not legally mandated the way the EU AI Act does it, but it's the safest default and matches EU practice.

PECR — the UK's sharpest edge (marketing calls/emails/SMS):

- Screen against **TPS/CTPS** before any live marketing call.
- Never call anyone who's objected.
- State who's calling; show a real, callable number.
- **Automated marketing calls are much stricter** — don't use an AI voice agent for unsolicited automated sales calls without specific consent.
- Postal letters remain the lowest-risk UK cold-outreach channel — keep using them as the default.
- PECR fines now aligned with UK GDPR levels: **up to £17.5m or 4% of turnover.** Treat cold-outreach compliance as serious, not admin.

Data (Use and Access) Act 2025: updated UK data law — makes automated decision-making somewhat more permissive, but big/solely-automated decisions still need safeguards. Doesn't change the core rule: don't let the bot make final calls on anything legally significant.

Call recording notice (UK wording):

> "Calls may be recorded and transcribed so we can handle your enquiry, keep accurate records, and improve service."

Ofcom / Calling Line ID: use real, assigned caller IDs. Never spoof numbers. Displayed number must be callable back.

Consumer protection / GEO claims: no fake reviews, no hidden incentivised reviews, no "guaranteed ChatGPT ranking" claims. CMA is actively enforcing on fake reviews.

Online Safety Act: only a real risk if a chatbot allows user-to-user content, search, or open-ended public chat. Ordinary single-business FAQ/lead-capture bots are low risk — keep them scoped that way on purpose.

UK risk table (same shape as EU, different flavour):

Use case	UK risk	Obligation
Inbound AI receptionist	Low-medium	AI disclosure, call-recording notice, UK GDPR, human escalation
Website FAQ/lead chatbot	Low-medium	AI disclosure, privacy notice, scope discipline
Appointment booking	Low-medium	Lawful basis, transparency
Lead scoring for sales priority	Medium	Profiling transparency, no protected-trait inference
Unsolicited outbound AI sales calls	**High**	Avoid unless explicit consent + PECR review
Solicitor/legal chatbot giving advice	High	Intake/admin only unless legally supervised
HR screening, credit/insurance decisions, health triage, emergency dispatch	High	Avoid for Antek's ICP

UK compliance pack — same 16-item shape as the EU one, plus: controller/processor role matrix, UK IDTA/UK SCC Addendum for transfers, PECR checklist, TPS/CTPS suppression-list process.

UK sales line:

> "UK-ready AI receptionist and chatbot automation: clear AI disclosure, human fallback, UK GDPR-aware data handling, PECR-safe outreach, and no risky automated decisioning."

UK objection answer:

> "The UK doesn't have a broad EU-style AI Act for standard business receptionists and chatbots. The real compliance issues are UK GDPR, PECR, call-recording transparency, telecoms caller-ID rules, and consumer protection. We design around clear AI disclosure, human escalation, limited data capture, sensible retention, and no high-stakes automated decisions."

If selling to both: keep EU and UK compliance packs separate — EU clients still need the EU AI Act pack even if Antek is UK-based; UK clients don't need "AI Act" language at all.

PART 6: THE BASELINE DOCUMENTATION EVERYONE NEEDS — EVEN "WE DON'T REALLY USE AI"

There's a lot of fearmongering doing the rounds about the AI Act right now. One thing is genuinely true and worth taking seriously: **you don't need a "certified AI Officer," but you do need baseline documentation — and "we're not sure which AI tools we use" stops being a defensible answer.**

Article 4 — AI literacy (already in force, not a future date):

- Applies since **2 February 2025** — this is not part of the 2 August 2026 milestone, it's already live.
- Applies to **every provider and deployer of an AI system, at every risk tier** — not just high-risk.
- Requires the organisation to ensure staff have "sufficient AI literacy" — understanding what the AI tools do, their risks, and how they're used.
- The obligation to **document** that literacy sits with the company. An auditable record (who uses what tool, what training they've had, what the tool is for) is the practical way to meet it.

Why 2 August 2026 matters on top of that:

- High-risk Annex III obligations (biometrics, critical infrastructure, education, employment, essential services, law enforcement, migration, justice, democratic processes) become enforceable.
- Article 50 transparency duty (AI disclosure — see Part 2) also activates this date.
- Regulators can reasonably expect companies to be able to show at least minimum documentation by this point — not hundreds of pages, but something.

The GDPR angle the post makes well: an AI system can be low-risk under the AI Act while still being a real GDPR problem. AI phone assistants, chatbots, meeting transcription tools, CV-screening tools, and generative AI tools are the textbook examples — exactly Antek's product category. Low AI Act risk tier does not mean low data protection risk. Treat them as two separate checklists, not one.

Minimum baseline documentation every company (including Antek) should have — proportionate, not hundreds of pages:

1. An **AI tool inventory** — which AI tools/models are used, by whom, for what purpose (including vendor tools like OpenAI, ChatGPT, Retell, transcription tools — not just custom-built systems).
2. **Staff AI-literacy records** — evidence people using/configuring AI tools understand what they do and their risks (Article 4).
3. **Risk classification per use case** — a one-line note on why each AI use sits in "limited/transparency" and not "high-risk" (see Part 2 table).
4. **Supplier/vendor due diligence** — even if Antek's own system is low-risk, the upstream model/voice providers (OpenAI, Anthropic, Retell, Twilio, ElevenLabs) need to be assessed and listed. This is the "assessment and control of suppliers" point — it applies even to companies that think they "don't use AI directly."
5. **Data flow note** — tied to the GDPR data flow diagram already recommended in Part 4/5.

Penalties — why this isn't optional admin:

Violation tier	Maximum fine
Prohibited practices (Article 5)	€35m or 7% of global turnover, whichever is higher
Other operator obligations (e.g. missing/incomplete documentation, governance failures)	€15m or 3% of global turnover, whichever is higher
Misleading information to authorities	€7.5m or 1% of global turnover, whichever is higher

SME/start-up fines use the same tiers but the lower of the fixed amount or percentage applies — still real money, not a rounding error.

What Antek should actually do with this:

- Antek's own compliance pack (Parts 4 and 5) already covers most of items 1–5 above for the products Antek builds. The gap this section closes is Antek's own internal use of AI tools (writing outreach, running the agent stack, using LLM vendors for internal work) — that needs its own mini-inventory and literacy record, separate from client-facing product documentation.

- When positioning to clients: "we help you get from 'we don't know what AI tools are in use' to a documented, defensible baseline" is a legitimate sales angle in its own right, distinct from the receptionist/chatbot pitch.

QUICK REFERENCE CHECKLIST

- ☐ Bot discloses it's AI at the start of every call/chat
- ☐ Human handoff option exists
- ☐ No high-risk use case in scope (HR, credit, insurance, emergency, biometrics, education access)
- ☐ DPA + subprocessor list ready to send
- ☐ Retention periods defined for recordings/transcripts/logs
- ☐ Deletion/export process exists
- ☐ No client data used for model training without separate written agreement
- ☐ Call-recording notice included if calls are recorded
- ☐ Marketing messages have proper consent basis (not covered by AI Act)
- ☐ (UK) TPS/CTPS screened before any live marketing call
- ☐ (UK) No unsolicited automated AI sales calls without specific consent
- ☐ (UK) Caller ID is real, assigned, not spoofed
- ☐ (UK) No fake/incentivised reviews or unsubstantiated "guaranteed AI ranking" claims
- ☐ (UK) Chatbot scoped to business support/lead capture, not open public chat
- ☐ AI tool inventory exists (which tools, who uses them, what for) — including Antek's own internal AI use
- ☐ Staff AI-literacy/training record exists (Article 4, already in force since Feb 2025)
- ☐ Upstream AI vendors/suppliers assessed and listed, not just Antek's own system

KEY DATES

Date	What happens
2 Aug 2026	EU AI Act Article 50 transparency duty (AI disclosure) becomes active
2 Dec 2026	Deadline for EU-facing bots already live before Aug 2026 to add disclosure
19 Jun 2025	UK Data (Use and Access) Act 2025 received Royal Assent
2 Feb 2025	EU AI Act Article 4 (AI literacy) already in force — applies to every risk tier, not just high-risk

SOURCES (OFFICIAL — EU)

- EU AI Act full text: eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- EU AI Act timeline: ai-act-service-desk.ec.europa.eu
- EU Commission transparency guidelines (29 Jul 2026): digital-strategy.ec.europa.eu
- GDPR overview: commission.europa.eu/law/law-topic/data-protection_en
- ePrivacy Directive: eur-lex.europa.eu (Directive 2002/58/EC)
- EU AI Act Article 4 (AI literacy): artificialintelligenceact.eu/article/4/
- EU AI Act Article 99 (penalties): artificialintelligenceact.eu/article/99/

SOURCES (OFFICIAL — UK)

- GOV.UK, "A pro-innovation approach to AI regulation" white paper: gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
- ICO, "Guidance on AI and data protection": ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/
- ICO, business-to-business marketing / live call rules: ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/

- Legislation.gov.uk, Data (Use and Access) Act 2025: legislation.gov.uk/ukpga/2025/18/contents
- GOV.UK, Data (Use and Access) Act 2025 factsheets (incl. PEC Regulations): gov.uk/government/publications/data-use-and-access-act-2025-factsheets
- Ofcom, Calling Line Identification guidance: ofcom.org.uk/phones-and-broadband/phone-numbers/calling-line-identification
- Ofcom, "AI chatbots and online regulation": ofcom.org.uk/online-safety/illegal-and-harmful-content/ai-chatbots-and-online-regulation-what-you-need-to-know
- GOV.UK, Online Safety Act explainer: gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
- CMA, fake and misleading reviews guidance: gov.uk/government/news/fake-and-misleading-reviews-5-businesses-under-cma-investigation

Confidence: High on the legal facts and dates (official EU and UK sources). Medium-high on how this plays out client-by-client — exact needs vary by sector, data flow, and (for UK) evolving ICO/Ofcom guidance on automated decisions and Online Safety Act scope.