✅ Marketbotics CPRA Compliance Checklist (California AI Integration)

Purpose:
Ensure all AI integration projects implemented by Marketbotics and its California clients comply with the **California Privacy Rights Act (CPRA)** and related obligations under the **California Consumer Privacy Act (CCPA)** — while maintaining transparency, data minimization, and consumer trust.

---

1. Governance & Applicability

Requirement	Description	Status	Notes / Evidence
1.1 Business Applicability	Confirm the client or Marketbotics entity meets CPRA applicability thresholds (>$25M revenue, >100,000 consumers' data/year, or >50% revenue from data sale/sharing).	☐	
1.2 Designate Privacy Lead	Assign a Data Protection Officer (DPO) or Privacy Officer to oversee AI system data compliance.	☐	
1.3 Data Mapping & AI Inventory	Maintain a current map of data flows and an inventory of AI systems processing personal data (purpose, source, storage).	☐	
1.4 Policies & Training	Ensure employees are trained on CPRA requirements and AI data-handling protocols.	☐	

---

2. Data Collection & Processing

Requirement	Description	Status	Notes / Evidence
2.1 Notice at Collection	Provide a clear privacy notice before collecting personal information — specify categories, purposes, and retention.	☐	
2.2 AI-specific Disclosure	State if AI or automated decision-making systems use personal data; explain purpose and scope in plain language.	☐	

Requirement	Description	Status	Notes / Evidence
2.3 Data Minimization	Limit data collection to what's necessary for the AI's function; avoid unnecessary sensitive data ingestion.	☐	
2.4 Purpose Limitation	Use data only for disclosed business purposes; update notices if new AI use cases arise.	☐	
2.5 Retention Policy	Document data retention periods for AI logs, model training data, and outputs; implement deletion schedules.	☐	
2.6 Sensitive Personal Information Controls	Apply extra protection and purpose limits for SPI (health, biometrics, race, location, etc.). Provide a "Limit Use of SPI" mechanism.	☐	

---

3. Consumer Rights Enablement

Requirement	Description	Status	Notes / Evidence
3.1 Right to Know / Access	Provide individuals with access to their personal data used in AI systems upon request.	☐	
3.2 Right to Delete	Implement deletion workflows for data used in AI processing and model retraining.	☐	
3.3 Right to Correct	Allow consumers to correct inaccurate data feeding AI logic or profiles.	☐	
3.4 Right to Opt-Out (Sale/Sharing)	Offer a "Do Not Sell or Share My Info" link; ensure AI modules respect opt-out status (e.g., no personalized models post opt-out).	☐	

Requirement	Description	Status	Notes / Evidence
3.5 Global Privacy Control (GPC)	Detect and honor browser-level GPC signals; auto-opt-out from data sale/sharing upon signal detection.	☐	
3.6 Right to Limit SPI Use	Allow users to limit how their sensitive personal information is used in AI features.	☐	
3.7 Right to Automated Decision Information	Upon request, provide meaningful information about AI logic and factors influencing automated decisions.	☐	

---

4. Vendor & Third-Party Management

Requirement	Description	Status	Notes / Evidence
4.1 Data Processing Agreements (DPAs)	Execute CPRA-compliant contracts with all vendors handling personal data. Include prohibitions on selling/sharing data.	☐	
4.2 Vendor Inventory	Maintain a list of service providers and contractors with access to AI-related data, including data flow diagrams.	☐	
4.3 Sub-Processor Controls	Require vendors to seek approval before engaging new sub-processors; flow down same obligations.	☐	
4.4 Vendor Due Diligence	Evaluate vendor privacy/security posture and AI use; verify compliance with CPRA and CCPA.	☐	
4.5 Audit Rights	Reserve the right to audit vendors' handling of Marketbotics or client data.	☐	

---

5. Security & Data Protection

Requirement	Description	Status	Notes / Evidence
5.1 Access Controls	Enforce role-based access to AI data, embeddings, and logs; restrict admin privileges.	☐	
5.2 Encryption	Apply encryption at rest and in transit for all personal data handled by AI.	☐	
5.3 Incident Response	Maintain breach response plan covering AI system vulnerabilities and data exposures.	☐	
5.4 Logging & Monitoring	Log AI system interactions, retrieval queries, and access to personal data.	☐	
5.5 Anonymization & Aggregation	Anonymize or aggregate personal data for model training whenever possible.	☐	
5.6 Security Review of AI Vendors	Confirm external AI API providers (e.g., OpenAI, Google Vertex, Anthropic) meet security and privacy standards.	☐	

---

6. Transparency, Auditability & Accountability

Requirement	Description	Status	Notes / Evidence
6.1 Explainability	Document logic behind AI systems, especially for high-impact decisions (e.g., hiring, credit, healthcare).	☐	
6.2 Data Protection Impact Assessment (DPIA)	Conduct DPIAs or Algorithmic Impact Assessments for AI with potential privacy or bias risks.	☐	
6.3 Regular Audits	Schedule annual AI privacy and ethics audits; track remediation items.	☐	
6.4 Accuracy Verification	Periodically test AI outputs for accuracy and bias; document findings.	☐	

Requirement	Description	Status	Notes / Evidence
6.5 Compliance Reporting	Prepare internal compliance report (or CPRA readiness statement) summarizing status for executives or clients.	☐	

---

7. User Experience & Notices

Requirement	Description	Status	Notes / Evidence
7.1 Privacy Policy Update	Update website and app privacy policies to mention AI and automated decision-making usage.	☐	
7.2 "Your Privacy Choices" Page	Provide a dedicated, easy-to-find preference center with opt-out/limit options.	☐	
7.3 AI Transparency Notice	On any AI interface (chatbots, forms, or dashboards), clearly label AI usage and data handling practices.	☐	
7.4 Accessibility Compliance	Ensure notices and opt-out interfaces meet accessibility standards (WCAG 2.1+).	☐	

---

8. Continuous Improvement

Requirement	Description	Status	Notes / Evidence
8.1 Policy Review Cycle	Review and update CPRA-related policies annually or upon regulatory change.	☐	
8.2 Staff Retraining	Re-train staff annually on CPRA, privacy, and AI compliance protocols.	☐	
8.3 AI Model Review	Review AI models regularly for drift, privacy compliance, and bias.	☐	
8.4 Stakeholder Feedback	Collect and analyze user/employee feedback on AI transparency and data usage practices.	☐	

Requirement	Description	Status	Notes / Evidence
8.5 Future-Proofing	Monitor new California AI regulations (e.g., Automated Decision-Making Technology regulations) and update practices accordingly.	☐	

📘 Checklist Summary Table

Category	Total Items	Complete	In Progress	Pending
Governance	4			
Data Processing	6			
Consumer Rights	7			
Vendor Mgmt	5			
Security	6			
Auditability	5			
User Notices	4			
Continuous Improvement	5			