MCP NET

DDRC FOR MOBILE CARRIERS
Reduce complaints, fines and brand damage

METHODOLOGY
The holistic journey of Due Diligence and Risk Control (DDRC) to protect the mobile carriers' DCB ecosystem

- PARTNER ACCREDITATION
- SECURITY CHECKS & PEN TESTING
- COMPLIANCE SUPPORT
- DDRC SECURE STORAGE
- GOVERNANCE AND REPORTING
- CODE OF CONDUCT & COMPLIANCE ADVICE
- 3RD PARTY CONSENT
- CUSTOMER CARE TESTING
- ANTI-FRAUD SOLUTIONS
- SERVICE ONBOARDING & GO LIVE
- ESCALATION MANAGEMENT
- AD MONITORING

Explore best practice below

DUE DILIGENCE
Ensure you only partner with reputable companies

PARTNER ACCREDITATION
Ensure that company registrations align, including regulatory and government requirements, examine the company's operating history and conduct additional online investigations to identify any other related entities.

SECURITY CHECKS & PEN TESTING
Verify that details match, conduct searches across multiple sources to uncover any adjudications or evidence of bad practice, director checks, evaluate traffic sources and affiliate partnerships, and perform penetration testing and other security checks on partners' platforms.

DDRC SECURE STORAGE
Securely store accreditation, security audits, policies and other documentation in an auditable, tamperproof data management system to demonstrate compliance.
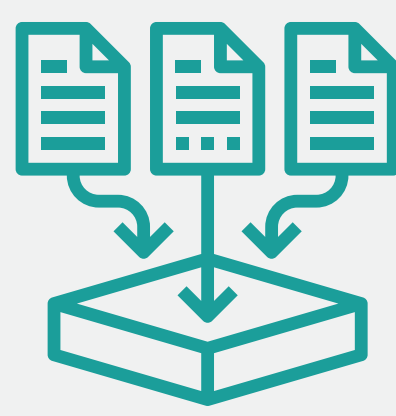
CODE OF CONDUCT
Develop a Code of Conduct, to protect customers and the brand from the negative impact of fraudulent and non-compliant activities and grow a sustainable DCB business.

Check services on your network are compliant before they go live

SERVICE ONBOARDING & GO LIVE
Review ad banners for compliance issues, such as identifying misleading content, test the ad flow to ensure a compliant customer journey, and record the entire flow for audits.

CUSTOMER CARE TESTING
Test all customer care channels in the value chain to ensure they comply with regulations and Code of Conduct.

RISK CONTROL
Ongoing risk management for live services on your network

ESCALATION MANAGEMENT
Ensure compliance issues are documented and escalated to the appropriate team, and an audit trail of actions taken to identify, notify, and rectify the compliance issues ensures transparency and accountability

3RD PARTY CONSENT VERIFICATION
Consent to Charge is managed by a 3rd party solution providing a full audit trail of the transaction and customer journey.

AD MONITORING
Monitor all ads on the network for compliance issues, capture a record of the test from the ad banner to the payment page, and actively track approved services to evaluate their ongoing compliance status.

DATA ANAYLTICS
Utilise platforms that allow you to monitor key metrics for trends and anomalies to aid decision-making and governance and reporting.

ANTI-FRAUD SOLUTIONS FOR PAYMENT PAGES
Protect payment pages from technical fraud, such as malware, with anti-fraud solutions that identify and block suspicious transactions.

COMPLIANCE EXPERTS
Leverage the expertise of compliance specialists in the mVAS/DCB space to provide additional support and bespoke services as an extension of your team.

Speak to your account manager or visit mcpinsight.com/ddrc-as-a-service for more information.

MCP INSIGHT