# 🔒 GDPR Compliance + API Usage Control Panel

## ✅ Module Overview

This module ensures that the SaaS platform strictly adheres to global privacy and data usage standards (especially GDPR), while offering each brand owner complete transparency and control over how third-party APIs are used across the system. It is crucial for building trust with clients, protecting user data, and staying legally compliant across jurisdictions.

This panel also gives Superadmins fine-grained control over API usage limits, throttling rules, audit logs, and billing alignment for each brand using third-party resources.

## 🎯 Goals

* Comply with GDPR and similar global data protection laws.
* Allow full audit and control over 3rd-party API access, data syncs, AI usage.
* Let customers manage consent, deletion, and data portability requests.
* Track per-module API usage, cost, and limits by brand.
* Prevent overuse and abuse of AI tools or integrations.

## 🧩 Features Breakdown

### 1. **GDPR Settings Panel (Brand-Level)**

* **Consent Management:**
  + Consent banners + checkboxes embedded in widgets/forms (UGC campaigns, comments, profile pages).
  + Records user consent timestamp and metadata in a separate audit log.
* **Data Rights Interface (Frontend):**
  + “Download My Data” request button.
  + “Delete My Account + All Data” request.
  + Option to revoke previous consent.
* **Data Exports:**
  + JSON/CSV export of customer data: interactions, orders, replies, UGC entries, campaigns joined, reward points.
* **Privacy Policy Link:**
  + Auto-injected into all user-facing pages, UGC forms, and email footers.

### 2. **Superadmin API Usage Dashboard**

* View all 3rd-party APIs used per brand:
  + GPT/OpenAI
  + Facebook/Instagram Graph API
  + WhatsApp Business Cloud API
  + Shopify/WooCommerce APIs
  + Email/SMS gateways (e.g., Twilio, SendGrid, WhatsApp)
* Metrics Tracked:
  + API calls/day/week/month
  + Token usage for GPT calls
  + Errors, retries, fallbacks triggered
  + Latency and rate limits
* Tools:
  + Throttling rules: Define daily/weekly quotas per brand/module/API
  + Cost mapping: View API cost breakdown per feature/brand
  + Disable toggle for any integration at brand or global level
  + Alerts for overage or abuse

### 3. **Compliance Engine Services**

* **Data Audit Logger**:
  + Tracks every data write, sync, or API response involving PII
  + Logs brand, timestamp, endpoint, user ID, payload hashes
* **Data Access Request Handler**:
  + When customer clicks “Delete My Data”, notifies brand admin
  + Auto-deletes data if no response within X days (configurable)
  + Purges data across:
    - Comment logs
    - UGC
    - Reward profile
    - CRM fields
    - Campaign history
* **Consent Syncer:**
  + Pushes/revokes consent from customer to 3rd party if supported (e.g., Shopify customer deletion API, FB data deletion callback, etc)

## 🔐 Backend Tables

* api\_usage\_logs:
  + id, brand\_id, module, api\_name, call\_count, tokens\_used, cost\_estimate, timestamp
* consent\_logs:
  + user\_id, brand\_id, consent\_type, timestamp, source
* data\_deletion\_requests:
  + user\_id, brand\_id, request\_time, status, completion\_time, modules\_affected
* gdpr\_settings:
  + Per brand configuration: auto-delete time, consent enforcement toggle, export enablement

## 📊 Admin Insights

* Weekly email to Superadmin:
  + API usage summary across brands
  + Consent violations or pending deletion actions
  + Brands nearing quota
* Brand-level dashboard shows:
  + Their current quota & cost estimation
  + Last 30 days’ usage
  + Toggle consent & deletion workflow

## 🧠 Benefits

* Prevents legal/regulatory risks at scale
* API usage tracking keeps server cost optimized
* Puts brands in control of customer privacy
* Adds transparency and confidence to clients

✅ This document is ready. Let me know if you want GDPR request flows or API usage charts designed next.