COMPLIANCE FACT SHEET

Digital compliance and governed product information

Midiacode helps organizations connect physical products and packaging with governed digital information. This fact sheet describes platform capabilities and should not be interpreted as legal advice or a certification statement.

Digital Product Passport

Dynamic digital product experiences can provide structured information about products, materials, provenance, circularity, compliance and related evidence, subject to the applicable regulation and data model.

Electronic Product Information

Digital leaflets and ePI-style experiences can replace or complement paper information with controlled, updateable and multilingual mobile delivery.

PPWR-oriented workflows

The platform can support digital carriers, declarations, recycling guidance, product data and API-driven deployment across product catalogs.

Smart Packaging

Packaging becomes a governed digital touchpoint for information, accessibility, post-purchase engagement, traceability and analytics.

GOVERNANCE

Controlled publication and evidence

Versioned content

Published information can be created, reviewed, scheduled, localized, updated and retired through a controlled lifecycle.

Auditability

Workspace governance and audit trails can record relevant publishing changes, including who changed what and when, according to the configured scope.

Access control

SSO, roles, permissions and groups help restrict sensitive content and publishing operations to authorized users.

Portable carriers

Dynamic QR Codes and short links can preserve the physical carrier while allowing governed digital content to evolve.

Evidence workflows

Reports, exports and linked documents can support internal reviews, supplier evidence and regulatory-readiness processes.

Human responsibility

Regulatory interpretation, approval of claims and final product information remain the responsibility of the organization and its qualified advisors.

SECURITY AND INFORMATION MANAGEMENT

Security controls and quality operating model

Information security policy

Midiacode maintains a documented information-security policy and related procedures; confidential versions are not reproduced in this public fact sheet.

Quality policy

The quality system is based on continuous improvement, internal audits, indicators, risk management and controlled procedures.

Observability and security

Documented procedures address operational visibility, security monitoring and response practices.

Software development

A controlled software-development procedure supports requirements, implementation, review, testing and release.

Resilience

Disaster recovery, backup and recovery and infrastructure-management procedures support operational continuity.

Document control

Policies, procedures, models and records are maintained through a document-control process.

PLATFORM CAPABILITIES

Technical mechanisms supporting compliance

Dynamic delivery

One physical carrier can deliver different languages, profiles, locations or versions through controlled rules.

API automation

ERP, product-management and other corporate systems can automate the deployment and update of digital product information.

Analytics

Scans, views and interactions provide operational visibility and help identify gaps in content delivery.

Accessibility

Mobile-optimized content and accessibility features can improve access for diverse users, including Libras-ready experiences where implemented.

Serialization

Unique or serialized QR Codes can support product-level journeys, traceability and anti-fraud intelligence, subject to the selected implementation.

Availability

Service levels and uptime commitments are defined in the applicable agreement; they are not assumed solely from the platform description.

SCOPE AND LIMITATIONS

What this fact sheet does and does not claim

Platform capability

The document describes technical capabilities that may be configured for a specific implementation.

No legal opinion

Regulatory applicability, deadlines, product classification and evidence sufficiency require review by the customer and qualified legal or regulatory specialists.

No automatic compliance

Using a QR Code or digital platform does not by itself make a product compliant.

Implementation scope

Data sources, approval workflows, integrations, retention, security controls and service levels must be agreed for each project.

Confidential materials

Detailed security, quality, SLA and operational documents are available under the appropriate access conditions.

Current documentation

The platform and its procedures evolve through controlled improvement; the applicable contractual and technical documents prevail.