Comparing Algeria's Personal Data Transfer Rules with general data protection regulation

مقارنة قواعد نقل البيانات الشخصية في الجزائر مع التنظيم العام الأوروبي لحماية المعطيات

بوتمجت جلال
طالب دكتوراه
جامعة الجزائر1
jboutemedjet@yahoo.fr

عليوش قربوع كمال
أستاذ التعليم العالي
جامعة باجي مختارعنابة

Date of send:02/11 /2025	*date of acceptance:* 21/12/2025	*date of publication*: 29/12/2025

Abstract:

This article evaluates how Algeria's dual framework for international transfers of personal data the general regime established by Law 18-07 and the special regime introduced by Law 25-11 compares with the transfer architecture of the European Union's General Data Protection Regulation and with widely accepted international standards. The study uses a doctrinal and comparative method and proposes an efficacy rubric that scores legal adequacy, enforceability, procedural pathways, technical alignment, cross-border governance, online-specific safeguards, and institutional capacity. The analysis maps the adequacy-led approach and the enumerated derogations in Law 18-07 alongside the new regime for transfers by competent authorities under Law 25-11, which adds prior-consent control over onward transfers. Findings indicate meaningful convergence and legislative maturation, while showing that effectiveness depends on clear authorization criteria and timelines from the National Data Protection Authority, standardized contractual clauses and transfer impact templates, and operational procedures for competent authorities, including narrowly framed emergency use. The article concludes with policy and practice recommendations to strengthen predictability and interoperability, support trusted cross-border data flows, provide practical guidance, and safeguard national sovereignty together with the rights of individuals.

Keywords: cross-border data transfers; adequacy; SCCs; derogations; onward transfers; competent authorities; NAPPD; GDPR; Convention 108+.

ملخص

يقوم هذا المقال بتقييم الإطار المزدوج في الجزائر المتعلق بالنقل الدولي للبيانات ذات الطابع الشخصي، حيث يجمع بين النظام العام الذي أقرّه القانون 18-07، والنظام الخاص الذي أدخله القانون 25-11، بالمقارنة مع نظام النقل المعتمد في اللائحة العامة لحماية البيانات بالاتحاد الأوروبي (GDPR) ومعايير الحماية المعترف بها دولياً. وتعتمد الدراسة على منهج تحليلي ومقارن، وتقترح أساساً لقياس الفعالية يتضمن: الملاءمة القانونية، إمكانية التنفيذ، المسارات الإجرائية، التوافق التقني، الحوكمة عبر الحدود، الضمانات الخاصة بالأنشطة الإلكترونية، والقدرة المؤسساتية.

ويعرض التحليل مقاربة قائمة على مبدأ "الملاءمة" والاستثناءات الواردة عليه في القانون 18-07، إلى جانب النظام الجديد الذي جاء به القانون 25-11 والمتعلق بالنقل من قبل السلطات المختصة، والذي أضاف شرط الحصول على موافقة مسبقة للتحكم في عمليات النقل اللاحقة. وتشير النتائج إلى وجود تقارب ذي دلالة ونضج تشريعيين، مع إظهار أن الفعالية تعتمد على وجود معايير واضحة للترخيص والآجال الزمنية من قبل السلطة الوطنية لحماية البيانات، فضلاً عن العقود النموذجية الموحدة وقوالب تقييم أثر النقل، والتدابير العملية الخاصة بالسلطات المختصة بما في ذلك الاستخدام الاستثنائي المقيّد لحالات الطوارئ.

ويخلص المقال إلى توصيات قانونية وعملية تهدف إلى تعزيز القدرة على التنبؤ وقابلية التطبيق البيني، ودعم التدفقات الموثوقة للبيانات عبر الحدود، وتوفير إرشادات عملية، وضمان السيادة الوطنية جنباً إلى جنب مع حماية حقوق الأفراد.

Introduction

The digital age has fundamentally transformed how personal data is collected, processed, and transferred across borders. For the purposes of this study, an "international transfer" is any making available of personal data from Algerian territory to a recipient established abroad, including remote access from outside Algeria, and any subsequent onward transfer. "Personal data" is understood as any information relating to an identified or identifiable natural person, adopting a technology-neutral lens that captures contemporary practices such as cloud outsourcing, platform ecosystems, and cross-border cooperation among public authorities.

The central problem is how a domestic legal order can enable trusted cross-border data flows that support trade, innovation, and public-interest cooperation while safeguarding national sovereignty and the fundamental rights of individuals. Algeria approaches this by a dual framework: the general regime of Law 18-07[1], which conditions transfers on an adequate

level of protection and provides narrowly framed derogations, and the special regime introduced by Law 25-11[2] for transfers conducted by competent authorities for penal and security purposes, including a default bar on onward transfers without prior consent of the originating authority. The European model combines adequacy decisions, appropriate safeguards (including standardized contractual tools), and exceptional derogations, complemented by practice on transfer impact assessments. Grounded in statutory texts and operational needs, the inquiry asks how Algeria's dual system can deliver predictable and trusted cross-border flows without weakening protection for individuals or legitimate interests of the State?

The article adopts a doctrinal comparative method. It performs a close reading of the relevant provisions in Law 18-07 (notably articles 44–45) and Law 25-11 (notably articles 45 bis 13–14), and sets them against the structure and logic of GDPR[3] transfer rules (articles 44–49).

The essential elements of the article are fourfold. First, it defines the key concepts including "adequate level of protection," "derogations based on necessity or consent," and "onward transfer." Second, it maps the Algerian general regime, explaining the role of the National Data Protection Authority in assessing destinations and authorizing transfers, and sets out the sovereignty safeguard that allows refusal where vital interests are at stake. Third, it analyzes the new special regime for competent authorities, its purpose-bound assessments, its emergency derogations, and its prior-consent rule for onward sharing. Fourth, it conducts a side-by-side comparison with the European model, drawing out convergences, divergences, and opportunities for interoperability through implementing guidance, model clauses, and standardized assessment tools.

1. Concepts and analytical lens in law

This section fixes the vocabulary and analytical lens used throughout the article. It distinguishes privacy from data protection, clarifies who is a controller and a processor, explains what counts as an international transfer in practice, and sketches the transfer toolbox (adequacy → safeguards → derogations). It also separates general processing from law-enforcement

processing, which is essential when comparing Algeria's Law 18-07 and Law 25-11 with the GDPR and Council of Europe standards.

1.1 Privacy vs. Data Protection

Privacy is a broad fundamental interest in being let alone[4], controlling exposure, and preserving private life. In legal systems influenced by international human-rights law, privacy is protected against arbitrary or unlawful interference and balanced against legitimate aims (public security, public order, rights of others).

Data protection is a distinct, more operational framework governing the processing of personal data—regardless of whether private life is visibly at stake—through principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, accountability) and enforceable rights (access, rectification, erasure, portability, objection, restriction, human review of automated decisions). The GDPR crystallises this distinction: privacy is a fundamental right in the Charter; data protection is implemented through detailed rules and institutions (supervisory authorities, remedies). Convention 108+[5] and Law 18-07 adopt a similar logic by pairing high-level principles with institutional oversight.

1.2 Who is a Controller? Who is a Processor?

A controller determines the purposes and means of processing. A processor acts on behalf of the controller and processes data only on documented instructions[6]. There may be joint controllers when two entities jointly determine purposes and means, and there may be sub-processors engaged by a processor.

Key consequences in both European union and Algerian practice:

- Controllers bear primary responsibility for lawfulness, transparency, and rights-handling; they must have a valid legal basis and respect purpose limitation and minimisation.

- Controller↔processor relationships require written contracts specifying subject matter, duration, nature/purpose, types of data, categories of data subjects, and technical or organisational measures (TOMs).
- Processors must implement security, keep records, assist the controller with rights requests and DPIAs, and refrain from re-use of data for their own purposes without a separate lawful basis7.

1.3 International Transfer in Practice

For comparative purposes we adopt a technology-neutral definition:" an international transfer occurs whenever personal data are made available from one legal order to a recipient in another "[8], including:

- Remote access from abroad to systems/databases hosted domestically (e.g., support, administration, incident response).
- Hosting or processing on foreign infrastructure (production, backups, mirrors, disaster-recovery).
- Disclosure to a foreign recipient that processes for its own or the exporter's purposes.
- Onward transfers by the initial foreign recipient to a third country or international organisation.

By contrast, mere transit routing of encrypted packets via foreign networks without access is generally not treated as a transfer. Truly anonymised data fall outside personal-data rules; pseudonymised data do not. This practical definition aligns with GDPR guidance on Chapter V and with modernised Convention 108+ principles, and it maps to Algeria's split between Law 18-07 (general regime) and Law 25-11 (competent-authority regime).

1.4 Transfer Tools & Safeguards

The transfer toolbox follows a three-step decision tree:

- Adequacy (primary route)
- Under the GDPR, the European Commission may adopt adequacy decisions for destinations ensuring protection essentially equivalent to the

EU (Article 45)[9]. Under Law 18-07, adequacy is assessed by the NAPPD[10] for the specific

- transfer and destination[11].

- Appropriate safeguards when there is no adequacy decision
  - GDPR tools include Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and where available codes or certifications with binding commitments (Article 46)[12].
  - After Schrems II, exporters must perform Transfer Impact Assessments (TIAs) and add supplementary measures where foreign law/practice may undermine protections (client-side encryption, robust pseudonymisation, split processing, challenge/notice clauses, audit rights).
  - In Algeria's general regime, similar protections can be achieved through NAPPD templates and model clauses that impose equivalent contractual and technical obligations on recipients, including sub-processor control and onward-transfer limits.

Derogations (exceptional gates) when adequacy and safeguards are not feasible in time.

Both frameworks recognise explicit consent, contract necessity at the data subject's request, important public interest, legal claims, and vital interests (GDPR Art. 49; Law 18-07 Art. 45).

These are narrow, case-specific and unsuitable for repetitive or structural transfers.

1.5 General Processing and law enforcement processing

The GDPR's transfer rules (Articles 44–49) govern general processing by public and private actors, but processing by competent authorities for Ocriminal-law purposes is addressed by the Law Enforcement Directive (LED) 2016/680.

Algeria mirrors this separation:

- Law 18-07 covers general processing and international transfers via adequacy and derogations;

- Law 25-11 creates a special regime for competent authorities with purpose-bound assessments (prevention, investigation, prosecution, execution of penalties) and a statutory bar on onward transfers without the originating authority's prior consent, plus a narrow emergency exception.

2. Algeria's General Regime Law 18-07 (articles. 44–45)

This regime governs international transfers of personal data through the rule of adequacy (Article 44) and limited derogations (Article 45). The NAPPD authorises transfers based on adequate protection, supported by documentation, and may block them if they endanger public security or vital interests[13].

2.1 Adequate Level of Protection (art. 44)

2.1.1 Concept of "adequacy" under Law 18-07

Adequacy requires protection equivalent in outcome, not identical in wording: enforceable rights, supervision, and remedies. Assessment is both systemic (legal framework) and contextual (risks of the specific transfer). [14].

2.1.2 Indicative criteria for NAPPD assessment

The NAPPD considers the existence of data-protection law, effective rights, supervisory authority independence, enforcement practice, technical safeguards like encryption and logging, and rules on government access. Controllers submit a dossier combining legal analysis and transfer-specific risk assessment [15] [16].

2.1.3 Evidence and documentation: building an "adequacy pack"

The adequacy pack typically includes mapping of destination law, recipient assurances on purpose and security, audit clauses, encryption measures, and a statement on residual risks. Alignment with NAPPD model clauses improves efficiency.

2.1.4 Managing change: monitoring, renewal, and withdrawal

Adequacy is dynamic: controllers should review changes regularly, renew or withdraw approvals as needed, and respond to incidents. The NAPPD may set review periods, suspend authorisations, or issue advisories where protections decline.

2.1.5 The sovereignty clause: absolute restrictions and governance

Article 44 contains a sovereignty safeguard: a transfer must not proceed if it would undermine public security or the State's vital interests, even where ordinary adequacy could be met. To keep this a targeted safeguard, governance should define triggers (e.g., critical-infrastructure telemetry, defence-related datasets, high-granularity geolocation of officials), apply a proportionality test (can scope-limitation or anonymisation neutralise risk?), require internal multi-disciplinary review and reasoned decisions, and maintain robust traceability. Where residual risk remains incompatible, prefer on-premises or synthetic/aggregated alternatives[17].

2.1.6 Illustrations (practice-oriented)

Cloud analytics may qualify with encryption and minimisation, while transfers of security-sensitive data to countries with weak oversight may be refused. In emergencies, such as urgent medical cases, a one-off derogation may apply.

2.1.7 Relationship with Article 45 (derogations) and onward-transfer control

Derogations cover consent, vital interests, contracts, public interest, or legal claims, but remain exceptional and unsuitable for recurring flows. Recipients must be barred from onward transfers unless equivalent safeguards or prior approval exist.

3. Algeria's Special Regime — Law 25-11 (arts. 45 bis 13–14)

While Law 18-07 establishes the general rule for international transfers through an adequacy-first approach, Law 25-11 creates a special regime tailored to transfers made by or between "competent authorities" for penal and security purposes. This regime recognises that law-enforcement contexts raise distinct necessities (speed, integrity of evidence, operational secrecy) and therefore requires purpose-bound assessments, targeted derogations, and tight control of onward transfers. Articles 45 bis 13 (competent authorities and assessment) and 45 bis 14 (onward-transfer control) are the keystones of that design[18].

3.1 Competent Authorities & Purposes (art. 45 bis 13)

3.1.1 Scope: actors and purposes

Article 45 bis 13 defines the institutional scope and objectives of the special regime. In substance, competent authorities include, at minimum, judicial authorities, law-enforcement and security services, and the penitentiary administration acting within their lawful remits. The exclusive purposes for which international transfers may occur under this regime are those classically associated with criminal justice: prevention, investigation, detection, prosecution, and execution of penalties. The "purpose-bound" structure functions as an internal limiter: even when an authority is within scope institutionally, the transfer must be necessary for a listed penal purpose and not for general administrative convenience.

Borderlines.

- If a ministry or public agency transfers personal data for administrative or service-delivery objectives unrelated to criminal justice, the general regime (Law 18-07) should govern.
- If the same agency undertakes a dual-purpose processing (for example, a social-service dataset that also informs a specific criminal investigation), the dominant, documented purpose and the legal basis should determine the applicable regime.

3.1.2 Specific assessment: relevance, proportionality, rights lens, destination oversight, and safeguards

Transfers under 45 bis 13 require a specific, documented assessment—stricter than ordinary proportionality tests because cross-border effects are harder to unwind. A robust assessment typically covers five blocks:

A. Relevance and necessity.

Describe the precise penal purpose and the strict necessity of the transfer for that purpose.

Justify the data selection (fields, categories, time span) and exclude non-essential attributes.

Consider less intrusive alternatives (on-site access, pseudonymised extracts, filtered reports) and explain why they are insufficient.

B. Proportionality and human-rights lens.

Assess foreseeable impacts on privacy, freedom of expression/association, non-discrimination, and due-process rights.

Identify vulnerable groups (minors, protected witnesses) and apply heightened safeguards.

Record the retention period and conditions for purging or sealing data post-use.

C. Supervisory landscape at destination.

Note the existence, powers, and independence of a supervisory authority at the destination (or equivalent oversight for criminal-justice processing).

Describe complaint and redress avenues available to affected persons and any judicial controls on law-enforcement data use.

D. Operational safeguards at the recipient.

Technical security (encryption at rest and in transit, exporter-controlled or escrowed keys where feasible, strict access controls, tamper-evident logs, secure environments segregated from intelligence databases not relevant to the purpose).

Organisational controls (named roles, need-to-know access, dual-control for export/import, chain-of-custody records).

Use limitation commitments (no re-purposing outside the specified penal objective without renewed assessment and authorisation).

E. Documentation and authorisation trail.

A signed transfer decision citing the legal basis, purpose, data scope, safeguards, and the destination authority;

Evidence of internal review (legal and operational), and where applicable, consultation with oversight bodies;

A notification/record in an internal register of cross-border penal transfers for auditability[19].

This structure mirrors comparative standards in Europe's law-enforcement data-protection directive and the Council of Europe's Convention 108+ context, adapted to Algeria's statutory vocabulary.

3.1.3 Targeted derogations under 45 bis 13

Recognising operational urgency, Article 45 bis 13 frames narrow derogations:

Vital interests of a natural person. Immediate risks to life or physical integrity can justify a one-off transfer with expedited procedures; documentation follows as soon as practicable.

Serious and immediate threat to public security. When delay would materially increase risk (for example, imminent mass-casualty threats), authorities may proceed under emergency provisions, subject to a strict necessity narrative and ex post review.

Rights of the defense. Transfers necessary to ensure fair-trial rights especially reciprocal sharing relevant to exculpatory evidence may proceed with balanced safeguards protecting third-party data.

Guardrails. Even in emergencies, the authority should (i) minimise the dataset, (ii) use secure channels with auditable logging, (iii) set short retention pending confirmation, and (iv) conduct an after-action review.

3.2 Onward-Transfer Controls (art. 45 bis 14)

3.2.1 Default rule: prior consent of the originating authority

Article 45 bis 14 introduces a categorical control on onward transfers: data received from a foreign authority may not be retransferred to any third country or international organisation without the originating authority's prior consent. In practice, it requires the recipient to embed procedural gates so that any contemplated onward sharing is paused until a renewed necessity/proportionality check is recorded and explicit consent is obtained from the origin[20].

Implications for cooperation.

Contractual or operational alignment: memoranda of understanding or cooperation protocols should encode the no-onward-transfer rule, define the

contact point, the time to decide, and the format of consent (signed form, secure channel).

System design: recipients should configure systems to technically enforce "no forward" constraints (for example, role-based restrictions, data-loss-prevention rules on export, immutable logs and alerts on attempted exfiltration).

Evidence handling: chain-of-custody artefacts should record onward-transfer checks and consent IDs to preserve evidentiary integrity.

3.2.2 Emergency exception and ex-post duties

Article 45 bis 14 recognises a single, narrow exception: where a serious and immediate threat to public security requires urgent onward sharing. Even then, the recipient must (i) ensure strict minimisation, (ii) use secure channels, (iii) document the decision with reasons and scope, and (iv) notify ex post the originating authority without undue delay.

Good practice for emergencies.

Maintain a pre-approved emergency playbook specifying roles, thresholds for activation, secure communications, and immediate logging requirements.

After action, run a formal review to assess proportionality, improve thresholds, and, where appropriate, inform oversight bodies.

3.2.3 Alignment with international cooperation standards

The prior-consent model and the narrow emergency escape align with contemporary cooperation norms found in European instruments and Council of Europe practice: they privilege purpose limitation, mutual trust, and traceability, while leaving space for urgent operational needs. This approach also resonates with the European Union's separation between the general GDPR toolbox and law-enforcement-specific rules under Directive (EU) 2016/680, which stresses purpose-bound sharing, oversight, and record-keeping[21].

3.2.4 Traceability and auditability requirements

To make Article 45 bis 14 effective, authorities should implement:

- Comprehensive logging: immutable, time-stamped logs of receipt, access, analysis steps, any disclosure events, and onward-transfer checks.
- Register of penal transfers: a central register holding purpose statements, legal bases, data scopes, safeguards, retention, and any ex-post notifications.
- Periodic audits: internal and, where indicated, external audits to test compliance with the no-onward-transfer rule and the emergency protocol.
- Data-subject interfaces (where compatible with secrecy constraints): mechanisms to access or contestation rights after proceedings conclude, with redactions as required by law.

4. GDPR Transfer Regime (articles 44 - 49)

The GDPR structures international personal-data transfers around three concentric layers: (i) adequacy decisions adopted by the European Commission; (ii) appropriate safeguards that controllers and processors can implement when no adequacy exists; and (iii) narrowly framed derogations for exceptional, case-specific situations. This section distils the core mechanics relevant to comparing Algeria's framework with the GDPR[22].

4.1 Adequacy decisions: scope, periodic review, essential equivalence

Under article 45, the Commission may find that a third country (or a sector/organisation within it) ensures a level of protection essentially equivalent to that guaranteed in the Union. "Essential equivalence" focuses on outcomes rather than textual identity: enforceable rights, effective oversight by an independent authority, rules on purpose limitation, security and redress, and proportional access by public bodies.

Scope: Adequacy can be country-wide, sector-specific, or organisation-specific (e.g., frameworks certified against Commission decisions).

Review and suspension: Decisions are subject to periodic review and may be adapted, suspended, or repealed if circumstances change. Controllers retain a due-diligence duty: if facts indicate erosion of protection, they must reassess and, where needed, switch to safeguards or suspend transfers.

Practical upshot: Adequacy is the lowest-friction route: once a transfer falls within its scope, no additional authorisation is needed, though accountability (records, transparency, minimisation) still applies.

4.2. Appropriate safeguards: SCCs, BCRs, codes/certifications and post-Schrems II

Obligations

When no adequacy decision applies, article 46 permits transfers if the exporter implements appropriate safeguards ensuring data-subject rights and effective remedies.

Standard Contractual Clauses (SCCs).

The Commission's 2021 modular SCCs cover controller↔controller, controller→processor, and processor→processor scenarios, with docking clauses, onward-transfer restrictions, third-party-beneficiary rights, audit and termination levers. Exporters must complete the annexes (data description, technical/organisational measures, sub-processors) and ensure practical enforceability.

Binding Corporate Rules (BCRs).

Group-internal codes approved by a lead supervisory authority via the GDPR's cooperation mechanism. BCRs embed rights, complaint handling, audit, and liability allocation across multinational groups. They suit steady, intra-group flows but require significant governance and maintenance.

Codes of conduct and certifications (articles. 40–42).

Sector codes and certification schemes may serve as safeguards if coupled with binding and enforceable commitments by the overseas recipient. Adoption remains uneven; where available, they can standardise expectations and audits.

After Schrems II: Transfer Impact Assessments (TIAs) and "supplementary measures".

The Court of Justice clarified that exporters using SCCs (or similar tools) must verify, case by case, that the third-country legal and practical

environment allows the clauses to work in practice. The EDPB recommends a TIA workflow:

A- Map transfers and identify the tool in use;

B- Assess destination law and practices, especially public-authority access and redress;

C- Select and implement supplementary measures where needed;

D- Adopt procedural safeguards (policies, audit, transparency);

E- Re-evaluate periodically.

Supplementary measures may be:

Technical (end-to-end or client-side encryption with keys under exporter control; robust pseudonymisation; split or proxy processing; trusted execution with remote attestation).

Contractual (obligations to challenge unlawful requests, narrow data-disclosure logs, notification clauses, "no back-doors" warranties, enhanced audit and suspension rights).

Organisational (access governance, incident playbooks for government requests, staff training, internal approvals for exports).

Where no combination of measures can achieve essential equivalence, the transfer should not proceed[23].

4.3 Derogations (art. 49): strict necessity and exceptional use

The article 49 provides exceptional gates when neither adequacy nor safeguards are feasible in time. These include: explicit consent (informed and specific to the transfer, with risk disclosure), contract necessity at the data subject's request, important public interest recognised in EU or Member-State law, legal claims, vital interests, and public registers. Regulators stress that derogations are not for repetitive or structural transfers. Use requires a necessity/proportionality analysis, strict data minimisation, secure channels, and documentation. Exporters should promptly migrate recurring flows to article 46 safeguards[24].

4.4 Enforcement and guidance: EDPB role, DPA cooperation, recent trends

Supervision. National Data Protection Authorities (DPAs) oversee compliance, cooperate via the GDPR's consistency mechanism, and may issue or participate in joint operations. The EDPB publishes recommendations (notably on supplementary measures) and guidance on international transfers and "what counts as a transfer"[25].

Trends impacting transfers.

Adtech and cookies. Enforcement against unlawful tracking and dark-patterns raises the bar for "consent" and for downstream sharing with non-EEA partners. Exporters must verify lawful collection before exporting, then ensure appropriate transfer tools.

Cloud and remote support. Remote access from outside the EEA is a transfer; processors must implement strict access segregation, exporter-held keys where feasible, granular logging, and robust sub-processor control.

Vendor chains. DPAs expect full chain transparency: onward transfers by processors require equivalent tools and measures, with documented TIAs for each leg.

4.5 Law-enforcement parallel: Directive (EU) 2016/680 (LED)

The GDPR's articles 44–49 do not govern processing by competent authorities for criminal-law purposes. That domain is covered by the Law Enforcement Directive (LED), which accents purpose limitation, oversight, record-keeping, and onward-sharing controls in cooperation settings. Conceptually, the LED's approach (purpose-bound sharing, audit trails, and limits on onward transfer) parallels Algeria's Law 25-11 (arts. 45 bis 13–14), which requires a documented assessment and prior consent for onward transfers with a narrow emergency exception.

5. Structured Comparative Analysis

This section compares Algeria's two-tier system general regime (Law 18-07) and special regime for competent authorities (Law 25-11) with the GDPR transfer architecture. We focus on (i) the institutional locus and

authorisation model, (ii) assessment criteria and safeguards, (iii) law-enforcement transfers, and (iv) convergence, divergence, and interoperability pathways. A compact scoring matrix (planned Table 3) closes the section to visualise relative strengths using the article's efficacy rubric.

5.1 Institutional Locus & Authorization

Algeria (NAPPD-centred model)

Under Law 18-07, article 44 places the NAPPD at the heart of international transfer governance. Adequacy is the default gate, reached through an NAPPD assessment of the destination's legal-institutional environment and the specifics of the transfer. Where adequacy is unavailable, article 45 offers narrow derogations (consent or necessity) for exceptional use. Law 25-11, for its part, creates a parallel locus for transfers by competent authorities (article 45 bis 13): the authority itself performs a purpose-bound assessment, while article 45 bis 14 locks onward transfers behind prior consent from the originating authority. In both tracks, predictability depends on secondary instruments (guidance, templates, model clauses, timelines) to standardise submissions and decisions[26].

European Union (decentralised controller model under Commission umbrella).

The GDPR couples a central mechanismc commission adequacy decision (article 45) with a decentralised regime, where controllers and processors can transfer on the basis of appropriate safeguards, they implement themselves (article 46), notably Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), subject to Transfer Impact Assessments and, where needed, supplementary measures after Schrems II. Member-State DPAs supervise ex post and cooperate via the EDPB, while the Commission periodically reviews adequacy.

Transparency, timelines, guidance.

GDPR practice is dense: adequacy decisions are public; SCCs are standardised; EDPB issues detailed guidance and FAQs; DPAs publish

expectations and case trends (e.g., remote support = transfer; cloud chains require leg-by-leg TIAs).

Algeria's path to similar predictability lies in publishing NAPPD checklists, model clauses, review timelines, and non-confidential summaries of decisions (positive and negative). For the special regime, short SOPs and forms for competent-authority transfers would align implementation across ministries.

Takeaway.

GDPR emphasises controller self-reliance within an EU-set toolbox; Algeria emphasises ex ante public-authority assessment (NAPPD or competent authority). Both models can yield certainty if transparent and standardised.

5.2 Assessment Criteria & Safeguards

Legal criteria.

All three frameworks (Algeria general, Algeria special, GDPR) converge on core benchmarks: existence of a data-protection law, enforceable rights, an independent supervisory authority, and effective remedies. Algeria's general regime also contains a sovereignty safeguard (public security/vital interests) that can override adequacy.

Organisational and technical measures.

GDPR (arts. 5, 24–32, 44–49) expects risk-based technical and organisational measures and, post-Schrems II, supplementary measures when third-country law threatens clause effectiveness (e.g., client-side encryption, robust pseudonymisation, access governance, logging, onward-transfer controls).

Algeria (general) can embed the same suite through NAPPD checklists and model contractual clauses: encryption with exporter-controlled keys where feasible, sub-processor approval and mapping, retention and deletion rules, audit rights, government-request handling policies, and a "no onward transfer without equivalent safeguards or prior authorisation" covenant.

Algeria (special) superadds chain-of-custody and use-limitation controls tied to the penal purpose, and requires prior consent for onward sharing (see 5.3).

Documentation standards & risk-based approach.

GDPR operationalises risk via TIAs (EDPB Rec. 01/2020) and context-specific annexes to SCCs (data categories, processing operations, TOMs).

Algeria (general) can mirror this with an "adequacy pack": destination legal profile, transfer risk analysis, security annex, sub-processor map, government-access posture, and residual-risk statement cross-referenced to article 44.

Algeria (special) needs a purpose-bound assessment: necessity/proportionality narrative, rights lens (minors, witnesses), destination oversight, channel security, minimisation, retention, and ex post review for any emergency use.

Onward-transfer limitations.

GDPR SCCs restrict onward transfers absent equivalent safeguards; Algeria (general) should do the same contractually; Algeria (special) imposes a statutory prior-consent rule (article 45 bis 14).

5.3 Law-Enforcement Transfers

Algeria's special regime.(11-25)

Article 45 bis 13 defines competent authorities and penal purposes; it requires a documented transfer assessment with a human-rights lens. Article 45 bis 14 creates a default ban on onward transfers without the originating authority's prior consent, plus a narrow emergency exception for serious and immediate public-security threats with ex post notice.

EU parallel (LED logic).

The Law Enforcement Directive (Directive 2016/680) governs criminal-law processing by competent authorities, stressing purpose limitation, oversight, record-keeping, and controlled onward sharing in international cooperation. The LED does not carbon-copy GDPR tools but

pursues the same trust-and-traceability logic: documented necessity, limited data, logs, and cooperation channels subject to law and supervision.

Emergency derogations and proportionality controls.

Both systems recognise urgent scenarios. Under Algeria's 25-11, emergency use is exceptional, minimised, and audited after the fact; under EU practice, emergency channels must still respect necessity, proportionality, and record-keeping.

Comparative note.

Algeria's prior-consent rule for onward transfer creates a clear ex ante gate that is sometimes only contractual in non-penal GDPR contexts. In the penal context, the LED's emphasis on record-keeping and oversight is conceptually aligned; Algeria hard-codes the consent requirement, which may strengthen mutual trust while requiring responsive consent workflows to avoid operational friction.

5.4 Convergence, Divergence, and Interoperability

Convergences (clean mapping to GDPR logic).

Adequacy-first design (Algeria art. 44 ↔ GDPR art. 45).

Narrow derogations as safety valves (Algeria art. 45 ↔ GDPR art. 49).

Risk-based safeguards rooted in organisational and technical controls; onward-transfer limitations in the general regime through contracts and in the special regime by statute.

Divergences (where secondary instruments are needed).

Tooling and templates. GDPR offers standardised SCCs and established TIA methods. Algeria would benefit from model clauses aligned to Law 18-07 and checklists that approximate TIA logic for exports under authorisation.

Public transparency of decisions. The EU publishes adequacy decisions and EDPB guidance. Algeria can enhance certainty with non-confidential decision abstracts, review timelines, and a living FAQ on typical scenarios (remote support, cloud replication, research).

Sovereignty clause operation. Algeria's explicit public-security/vital-interests stop-rule is distinctive; clear triggers, proportionality tests, and recorded reasoning will preserve targeting and resist over-breadth.

Interoperability pathways.

Convention 108+ offers a shared vocabulary for adequacy criteria (rights, oversight, redress) and can anchor bilateral or regional cooperation.

Bridging artefacts. Algeria can publish SCC-like model clauses (purpose limitation; security; sub-processor control; audits; government-request handling; onward-transfer bar) and a transfer-risk checklist that echoes EU TIA steps without importing EU law.

Competent-authority cooperation. For Law 25-11, memoranda of understanding can encode prior-consent mechanics, emergency thresholds, secure channels, and chain-of-custody requirements compatible with LED practice.

6. Practical Challenges & Case-Style Illustrations

This section turns doctrine into practice. It highlights recurring operational challenges that organisations and public bodies face when exporting personal data and then presents case-style illustrations showing how Algeria's general regime (Law 18-07), the special regime (Law 25-11), and the GDPR toolbox are applied in real decisions.

6.1. Recurring Practical Challenges

Mapping cross-border flows and vendor chains

Controllers often under-document remote access by overseas support teams, which is itself a transfer under both frameworks. Failure to map sub-processors of sub-processors leads to uncontrolled onward transfers that breach article 44 (Algeria) or articles 46–49 (GDPR).

Choosing the right legal path

Routine exports must not rely on derogations (consent/necessity) designed for exceptional use (18-07 art. 45; GDPR art. 49). The durable path is adequacy or appropriate safeguards with documented risk controls.

Documentation standards

The adequacy pack (Algeria) or Transfer Impact Assessment (GDPR) is frequently incomplete: missing destination-law analysis, vague security annexes, no onward-transfer covenant, or no government-access posture.

Encryption and key management.

"Encryption" in name only is common. Where third-country law poses access risks, exporter-controlled keys, strong pseudonymisation, and split processing may be needed; otherwise, the transfer should not proceed.

Timelines and transparency

Business teams need predictable authorisation timelines (Algeria/NAPPD) or clear internal approvals (GDPR). Absent templates and checklists, reviews stall and risk drift into unlawful exports.

Sovereignty safeguard triggers (Algeria)

Data about critical infrastructure, defence, or high-granularity geolocation of public officials may trigger article 44's public-security/vital-interests stop-rule even where other criteria point to adequacy.

Law-enforcement edge cases.

Mixed-purpose datasets (administrative + penal) pose regime-selection issues. The dominant, documented purpose and legal basis should drive whether the general or special regime applies, with coordination between the NAPPD and the competent authority.

6.2. Case-Style Illustrations

Case 1 Cloud CRM Migration to a Non-Adequate Destination

Facts. An Algerian retailer plans to host its customer-relationship platform in a data centre located in a third country with modern but not EU-recognised privacy law. Multiple analytics plug-ins are involved.

Issue. What legal path enables the transfer, and what safeguards are required?

Applicable law. Algeria: art. 44 (adequacy), art. 45 (derogations). GDPR: arts. 46–49 (SCCs/BCRs); Schrems II; EDPB Rec. 01/2020.

Analysis

Not a candidate for derogations: the flow is structural.

Algeria: prepare an adequacy pack to seek NAPPD authorisation. Include destination-law mapping, security annex, onward-transfer flow-down for every plug-in, and a government-access section.

GDPR comparator: execute 2021 SCCs (controller→processor), run a TIA, and implement supplementary measures (client-side encryption; keys held in Algeria; strict role-based access; immutable logs; vendor chain transparency).

Outcome & artefacts. Approval contingent on: (i) SCC-like clauses under Algerian law; (ii) exporter-keyed encryption; (iii) sub-processor approval gate; (iv) audit rights and incident-notice SLAs; (v) a no-onward-transfer covenant absent equivalent safeguards or prior authorisation.

Case 2 Competent-Authority Emergency Share under Law 25-11

Facts. An Algerian security service receives intelligence indicating an imminent mass-casualty threat abroad. The partner authority in State X requests identifiers and travel data within hours.

Issue. Can data be transferred immediately, and may State X onward-transfer to a second partner without consent?

Applicable law. Law 25-11 art. 45 bis 13–14 (penal purposes, prior consent for onward transfers, emergency exception with ex post notification). LED 2016/680 as conceptual analogue.

Analysis

The situation meets the serious and immediate public-security threshold. Transfer a minimised dataset via secure channels.

Onward transfer by State X is prohibited unless Algeria's originating authority grants prior consent. In this narrow emergency, State X may share immediately only what is strictly necessary, but must notify ex post without undue delay; Algerian origin then validates, conditions, or objects.

Record necessity/proportionality, recipients, time stamps, and measures (chain-of-custody). After action, conduct a review and seal non-necessary data.

Outcome & artefacts. Emergency playbook; ex post notification template; internal oversight note; retention and sealing orders.

Case 3 Research Collaboration: Consent vs Safeguards

Facts. A university hospital in Algiers collaborates with a laboratory in a non-adequate country to study rare diseases. The project anticipates repeated exports of pseudonymised clinical data over two years.

Issue. Is consent sufficient, or should the parties use safeguards?

Applicable law. Algeria art. 45 (consent/necessity derogations are exceptional); GDPR art. 49 (same); article 46 (safeguards).

Analysis

Repeated, planned transfers should not rest on consent derogation alone.

Build an adequacy pack (Algeria) and, in parallel, deploy SCCs (GDPR comparator), paired with supplementary measures: strong pseudonymisation with keys held in Algeria, cell suppression rules, role-based access, and audit.

Provide participant transparency and withdrawal mechanics, but do not treat withdrawal as the sole legal control for international transfers.

Outcome & artefacts. Ethics approval; SCC-like clauses; pseudonymisation protocol; sub-processor map; TIA/adequacy analysis; periodic reviews.

6.3. Practical Checklists (for counsel and DPOs)

Pre-transfer:

- Identify trigger and destination.
- Select path: adequacy or safeguards (SCCs/BCRs).
- Prepare adequacy pack/TIA with key legal, oversight, and technical points.
- Ensure flow-down clauses, sub-processor approval, encryption, logging, and retention.

During transfer:

- Use secure channels, least-privilege, and time-limited access.
- Keep immutable logs and monitor anomalies.

Post-transfer:

- Review destination law and renew approvals.
- Audit sub-processor chain and onward-transfer controls.

For emergencies, document and notify ex post.

6.4. Key Takeaways

Do not normalise derogations. They are bridges, not roads.

Paper is not enough. Without exporter-controlled keys, onward-transfer locks, and auditable logs, contractual promises may fail in practice.

Be ready for sovereignty triggers. Some datasets will not travel, even with strong safeguards; design hybrid/on-prem alternatives early.

For competent authorities, consent-gate onward transfers. Article 45 bis 14 strengthens mutual trust but requires responsive consent workflows to avoid operational delays.

Conclusion

This article has argued that Algeria's two-tier architecture—an adequacy-led general regime under Law 18-07 and a purpose-built special regime for competent authorities under Law 25-11—maps closely to contemporary international models while preserving a distinct sovereignty safeguard. Substantive convergence with the European Union's framework is significant (adequacy logic, narrow derogations, risk-based safeguards). The decisive variable is implementation: whether clear authorisation pathways, standardised safeguards, and auditable controls can translate statutory principles into predictable practice for controllers, processors, and public authorities. The recommendations below are designed to close that implementation gap and to enhance interoperability with GDPR practice and Convention 108+.

A. Regulatory recommendations

1. Publish an adequacy toolkit: issue criteria and checklists for Article 44, a standard adequacy pack, and model contractual clauses (purpose limitation, security, encryption, sub-processor approval, breach notice, audit rights, onward-transfer limits).
2. Operationalise the sovereignty clause: define trigger categories, require proportionality review, and publish non-confidential summaries.

3. Guidance on derogations (Art. 45): clarify they are exceptional, provide examples, and require a short proportionality worksheet.
4. Special regime SOPs (Law 25-11): adopt standard assessment forms, codify onward-transfer consent workflow and emergency playbook, and mandate audits.
5. Transparency and metrics: publish annual statistics and a FAQ on common scenarios.

B. Legislative and policy recommendations

1. Secondary instruments: empower NAPPD to update model clauses and technical baselines; create recognition pathways for codes/certifications.
2. International interoperability: use Convention 108+ as adequacy benchmark and pursue bilateral protocols with GDPR jurisdictions.
3. Procedural guarantees: provide appeal routes, confidential submissions, and clarify post-proceeding rights.

C. Organisational recommendations (controllers and processors)

1. Governance program: maintain a transfer register and apply two-tier reviews (legal + technical).
2. Essential equivalence: prefer exporter-controlled encryption, pseudonymisation, and strong access/logging; contract for audits and request handling.
3. Derogations: restrict to one-off or urgent cases, with migration to safeguards.
4. Capacity and culture: train teams on transfer triggers; designate officers and rehearse emergency procedures.

References

1 Law number 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of Personal Data. Official Journal of 2018, No. 34, pp. 11–23.
https://droit.mjustice.dz/sites/default/files/portail/loi_18-07_ar.pdf

2 Law number 25-11 of 24 July 2025, amending and supplementing Law No. 18-07 of 10 June 2018, relating to the protection of natural persons with regard to the processing of personal data. Official Journal of 2018, No. 48, pp. 14–19. https://droit.mjustice.dz/sites/default/files/loi-25-11-ar.pdf

3 (General Data Protection Regulation). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4 May 2016, pp. 1–88.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

4 The first study on the right to privacy can be found in an article published by the famous Warren & Brandeis. They define it as the right to enjoy life and to be let alone.
Samuel D. Warren et Louis D. Brandeis, « The Right to Privacy », Harvard Law Review, vol. 4, n° 5, 15 décembre 1890, p. 193. https://doi.org/10.2307/1321160

5 Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), adopted 18 May 2018 in Strasbourg.
https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

6 Article 3 of 18-07 Law.

7 European Union Agency for Fundamental Rights (FRA) & Council of Europe. (2018). Handbook on European data protection law. Publications Office of the European Union.
https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

8 Adam A., « L'échange de données à caractère personnel entre l'Union européenne et les États-Unis, Entre souci de protection et volonté de coopération », RTD EUR, n° 42 (3), juillet-septembre, 2006, pp. 411-437.

9 Regulation (EU) 2016/679 (GDPR), OJ L 119, 4 May 2016

10 "The National Authority for the Protection of Personal Data", regulated by Articles 23 and after of 18-07 law.

11 Algeria, Law No. 18-07 of 10 June 2018 on the protection of natural persons in the processing of personal data (esp. Arts. 44–45; institutional rules incl. Arts. 23 et seq.)

12 European Commission, Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for transfers to third countries, OJ L 199, 7 June 2021; Regulation (EU) 2016/679 (GDPR), OJ L 119, 4 May 2016 (Art. 46 on BCRs/codes

13 Forest, David, Données personnelles: RGPD, loi informatique et libertés, Dalloz, 2023, p 119.

14 Mattatia, Fabrice, RGPD et droit des données personnelles, Eyrolles, 2018, p 79.

15 Solove, Daniel J., Understanding Privacy, Harvard University Press, 2008, p 205

16 OECD, "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies," 2019; CNIL, Le RGPD dans la jurisprudence, Rapport 2021, p 67.

17 Nicolas-Vullierme, Laurence, "Protection des données personnelles sur internet," Revue internationale de droit comparé, vol. 71(2), 2019, pp. 389–411.

18 De Hert, Paul & Papakonstantinou, Vagelis, "The New Police and Criminal Justice Data Protection Directive: A First Analysis," Computer Law & Security Review 32(6), 2016), p 347.

19 Boehm, Franziska, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Springer, 2012, p 134.

20 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28 Jan. 1981.

21 Directive (EU) 2016/680 of 27 April 2016 (Law Enforcement Directive), OJ L 119, 4 May 2016.

22 Brunet, Emmanuel, « Règlement général sur la protection des données à caractère personnel – Genèse de la réforme et présentation globale », Dalloz IP/IT, 2016, p. 567

23 European Data Protection Board, Guidelines 05/2021 on what constitutes an international transfer, 2021.

24 European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (WP 262 rev.01), adopted 5 Apr. 2018, revised 25 May 2018.

25 Court of Justice of the European Union, Case C-362/15, Maximillian Schrems v Data Protection Commissioner ("Schrems I"), Judgment of 6 Oct. 2015.

26 De Terwangne, C., "La Convention 108 du Conseil de l'Europe pour la protection des données, 40 ans et après ?", Politeia, n°39, 2021, pp. 157–195.