THE BURDEN IMPOSSED BY DATA PROTECTION LAWS ON SMALL SCALE BUSINESS

An analysis on whether the regulatory burden imposed upon businesses by data protection laws bears a rational and proportionate relationship to the privacy harm that the law seeks to prevent.

The objectives of privacy protection are legitimate, but can the same be said of the proportionality, predictability and economic calibration of enforcement?

1. THE CONSTITUTIONAL BALANCE

Article 31 of the Constitution protects privacy, including the right not to have information relating to a person's family or private affairs unnecessarily required or revealed. The DPA was enacted principally to give practical effect to that constitutional right. The courts have therefore treated data protection as a substantive constitutional interest rather than a mere administrative requirement.

But the Constitution does not establish privacy as the only economic value. Kenya's constitutional order also protects property, economic activity and legitimate business interests. The proper question is consequently not whether businesses should be regulated, but whether the regulatory burden imposed upon them bears a rational and proportionate relationship to the privacy harm that the law seeks to prevent.

That distinction is critical. A regulatory regime can be perfectly legitimate in its objective while nevertheless becoming economically counterproductive through excessive compliance costs, uncertainty, disproportionate sanctions or enforcement that fails to distinguish between a multinational corporation and a micro-enterprise.

2. THE DPA IS SUBSTANTIALLY MORE THAN A PRIVACY STATUTE

The DPA imposes a comprehensive regulatory framework upon controllers and processors. It regulates the collection, storage, disclosure, transfer and other processing of personal data and imposes obligations concerning lawfulness, fairness, transparency, purpose limitation, data minimisation, retention, security and accountability.

CM ADVOCATES LLP

For high-risk processing, section 31 additionally requires a Data Protection Impact Assessment before processing is undertaken. The assessment must consider necessity, proportionality, risks to data subjects and safeguards.

From a large corporation's perspective, these are manageable governance requirements. From the perspective of a five-person business, however, they can become a substantial transaction cost.The question therefore becomes particularly acute where the enterprise is not exploiting data in any commercially abusive manner but is simply using ordinary customer information to conduct business.

3. THE PENALTIES ARE POTENTIALLY SEVERE

Section 63 of the DPA gives the Commissioner power to impose an administrative penalty of up to KShs. 5 million or 1% of annual turnover, whichever is lower. The enforcement architecture also permits enforcement notices requiring corrective action.

The significance of the penalty regime should not be underestimated. For a corporation turning over KShs. 1 billion, a KShs. 5 million maximum penalty represents 0.5% of turnover. For a business turning over KShs. 20 million, the same KShs. 5 million represents 25% of annual turnover. The nominal equality of the maximum penalty therefore does not produce economic equality in its effect. This is precisely where the regulatory proportionality argument becomes powerful: a penalty that is tolerable to a large corporation can be existential to a small business.

4. ODPC HAS ACTUALLY IMPOSED KSHS. 5 MILLION PENALTIES

The ODPC reported issuing KShs. 5 million penalty notices against companies that failed to comply with enforcement notices. The courts have subsequently been required to deal with challenges to substantial penalties.

In *Regus Kenya Limited v Data Protection Commissioner & another [2025] KEHC 13491 (KLR)*, the Commissioner had imposed a KShs. 5 million penalty for failure to demonstrate compliance with the DPA. The company appealed the penalty to the High Court.

Similarly, in *Mulla Pride Limited v Office of the Data Protection Commissioner [2025] KEHC 11287 (KLR)*, the ODPC imposed a penalty of approximately KShs. 2.975 million after issuing an enforcement notice. The company's position was that it had responded to the regulator and was implementing measures including staff training and a verification mechanism.

These cases demonstrate something important for the business-growth debate: compliance expenditure is not hypothetical; businesses are increasingly required to spend money and managerial resources defending, responding to and remediating data-protection enforcement.

5. COMPENSATION CREATES A SECOND FINANCIAL EXPOSURE

The regulatory penalty is only one side of the equation. Section 65 creates civil liability for damage caused by a contravention of the Act. Importantly, "damage" includes financial loss and non-financial damage, including distress. Consequently, a business can potentially face: regulatory enforcement , administrative penalty , compensation , legal costs , compliance expenditure and reputational damage. That cumulative exposure changes the commercial calculus considerably.

The jurisprudence shows that compensation is not merely theoretical. In several matters, the ODPC has awarded compensation of KShs. 200,000 or KShs. 250,000 to individual complainants. In *Aventus Technology Limited v Ndambuki [2025] KEHC 9218 (KLR)*, the High Court considered an ODPC award of KShs. 250,000 arising from the alleged unlawful use of a person's telephone number as a guarantor contact. The court considered, among other matters, whether the award was excessive. The potential awards can be much higher.

In *Ceres Tech Limited v Commissioner, ODPC [2024] KEHC 12833 (KLR)*, the impugned compensation award was KShs. 2.6 million. In WPP Scangroup, the ODPC ordered compensation of approximately KShs. 1.95 million concerning the handling of personal information. For businesses, therefore, the issue is not simply "a fine of KShs. 5 million." The exposure is potentially broader.

6. BUT THE COURTS HAVE SIMULTANEOUSLY STRENGTHENED THE POSITION OF BUSINESSES

The jurisprudence does not give the ODPC unlimited power. Section 64 expressly gives a person aggrieved by administrative action, including enforcement and penalty notices, a right of appeal to the High Court.

In *Arunda v ODPC [2025] KEHC 12262 (KLR)*, the High Court was specifically asked to determine whether the ODPC's powers under section 56 and the Enforcement Regulations were unconstitutional because they allegedly gave an executive agency judicial powers.

The Court rejected that challenge. It held that the ODPC's functions are administrative/quasi-judicial regulatory functions and that the statutory framework preserves judicial oversight through appeal to the High Court. That decision is important because it gives the enforcement regime constitutional legitimacy. But it simultaneously establishes something that is potentially burdensome for businesses: The ODPC is now firmly established as the specialist first-instance forum for data-protection disputes.

7. THE EXHAUSTION DOCTRINE INCREASES THE REGULATORY SIGNIFICANCE OF ODPC

The decision in *Kirima v Solar Panda Company & another [2024] KEHC 11499 (KLR)* is particularly important.

The High Court held that, following enactment of the DPA, disputes concerning breaches of privacy should ordinarily first be presented to the Data Commissioner. The High Court should generally operate as an appellate forum unless the statutory mechanism is incapable of providing an appropriate remedy. The Court essentially endorsed the architecture. Complaint to ODPC investigation ,ODPC determination ,administrative remedy/penalty, finally High Court appeal.

This is good administrative law. It promotes specialised decision-making. But from the business perspective, it also means that regulatory compliance is no longer something that can be treated casually or addressed only when litigation arises. A business must have the systems necessary to respond to an ODPC complaint.

8. THAT PRODUCES A PARTICULARLY SERIOUS PROBLEM FOR MSMES

The ODPC itself has now recognised the special position of MSMEs and issued guidance specifically addressing them. The guidance acknowledges that MSMEs require a simplified approach to compliance and sets out their obligations regarding collection, use, retention, disclosure and disposal of personal data. That is effectively an institutional acknowledgement that the compliance burden is not economically neutral.

Consider two enterprises:

a. **Company A:** 1,000 employees, annual turnover KShs. 5 billion, in-house lawyers, compliance department, IT security team and external privacy consultants.

b. **Company B:** 8 employees, annual turnover KShs. 30 million, one director, one accountant and an outsourced IT provider.

Both may possess customer names, telephone numbers and identification information. The legal principle may be identical but the economic impact of compliance is not.

9. THE REGISTRATION EXEMPTION HELPS—BUT DOES NOT SOLVE THE PROBLEM

The law recognises the problem by exempting certain very small businesses from mandatory registration where they fall below the prescribed turnover/revenue and employee thresholds, subject to sectoral exclusions. But this is only a registration exemption.

It does not mean:"You are a small business, therefore the Data Protection Act does not apply to you." The substantive obligations remain.Consequently, a small business can avoid registration and still have to maintain lawful processing, security, transparency, retention and data-subject rights mechanisms.

10. THE MOST TROUBLING AREA IS BUSINESS MODELS DEPENDENT ON PERSONAL DATA

The impact becomes much more pronounced in sectors such as:

a) digital lending;
b) telecommunications;
c) direct marketing;
d) recruitment;
e) insurance;
f) property management;
g) hospitality;
h) healthcare;
i) education;
j) fintech;
k) credit administration;
l) digital advertising;
m) e-commerce; and
n) BPO/outsourcing.

These businesses necessarily process personal data as part of their business model. The question is therefore not simply whether they can comply with the law. The more difficult question is:

Can a business whose commercial model necessarily depends upon data processing remain commercially viable under a regulatory regime in which almost every stage of its data lifecycle carries potential *regulatory liability?* That is a much more serious economic question.

11. DIRECT MARKETING IS A PARTICULARLY INTERESTING EXAMPLE

A traditional Kenyan business may have built its customer base through telephone calls, SMS, WhatsApp communication and customer databases. Data protection regulation transforms that activity from a relatively informal commercial practice into a regulated processing activity. The business must now consider the legal basis for processing, transparency, legitimate interests, consent where applicable, objections, retention and other data-subject rights. This is undoubtedly beneficial from a privacy standpoint. But there is a corresponding economic cost: the cost of customer acquisition increases when previously inexpensive marketing channels become compliance-sensitive. For a large corporation, that cost is absorbed into its marketing budget but, for a small trader, it may substantially alter the business model.

12. HOWEVER, THERE IS A POWERFUL ARGUMENT ON THE OTHER SIDE

The proposition that data protection inhibits business growth is not necessarily economically correct.

There is a counterargument that strong privacy regulation can actually facilitate economic development. Why?

Because investors and customers are more willing to participate in a digital economy where their information is protected. A Kenyan technology company seeking international contracts may actually benefit from having a credible data-protection framework. A foreign company considering Kenya as a BPO or technology destination may ask whether Kenya has credible privacy regulation.A fintech company handling financial information needs consumer confidence. An e-commerce company needs customers to trust its payment and identity systems.

Thus, data protection can be an economic infrastructure rather than merely a regulatory burden. The question is therefore not whether regulation is good or bad. It is how much regulation, imposed upon whom, for what risk, and at what economic cost?

13. THE RISKS OF REGULATING THE SYMPTOM RATHER THAN THE RISK

This is where I would make the argument considerably more forceful. The DPA adopts a broadly applicable regulatory architecture, but the economic consequences of non-compliance vary enormously according to the size of the enterprise and the sensitivity/volume of data involved. A business processing 300 ordinary customer telephone numbers should not necessarily be treated economically like a business operating a database containing millions of financial, biometric or health records. The principle of risk-based regulation should therefore dominate enforcement.

The DPA itself recognises risk in section 31 through the requirement for DPIAs where processing is likely to result in high risk.

The regulatory philosophy should therefore logically be: higher risk equals greater compliance burden and stronger enforcement and finally greater penalty rather than technical non-compliance, enforcement, potentially devastating financial sanction.That distinction matters enormously for entrepreneurship.

14. PROPORTIONALITY

The courts have increasingly insisted that regulatory decisions must remain within the statutory framework. The Regus litigation is particularly useful because the company challenged the KShs. 5 million penalty and the procedural basis upon which the ODPC acted. Likewise, Ceres Tech demonstrates that an affected business can challenge the regulator's decision, although the court emphasised the statutory appeal route and exhaustion requirement.

15. CONCLUSION

Kenya's data-protection framework is constitutionally legitimate and economically defensible in principle, but its present enforcement architecture risks becoming disproportionately burdensome to small and medium enterprises where compliance obligations, administrative costs, compensation exposure and penalties are not sufficiently calibrated to the size of the enterprise, volume and sensitivity of data processed, degree of culpability and actual harm suffered.

A law intended to protect citizens can, if disproportionately enforced, increase the cost of entrepreneurship.

But the converse is equally true: A weak data-protection regime can destroy consumer confidence, expose businesses to cybercrime, discourage foreign investment and ultimately make Kenya less competitive in the digital economy.

The proper objective should therefore be not deregulation, but proportionate regulation. The countries should move from a predominantly compliance-oriented data-protection culture to a demonstrably risk-based regulatory model.

The ODPC should distinguish between:

1. micro-enterprises and large corporations;
2. ordinary and sensitive personal data;
3. low-volume and mass processing;
4. technical breaches and deliberate exploitation;
5. actual harm and merely formal non-compliance;
6. first-time offenders and repeat offenders;
7. businesses that cooperate with remediation and those that obstruct investigations.

Penalties should then reflect those distinctions.

That would preserve **Article 31** privacy rights while advancing the constitutional and economic objective of creating an environment in which Kenyan businesses can innovate, employ people, attract investment and compete internationally.

In short: the problem is not that the law protects personal data too much. The problem is whether the law has calibrated the *cost of that protection* correctly.

Contributor:

Clapton Evans Kagimu
Principal Associate
ckagimu@cmadvocates.com

CM Advocates LLP – Contact Details

Head Office Nairobi
I&M Bank House, 7th Floor, 2nd Ngong Avenue
T: +254 20 2210978 or +254 716 209673
P.O. Box 22588 – 00505, Nairobi Kenya
E: law@cmadvocates.com

Mombasa Office
Links Plaza, 3rd Floor, Links Road, Nyali
T: +254 041 447 0758 / +254 41 447 0548
P.O. Box 90056 – 80100, Mombasa Kenya
E: mombasaoffice@cmadvocates.com

Regional Presence
Uganda | Tanzania | Rwanda | Zambia | Ethiopia | South Sudan

www.cmadvocates.com