DIGITAL OMNIBUS

WHAT CAN COMPANIES DO NOW TO PREPARE

1 Audit current consent mechanisms

Review existing consent banners and flows against proposed requirements. Check whether "Accept All" and "Reject All" buttons have equal visual prominence and interaction complexity. Can individuals refuse all non-essential purposes with a single click from the first banner layer? Are consent requests presented repeatedly after refusal?

Document which purposes currently rely on consent versus legitimate interest or other legal bases. Organizations that already follow consent best practices will have less work when requirements become mandatory.

2 Map data processing purposes

Create a detailed inventory of processing purposes across marketing, analytics, and operations. For each purpose, document what personal data is processed, which legal basis applies, which third-party processors are involved, and where consent signals need to propagate.

This mapping exercise often reveals purposes that should rely on consent but currently don't, or processing that could shift to legitimate interest with proper documentation.

3 Evaluate CMP capabilities

Assess whether your consent management platform (CMP) infrastructure can accommodate Digital Omnibus requirements. This entails:

- Single-click accept/reject mechanisms
- Six-month moratorium tracking after refusal
- Machine-readable signal recognition (when standards are published)
- Purpose-based consent granularity
- Consent signal propagation to all downstream systems
- Audit trails and consent lineage documentation

If current capabilities fall short, investigate CMP upgrades or alternatives that provide the flexibility needed to adapt as requirements evolve.

Discover the 8 leading consent management platforms of 2025.

4 Test consent signal propagation

Verify that consent choices actually propagate to every system that processes personal data. Common failure points include analytics platforms that load before consent is captured, marketing automation systems that don't receive updated consent status, and third-party tags that fire regardless of consent state.

Use browser developer tools, tag monitoring solutions, and consent signal validators to identify and remediate these gaps.

5 Prepare for machine-readable signals

While technical standards for browser-level preference signals aren't finalized, organizations can prepare by monitoring standard development through W3C and other standards bodies, engaging with browser vendors to understand implementation timelines, and building CMP architectures that can accept consent input from multiple sources.

Plan how to reconcile browser-level preferences with granular purpose-based consent. Consider how media service provider exemptions might apply to specific business lines.

6 Review incident reporting processes

Assess current breach notification and incident reporting procedures against the single-entry point model. Which incidents currently require reports under the GDPR, NIS2, DORA, or other frameworks? What information overlap exists across different reporting requirements?

Early preparation for consolidated reporting reduces scrambling when the system goes live.

7 Document AI processing legal bases

For organizations developing or deploying AI systems, conduct legitimate interest assessments for AI model training using personal data, bias detection using special category personal data, and AI system performance testing.

Document these assessments now, before the Digital Omnibus clarifies that legitimate interest can apply. If legitimate interest doesn't withstand scrutiny, organizations will need consent infrastructure for AI development activities.

8 Build cross-functional alignment

Digital Omnibus compliance spans legal, privacy, marketing, product, and technology functions. Establish working groups that monitor legislative developments, assess business impact, coordinate implementation planning, identify budget requirements, and align on risk tolerance.

Organizations where compliance, marketing, and technology teams work in silos struggle to implement complex regulatory changes effectively.