MONACO CREATIVE · LEAD MAGNET

Loi 1.565 Marketing Compliance Checklist

A Monaco-specific operational checklist covering the deltas between Loi 1.565 and GDPR. For brands whose marketing activity touches Monaco-based prospects, residents, or data subjects. Use this before launching a campaign, integrating a new vendor, or filing with the APDP.

> *This checklist is editorial guidance from a Monaco marketing practitioner. It is not a legal opinion. For binding legal certification, consult a Monaco-licensed attorney. 38 actionable items across 8 domains.*

A. Lawful basis 5 items

- [ ] Each marketing channel has a documented lawful basis (consent, legitimate interest, contract, legal obligation, vital interest, public interest).
- [ ] Legitimate-interest assessments (LIA) are written, dated, and stored for every direct-marketing flow not relying on consent.
- [ ] The Loi 1.565 article corresponding to the chosen basis is cited in the internal record of processing activities (ROPA).
- [ ] Children under 15 are excluded from marketing data collection unless verifiable parental consent is on file (Loi 1.565 sets the digital-consent threshold at 15, not 16 as default GDPR).
- [ ] No marketing flow relies on "soft opt-in" alone for non-customers domiciled in Monaco — the APDP has held that this defence does not survive the 2024 reform.

B. Consent — cookies + marketing 6 items

- [ ] Cookie banner has equally prominent "accept" and "reject" buttons. No pre-ticked boxes. No dark patterns (cookie wall, nag screens, hidden reject).
- [ ] Cookie consent is logged with timestamp, version of the banner, IP, and consent string. Logs retained 3 years minimum.
- [ ] Granular per-purpose toggles for analytics, advertising, personalisation, social, third-party — not a single bundled "accept all".
- [ ] APDP-compliant analytics deployment if measured: server-side, no third-party transfer outside Monaco/EU without explicit basis.
- [ ] Marketing email opt-in is double-opt-in for prospects, with audit trail showing both clicks (initial + confirmation) timestamped.
- [ ] Marketing SMS / WhatsApp opt-in is explicit; consent is captured separately from the email channel and stored with channel attribution.

C. Notice + transparency 5 items

- [ ] Privacy notice is bilingual (FR primary, EN where audience justifies). Plain language, not "translated boilerplate".
- [ ] Notice names the controller, DPO contact, lawful basis per processing, retention period, and APDP as the supervisory authority (not CNIL).
- [ ] Notice discloses cross-border data flows (which countries, which mechanism — adequacy, SCCs, BCRs, derogation).
- [ ] Last-updated date visible on the notice. Material changes trigger fresh consent capture, not silent updates.
- [ ] Cookie notice and privacy notice are linked from every footer and from every form submission page.

D. Data subject rights 5 items

- [ ] Documented procedure for access, rectification, erasure, restriction, portability, and objection requests. Response within 30 days.
- [ ] APDP-compliant contact channel (dedicated email or web form) for data-subject requests. Acknowledgement within 72 hours.
- [ ] Identity verification process for rights requests — proportionate, not abusive (no demanding scans of ID for low-risk queries).
- [ ] Internal log of rights requests handled, with outcome and timing, retained for APDP audit.
- [ ] "Right to object" to direct marketing is honoured immediately, not at the end of a campaign cycle.

E. Cross-border transfers 4 items

- [ ] Inventory of all marketing-tool vendors that store, process, or have access to Monaco-resident data, including their data-residency country.
- [ ] Adequacy decision check: vendors in EU/EEA + countries on the European Commission adequacy list (UK, Switzerland, Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Uruguay) require no extra mechanism. All others require SCCs, BCRs, or a derogation under Loi 1.565.
- [ ] Transfer impact assessment (TIA) on file for any vendor based in the US, including subprocessors. Post-Schrems II analysis applies; Data Privacy Framework certification noted.
- [ ] Onward-transfer clauses verified in vendor contracts (the vendor's vendor must also offer adequate protection).

F. APDP filing posture 4 items

- [ ] Sensitive-data processing (biometric, genetic, health, financial, ethnic, religious, political, sexual orientation) has been declared to the APDP where required.
- [ ] Automated decision-making with significant effects (credit scoring, fraud detection, dynamic pricing) is documented and, where required, declared.
- [ ] DPIA (Data Protection Impact Assessment) on file for high-risk processing — including large-scale UHNW profiling, behavioural advertising, and AI-mediated personalisation.
- [ ] Designated APDP point-of-contact (often the DPO) is named in the privacy notice and reachable.

G. Sector-specific 3 items

- [ ] **Financial services** — MiFID II marketing communication rules apply on top of Loi 1.565: pre-trade transparency, risk warnings, balanced disclosure. Loi 1.338 (Monaco banking) overlay applies to private-bank communications.
- [ ] **Medical / aesthetic** — sector advertising restrictions apply (Code de la santé publique). Before-and-after photography requires specific consent. Testimonials by patients are tightly regulated.
- [ ] **Real estate (Carré d'Or + premium segments)** — listing data and viewing-request data are personal data under Loi 1.565. Photography of residents or staff requires consent. Open-house attendee lists are processed under explicit notice.

H. Incident response 4 items

- [ ] Breach notification procedure: APDP within 72 hours of discovery of a personal-data breach, not "promptly".
- [ ] Internal incident-response runbook names the DPO, legal, communications, technical, and APDP-liaison roles with on-call rotation.
- [ ] Data-subject notification template (in FR) prepared and pre-approved for high-risk breach scenarios.
- [ ] Tabletop exercise run at least annually with a simulated marketing-database compromise.

Glossary

APDP

Autorité de Protection des Données Personnelles, Monaco's data-protection regulator. Equivalent role to CNIL in France or the ICO in the UK.

Loi 1.565

Law of 3 December 2024 on data protection, in force from 2025. Modernises the 1993 framework (Loi 1.165) and aligns Monaco's regime with GDPR-equivalent standards while preserving Monégasque specificities.

DPIA

Data Protection Impact Assessment, a written analysis of risks for high-risk processing.

LIA

Legitimate-Interest Assessment, balancing the controller's legitimate interest against the data subject's rights and freedoms.

SCC

Standard Contractual Clauses, an EU Commission-approved template for cross-border data transfers.

Primary references

1. Loi 1.565 of 3 December 2024 on data protection — Journal de Monaco.
2. Loi 1.165 of 23 December 1993 (as amended) — predecessor framework, partially superseded by Loi 1.565.
3. Regulation (EU) 2016/679 (GDPR) — Official Journal of the European Union, 4 May 2016.
4. APDP — Autorité de Protection des Données Personnelles (Monaco). Rulings and guidance published on apdp.mc.
5. European Commission adequacy decision on Monaco (2000/518/EC) — recognising adequate level of personal-data protection.
6. Council of Europe Convention 108+ (modernised) — Monaco is a signatory.

This checklist is editorial guidance from a Monaco marketing practitioner. It is not a legal opinion. For binding legal certification, consult a Monaco-licensed attorney.