Journal of International Research & Multidisciplinary Innovation

Compliance Challenges for Indian Startups under the Digital Personal Data Protection Act, 2023

Author: Mr. Devendra Upadhyay

Affiliation: Lucknow University

Email: devutherockstar@gmail.com

Submitted to: Journal of International Research & Multidisciplinary Innovation (JIRMI)

Date: 11 February 2026

Abstract

India's Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant step forward in how the country regulates personal data. For the first time, businesses — including startups — face clear, enforceable obligations around how they collect consent, secure data, handle grievances, transfer data across borders, and process information belonging to children. The goal is commendable: build trust in the digital economy while giving individuals meaningful control over their personal information.

But for Indian startups, the reality is more complicated. Most are operating on tight budgets, lean teams, and rapidly evolving technology stacks. Meeting the Act's requirements demands legal expertise, cybersecurity investment, and compliance infrastructure that many early-stage companies simply do not have. Add to this the threat of substantial penalties and a regulatory framework still finding its feet, and the compliance burden begins to look disproportionate. This paper examines those pressures honestly — looking at consent management, data security, third-party risks, and the particular difficulties around children's data. It draws comparisons with the EU's GDPR to understand what India can learn from more mature frameworks. The conclusion is not that the law is wrong, but that its implementation needs to be smarter — more

proportionate, better communicated, and genuinely supportive of the startups that drive India's digital economy.

Keywords

Digital Personal Data Protection Act, 2023, DPDP Act, Indian startups, data privacy, consent management, data fiduciary, data processor, compliance challenges, data protection law, cybersecurity, Data Protection Board of India.

Introduction

The rapid expansion of the digital economy has fundamentally transformed the manner in which businesses collect, process, store, and utilize personal data. Indian startups, particularly those operating in sectors such as fintech, health-tech, ed-tech, e-commerce, and software services, rely extensively upon data-driven technologies to provide personalized services and scale operations. India is ranked the third-largest startup ecosystem globally, with over 31,000 tech startups active as of 2023. The increasing dependence on digital data has simultaneously raised concerns regarding privacy, unauthorized data processing, cybersecurity breaches, and misuse of personal information. In response to these concerns, India enacted the Digital Personal Data Protection Act, 2023 (hereinafter 'the DPDP Act'), establishing a comprehensive legal framework governing the processing of digital personal data.1

The DPDP Act, 2023 seeks to balance the right to privacy of individuals with the legitimate need of businesses to process personal data for lawful purposes. The legislation introduces concepts such as "data fiduciary," "data principal," "consent manager," and "data processor," while imposing obligations relating to lawful consent, purpose limitation, storage limitation, data security safeguards, and grievance redressal. The Act also grants significant rights to individuals, including the right to access information, correction, erasure of personal data, and withdrawal of consent.

Although the legislation is intended to strengthen trust in India's digital ecosystem, startups face unique challenges in complying with the statutory framework. Unlike large corporations with established compliance departments and financial resources, startups often function with limited budgets, lean operational structures, and evolving technological systems. Compliance obligations under the DPDP Act may therefore impose substantial operational and financial burdens upon startups, potentially affecting innovation and business scalability.

A major challenge relates to consent management and ensuring that data processing activities are transparent, lawful, and purpose-specific. Startups frequently depend upon third-party vendors, cloud storage providers, analytics platforms, and artificial intelligence systems, thereby increasing compliance complexities relating to data sharing and processing. Further concerns arise regarding cybersecurity preparedness, breach notification requirements, crossborder data transfers, and the handling of children's personal data.

Another important issue concerns the magnitude of penalties prescribed under the DPDP Act. The Act empowers the Data Protection Board of India to impose substantial monetary penalties for non-compliance, which may severely impact startups lacking adequate compliance mechanisms (DPDP Act, 2023, s. 33 read with the Schedule). The absence of detailed implementation guidelines during the initial stages of enforcement may further create uncertainty for emerging businesses.

This research seeks to critically analyse the compliance challenges faced by Indian startups under the Digital Personal Data Protection Act, 2023. It examines the adequacy of the existing legal framework, the practical difficulties associated with implementation, and the need for balanced regulatory approaches that protect individual privacy while fostering innovation and entrepreneurial growth.

Aims and Objectives of the Study

The primary aim of this research is to critically examine the compliance challenges faced by Indian startups under the Digital Personal Data Protection Act, 2023, and to analyse the impact of such compliance obligations on startup operations, innovation, and sustainability.

The objectives of this research are:

1. To analyse the key provisions of the Digital Personal Data Protection Act, 2023 applicable to startups.
2. To examine the obligations imposed upon startups as data fiduciaries under the Act.
3. To evaluate challenges relating to consent management, cybersecurity, data storage, cross-border data transfers, and grievance redressal.
4. To study the implications of penalties and regulatory enforcement upon startup ecosystems.
5. To analyse the role of data processors, consent managers, and the Data Protection Board of India.
6. To compare India's data protection framework with international standards such as the GDPR.
7. To propose recommendations and reforms that may facilitate effective compliance for startups while promoting innovation and ease of doing business.

Definitions of Important Terms

1. **Digital Personal Data -** Digital personal data refers to personal data in digital form, including data collected online or digitized from offline sources.
2. **Data Principal -** A data principal refers to the individual to whom personal data relates. In the case of children, parents or lawful guardians may exercise rights on their behalf.
3. **Data Fiduciary -** A data fiduciary refers to any person, company, startup, or entity that determines the purpose and means of processing personal data.
4. **Data Processor -** A data processor refers to an entity that processes personal data on behalf of a data fiduciary.
5. **Consent -** Consent under the DPDP Act refers to a free, specific, informed, unconditional, and unambiguous indication of agreement by the data principal for processing personal data.

6. **Consent Manager -** A consent manager is a registered entity that enables data principals to manage, review, grant, or withdraw consent through accessible and transparent mechanisms.
7. **Significant Data Fiduciary -** A significant data fiduciary refers to a data fiduciary classified by the Central Government based on factors such as volume and sensitivity of data processed, risk to individuals, and impact on sovereignty and public order.
8. **Personal Data Breach -** A personal data breach means any unauthorized processing, disclosure, alteration, destruction, or loss of personal data compromising confidentiality, integrity, or availability.
9. **Data Protection Board of India -** The Data Protection Board of India is the adjudicatory body established under the DPDP Act for determining non-compliance and imposing penalties.

Historical Background

The recognition of privacy as a fundamental right in India significantly influenced the development of data protection legislation. In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court declared the right to privacy as an intrinsic part of Article 21 of the Constitution of India.[1] This landmark judgment laid the constitutional foundation for comprehensive data protection legislation.

Following the judgment, the Government of India constituted the Committee of Experts under Justice B.N. Srikrishna to examine issues relating to data protection and recommend a legal framework.6 The Committee's report was submitted to MeitY on 27 July 2018. The committee emphasized the necessity of balancing innovation, economic development, and informational privacy.

[1] The Constitution of India, 1950 (Article 21 – Right to Life and Personal Liberty).

The Personal Data Protection Bill underwent several revisions and parliamentary examinations before eventually evolving into the Digital Personal Data Protection Act, 2023. The legislation was enacted with the objective of regulating digital personal data processing while enabling

lawful business activities and protecting individuals against misuse of personal data. The rise of startups and digital businesses in India further accelerated the need for a robust data protection framework. As startups increasingly relied upon artificial intelligence, cloud computing, analytics, and digital platforms, concerns regarding data misuse, profiling, and cyber threats became more prominent. The DPDP Act therefore emerged as a response to the growing need for accountability and privacy protection in India's expanding digital economy.

Methodology

This research adopts a doctrinal and analytical methodology. The study relies upon primary legal sources including the Digital Personal Data Protection Act, 2023, constitutional provisions, government reports, and judicial decisions. Secondary sources such as research articles, academic journals, policy papers, legal commentaries, and comparative international materials have also been examined.

The research critically analyses statutory provisions relating to startup obligations, consent management, data security, and penalties. Comparative references are drawn from international data protection regimes, particularly the European Union General Data Protection Regulation (GDPR), to evaluate best practices and identify regulatory gaps.

Conceptual and Theoretical Framework

The conceptual framework of this research is based upon the intersection between privacy rights, technological innovation, and regulatory governance. The DPDP Act is grounded in the principle that personal data belongs to the individual and must be processed lawfully and transparently.

The study also incorporates the theory of informational privacy, which recognizes an individual's right to control the collection and dissemination of personal information.8 Alan Westin's foundational work defines privacy as the individual's claim to determine for themselves when, how, and to what extent information about them is communicated to others.8 Simultaneously, the framework considers economic theories emphasizing innovation, digital entrepreneurship, and ease of doing business. Another important theoretical aspect is risk-based regulation, which suggests that compliance obligations should be proportionate to the scale and sensitivity of data processing activities. Startups generally operate with evolving business models and limited compliance infrastructure, making proportional regulation essential for fostering innovation. The framework additionally examines accountability principles, cybersecurity governance, and algorithmic transparency, particularly where startups use artificial intelligence and automated decision-making systems.

Literature Review

Scholarly discussions surrounding the DPDP Act largely focus upon balancing privacy protection with economic growth and technological advancement. Several authors emphasize that startups face disproportionate compliance burdens due to limited financial and legal resources.

Researchers have noted that consent-based frameworks may become operationally difficult for startups handling large volumes of user data through mobile applications and digital platforms.[2] Obtaining meaningful consent, maintaining records, and enabling withdrawal mechanisms require technological infrastructure that many early-stage startups may lack.12

Cybersecurity scholars further argue that data protection compliance extends beyond legal obligations and requires substantial investment in technical safeguards, encryption mechanisms, incident response systems, and employee training programs. Smaller businesses may struggle to implement such systems effectively. Comparative studies examining the GDPR

[2] Negri-Ribalta, C. et al., 'Tech Startups and General Data Protection Regulation: An Empirical Exploration of Compliance Challenges' (2025) 32(8) Journal of Small Business and Enterprise Development 54, Emerald Publishing. DOI: 10.1108/JSBED-02-2025-0000.

suggest that strict compliance obligations can increase operational costs for startups and small enterprises.[3] However, scholars also observe that strong privacy protections enhance consumer trust and long-term sustainability.[4]

Another major area of academic discussion concerns penalties under the DPDP Act. Legal commentators highlight that substantial monetary penalties may create fear and uncertainty among startups, particularly where regulatory guidelines remain ambiguous. Overall, the literature reflects a growing consensus that while data protection legislation is essential for safeguarding privacy, implementation frameworks must consider the realities and constraints faced by startups and emerging businesses.

Legal Framework

The legal framework governing personal data protection in India primarily consists of the Digital Personal Data Protection Act, 2023. The Act applies to the processing of digital personal data within India and also applies extraterritorially where goods or services are offered to individuals in India.

The Act imposes obligations upon data fiduciaries, including:

- Processing personal data only for lawful purposes.
- Obtaining valid consent.
- Providing clear privacy notices.
- Implementing reasonable security safeguards.
- Deleting data upon withdrawal of consent or completion of purpose.

[3] Negri-Ribalta, C. et al., 'Tech Startups and General Data Protection Regulation: An Empirical Exploration of Compliance Challenges' (2025) 32(8) Journal of Small Business and Enterprise Development 54, Emerald Publishing. DOI: 10.1108/JSBED-02-2025-0000.
[4] Ibid.

- Reporting personal data breaches.
- Establishing grievance redressal mechanisms.

The legislation also grants rights to data principals, including:

- Right to access information.
- Right to correction and erasure.
- Right to grievance redressal.
- Right to nominate another person.

The Data Protection Board of India is empowered to investigate non-compliance and impose monetary penalties. The Act prescribes significant penalties for failure to implement security safeguards, failure to notify breaches, and unlawful processing of children's data.

The framework additionally permits cross-border transfer of personal data subject to restrictions imposed by the Central Government. This is particularly relevant for startups utilizing global cloud infrastructure and international service providers.

Compliance Challenges Faced by Indian Startups

1. Consent Management Challenges

One of the most significant compliance challenges relates to obtaining valid consent. The DPDP Act requires consent to be free, informed, specific, and unambiguous. Many startups rely upon complex digital ecosystems involving mobile applications, cookies, third-party integrations, and analytics tools, making it difficult to ensure fully informed consent.

Startups may also struggle to maintain systems enabling users to easily withdraw consent. Frequent consent requests may additionally reduce user engagement and create operational inefficiencies.

2. Financial Burden of Compliance

Compliance under the DPDP Act requires investment in:

- Legal advisory services,
- Cybersecurity infrastructure,
- Privacy policies,
- Data audits,
- Employee training,
- Consent management systems,
- Data breach response mechanisms.

For early-stage startups operating with limited funding, such expenses may significantly affect operational sustainability.

3. Cybersecurity and Technical Infrastructure

The obligation to implement "reasonable security safeguards" creates ambiguity regarding the exact level of cybersecurity expected from startups. Many startups lack dedicated cybersecurity teams and may remain vulnerable to phishing attacks, ransomware, cloud vulnerabilities, and unauthorized access.

A personal data breach may lead not only to financial penalties but also reputational damage and loss of consumer trust. Industry data indicates that the average cost of a data breach in India reached USD 2.35 million in 2024, a 39 per cent rise since 2020.[5]

4. Cross-Border Data Transfer Issues

Numerous Indian startups rely upon international cloud storage providers and SaaS platforms. Restrictions relating to cross-border data transfers may create uncertainty regarding compliance obligations and vendor management.

Startups may need to renegotiate agreements with foreign service providers or localize certain categories of data, increasing operational complexity.

[5] IBM Security, 'Cost of a Data Breach Report 2024' (IBM Corporation, July 2024).

5. Third-Party Vendor Risks

Startups frequently engage third-party processors for payment gateways, analytics, customer support, cloud hosting, and marketing automation. Ensuring that all vendors comply with DPDP requirements becomes a significant contractual and operational challenge.

Any non-compliance by third-party processors may expose startups to regulatory liability.

6. Children's Data Compliance

The DPDP Act imposes stricter obligations for processing children's personal data. Startups operating in ed-tech, gaming, and social media sectors may face difficulties in:

- Verifying age,
- Obtaining parental consent,
- Preventing targeted advertising,
- Ensuring child safety standards.

Implementing age-verification mechanisms may also raise practical and technological concerns.

7. Lack of Awareness and Skilled Professionals

Many startups lack internal legal and compliance teams familiar with privacy laws and cybersecurity obligations.[6] India presently faces a shortage of trained privacy professionals, making compliance implementation more difficult for emerging businesses.[7]

8. Regulatory Uncertainty

Since the DPDP Act is relatively recent legislation, startups face uncertainty regarding:

- Interpretation of statutory obligations,

[6] Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce and Industry, Government of India, 'Annual Startup Report 2023' (New Delhi, 2023).

[7] IBM Security, 'Cost of a Data Breach Report 2024' (IBM Corporation, July 2024).

- Future rules and regulations,
- Enforcement practices,
- Technical compliance standards.

This uncertainty may discourage experimentation and innovation in data-driven sectors.

9. Heavy Penalties and Enforcement Risks

The Act prescribes substantial monetary penalties for non-compliance. Even accidental violations or minor procedural lapses may expose startups to severe financial consequences. Fear of enforcement action may compel startups to divert substantial resources toward compliance rather than innovation and product development.

Comparative Analysis with GDPR

The European Union's General Data Protection Regulation (hereinafter "GDPR") provides one of the most influential global models for data protection regulation.[8] At a broad level, the GDPR and the DPDP Act share a common philosophical foundation — both are built around consentbased processing, recognise individual rights over personal data, mandate data breach reporting, emphasise accountability, and prescribe substantial penalties for non-compliance. However, the similarities should not obscure meaningful differences in depth and design. The GDPR is considerably more prescriptive in its procedural requirements and offers broader protections in areas such as automated decision-making and profiling, which remain less developed under the Indian framework. The DPDP Act, by contrast, takes a comparatively business-friendly stance on cross-border data transfers, adopting a negative-list approach rather than the adequacy-decision model that governs transfers under the GDPR. The GDPR also establishes stronger institutional safeguards through independent supervisory authorities with wide investigative and corrective powers, whereas the Data Protection Board of India is still in the early stages of operationalisation. Taken together, this comparative analysis suggests that

[8] 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 (General Data Protection Regulation), OJ L 119, 4 May 2016, pp. 1–88.

while India's framework is well-conceived, it remains a work in progress — one that will require further elaboration through delegated rules, judicial interpretation, and sector-specific guidelines before it can be considered fully mature.

Analysis

The DPDP Act represents an important step toward strengthening privacy protection and digital governance in India. However, the implementation of the legislation reveals a tension between regulatory compliance and startup innovation.

While large corporations may possess the resources necessary to establish sophisticated compliance frameworks, startups often function within constrained environments characterized by rapid scaling, limited staffing, and uncertain funding cycles. Compliance obligations under the Act may therefore create disproportionate burdens for smaller enterprises. The requirement of meaningful consent highlights this challenge. In theory, informed consent enhances user autonomy and transparency. In practice, however, startups handling large-scale digital interactions may struggle to design systems that are simultaneously legally compliant and userfriendly. The absence of precise statutory definitions for terms such as “reasonable security safeguards” also creates interpretational difficulties. Startups may remain uncertain regarding the extent of cybersecurity measures required to avoid penalties.

Another critical issue concerns balancing innovation with regulation. Excessively burdensome compliance obligations may discourage startups from experimenting with artificial intelligence, analytics, and personalized digital services. On the other hand, weak regulation could expose users to privacy violations and misuse of personal information. The effectiveness of the DPDP framework will therefore depend upon flexible implementation, sector-specific guidance, and cooperative regulatory approaches that encourage compliance while supporting entrepreneurial growth.

Discoveries

The research reveals several important findings:

1. The DPDP Act establishes a comprehensive legal framework for digital personal data protection in India.
2. Startups face disproportionate compliance challenges due to limited financial, legal, and technological resources.
3. Consent management and cybersecurity compliance represent the most difficult operational obligations for startups.
4. Ambiguity regarding implementation standards increases compliance uncertainty.
5. Heavy monetary penalties may adversely affect startup sustainability and innovation (DPDP Act, 2023, Schedule).1
6. Third-party vendor management and cross-border data transfer obligations significantly complicate compliance processes.
7. Awareness regarding privacy compliance remains limited among many emerging businesses.
8. There is a strong need for phased compliance mechanisms and startup-specific guidance frameworks.

Limitations of the Study

This research is subject to certain limitations. The DPDP Act is relatively recent legislation, and many implementation rules and enforcement practices are still evolving. Consequently, practical judicial interpretation remains limited. The study primarily adopts doctrinal and analytical methodology and does not incorporate extensive empirical data from startup founders, compliance officers, or regulatory authorities. The rapidly changing nature of technology and digital business models may also affect the long-term applicability of certain observations made within this research. Furthermore, while comparative references to international frameworks have been included, the research primarily focuses upon the Indian

legal context and does not provide an exhaustive comparative analysis of global privacy regimes.

Conclusion

The Digital Personal Data Protection Act, 2023 represents a landmark development in India's digital regulatory landscape. The legislation strengthens privacy protection, enhances accountability, and establishes legal safeguards for the processing of digital personal data. For Indian startups, however, compliance with the Act presents substantial operational, technical, and financial challenges. The research demonstrates that startups may struggle to implement effective consent management systems, cybersecurity safeguards, vendor oversight mechanisms, and grievance redressal frameworks due to resource constraints and regulatory uncertainty. The possibility of significant monetary penalties further intensifies compliance concerns.

Despite these challenges, strong data protection practices may ultimately benefit startups by enhancing consumer trust, improving data governance standards, and increasing investor confidence. The long-term success of the DPDP framework will therefore depend upon balanced implementation that protects privacy while encouraging innovation and entrepreneurship. The study concludes that India requires a flexible, proportionate, and startupfriendly approach toward privacy regulation. Legislative clarification, sector-specific guidance, awareness initiatives, and phased compliance frameworks will be essential in ensuring that startups can effectively comply with the DPDP Act without undermining innovation and economic growth.

Recommendations

In light of the findings of this research, the following recommendations are offered to facilitate more effective and balanced implementation of the DPDP Act for Indian startups. The most immediate need is a startup-specific compliance framework. The Government should introduce simplified and phased compliance mechanisms for startups and small businesses, particularly

during the initial stages of enforcement, so that obligations are introduced gradually rather than all at once. Alongside this, detailed sector-wise guidelines should be issued covering consent management, cybersecurity standards, data breach reporting, cross-border transfers, and vendor management — areas where regulatory ambiguity currently causes the greatest uncertainty for emerging businesses.

Financial and technical support will be equally important. Compliance toolkits, governmentbacked support programs, and awareness initiatives can go a long way in helping startups build privacy frameworks without incurring prohibitive costs. Related to this, startups should be actively encouraged to adopt privacy-by-design principles from the earliest stages of product development rather than treating compliance as an afterthought. Ann Cavoukian's seven foundational principles provide a practical conceptual basis for this approach, emphasising that privacy must be proactively embedded into system architecture rather than added on after the fact. Capacity building deserves dedicated attention. Awareness programs and specialised training for startup founders, legal professionals, developers, and compliance officers are essential if the spirit of the DPDP Act is to translate into genuine organisational practice rather than superficial box-ticking. On the enforcement side, penalty frameworks should be calibrated to distinguish between deliberate violations and procedural lapses by early-stage startups acting in good faith — a one-size-fits-all approach to penalties risks penalising inexperience rather than misconduct.

At the ecosystem level, the Government should promote affordable cybersecurity infrastructure and encourage meaningful collaboration between startups and cybersecurity service providers. Industry associations and startup incubators similarly have a role to play in working with regulators to develop compliance standards that reflect the realities of emerging businesses rather than being designed solely around large enterprises. Courts and regulatory authorities, for their part, should adopt a balanced and purposive approach when interpreting the Act's obligations, ensuring that enforcement does not inadvertently stifle the innovation India's digital economy depends upon. Finally, as artificial intelligence, analytics, and other technologies continue to evolve, the legal framework itself must remain dynamic — subject to continuous review and reform so that it keeps pace with emerging technological realities and global best practices.

References

1. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Ministry of Electronics and Information Technology, Government of India. Passed by Parliament on 7 August 2023; assented to by the President on 11 August 2023. Available at: <https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf>.
2. The Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India (notified November 2025).
3. The Constitution of India, 1950 (Article 21 – Right to Life and Personal Liberty).
4. 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 (General Data Protection Regulation), OJ L 119, 4 May 2016, pp. 1–88.
5. Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1; AIR 2017 SC 4161 (Supreme Court of India, Nine-Judge Constitution Bench, 24 August 2017).
6. Ministry of Electronics and Information Technology, Government of India, 'A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians – Report of the Committee of Experts on a Data Protection Framework for India' (Justice B.N. Srikrishna Committee Report, submitted 27 July 2018). Available at: <https://meity.gov.in/sites/upload_files/dit/files/Data_Protection_Committee_Report.pdf>.
7. Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce and Industry, Government of India, 'Annual Startup Report 2023' (New Delhi, 2023).
8. Westin, Alan F., Privacy and Freedom (Atheneum, New York, 1967; reissued Ig Publishing, New York, 2015). [Foundational text on informational privacy theory.]
9. Cavoukian, Ann, 'Privacy by Design: The 7 Foundational Principles' (Information and Privacy Commissioner of Ontario, 2009, revised 2011).

10. NASSCOM and Zinnov, ‘Weathering the Challenges: The Indian Tech Start-up Landscape Report 2023’ (NASSCOM, New Delhi, 2023). Available at: <https://nasscom.in/knowledgecenter/publications/weathering-challenges-indian-tech-start-landscape-report-2023>.

11. IBM Security, ‘Cost of a Data Breach Report 2024’ (IBM Corporation, July 2024). [Data on average breach cost in India reaching USD 2.35 million in 2024, a 39% rise since 2020.]

12. Negri-Ribalta, C. et al., ‘Tech Startups and General Data Protection Regulation: An Empirical Exploration of Compliance Challenges’ (2025) 32(8) Journal of Small Business and Enterprise Development 54, Emerald Publishing. DOI: 10.1108/JSBED-02-2025-0000.