STACKBASTION

Record of Processing Activities (RoPA) Template

A fill-in template for Article 30 GDPR, sized for a solo founder or small team running an AI-built app. One copy of this table per distinct processing activity (e.g. "user signup and accounts", "newsletter", "support tickets").

When you actually need this

Article 30(5) exempts organisations under 250 employees, unless the processing is not occasional, could risk someone's rights, or includes special-category data. Most apps handling user accounts, payments, or health/location data process regularly enough that the exemption doesn't apply in practice. When in doubt, keep the record. It costs an afternoon and it's the first document a regulator or an enterprise customer's security review will ask for.

Field	Your entry
Processing activity name e.g. "User signup and account management"	
Purpose of processing Why you collect and use this data. Be specific, not "to run the app".	
Categories of data subjects Who the data is about: customers, employees, website visitors.	
Categories of personal data Name, email, IP address, payment details, usage logs, etc.	
Special category data? (Y/N) Health, biometric, religious, political, or similar. If yes, note the legal basis for processing it.	
Legal basis for processing Consent, contract, legitimate interest, legal obligation, etc.	
Recipients / processors Who else touches this data: your database host, email provider, payment processor, analytics tool.	
Third-country transfers Does any processor store or access data outside the EU/UK? If yes, note the transfer mechanism (e.g. SCCs, adequacy decision).	
Retention period How long you keep this data, and what triggers deletion.	

Field	Your entry
Technical & organisational security measures Encryption at rest/in transit, access controls, backup policy, who has admin access.	
Last reviewed Date, and by whom.	

How to use this

Fill one table per processing activity, not one table for your whole app. Most small apps end up with 4 to 8 activities: accounts, payments, support, marketing email, analytics, and any AI/LLM calls that send user data to a third-party model provider. Keep the finished record somewhere your team can find it fast. "We don't know, let us check" is a worse answer to a regulator than a slightly imperfect record.
