September 2, 2025

Acting Director Elizabeth Harris
New Jersey Division of Consumer Affairs
124 Halsey Street
PO Box 45027
Newark, New Jersey 07101

RE: Comments of ACT | The App Association on the Proposed Rule Implementing the New Jersey Data Privacy Act.

Dear Acting Director Harris:

ACT | The App Association submits these comments in response to the proposed rule at N.J.A.C. 13:45L implementing the New Jersey Data Privacy Act.[1]

The App Association represents small business innovators and startups in the software development and high-tech space located in New Jersey and across the United States.[2] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, the app economy is worth more than $1.8 trillion and provides over 6.1 million American jobs.[3]

The proposed rule contains far-reaching and unusually restrictive mandates on privacy and security practices. As the Division of Consumer Affairs (Division) reviews recommendations to further its objectives, we encourage careful consideration of how the rules might impact small and medium-sized developers who may lack the resources of larger companies to manage complex compliance obligations. We appreciate the opportunity to weigh in on how the rule's goals of protecting consumer privacy can be achieved without unduly burdening small businesses or impeding digital innovation.

Supporting Small Business Compliance with the Rule

While the proposed rule offers strong protections for consumer data, it may also impose significant burdens on the small businesses subject to its requirements. Unlike most other states, New Jersey's consumer privacy law covers all businesses regardless of annual revenue, instead limiting applicability on thresholds tied to the number of New Jersey consumers from whom a business controls or processes personal data.[4] While the

[1] Proposed New Rules: N.J.A.C. 13:45L.

[2] ACT | The App Association, *About*, *available at* http://actonline.org/about.

[3] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf.

[4] 56 N.J. Rev. Stat. C.56:8-166.5(a) (2023).

threshold of 100,000 New Jersey consumers for businesses that do not sell personal data may exempt some of our member companies, those based in New Jersey likely must pay close attention in case they are near or over the applicable threshold. Therefore, the Division is not free to ignore small business compliance considerations and must consider them. To support effective implementation, the Division should revise certain provisions to ease compliance obligations and reduce associated operational challenges.

First, the Division should revise N.J.A.C. 13:45L-1.4(a)8, which currently requires that disclosures, notifications, and other communications be made available in printable format, to apply only where feasible. As written, the requirement does not account for the context and format in which many consumers receive privacy notices, such as interactive or multimedia formats within app environments where printable formats are not practical or meaningful. Moreover, requiring communications to be printable may not benefit consumers who primarily interact with controllers online. This requirement would also disadvantage small businesses, which may not have the administrative overhead to create, maintain, and update printable disclosures that conform to appropriate formatting and technical specifications to make printing reliable across different devices and browsers.

Second, in N.J.A.C. 13:45L-3.1 and 3.2, the Division should remove requirements that businesses provide consumers with an in-person method to exercise their data rights. This mandate overlooks the reality that many small businesses lack the resources to train customer-facing staff to handle such requests, especially when doing so could disrupt operations or compromise customer service. While enhancing the accessibility of consumer data rights is a laudable goal, the rule should allow more flexibility in how controllers accept and process these requests.

Third, in N.J.A.C. 13:45L-3.4(f), the Division should moderate the requirement that controllers wait at least 12 months after a consumer opts out of processing for targeted advertising, the sale of personal data, or profiling for decisions with legal or similarly significant effects before requesting consent again. Many small businesses rely on targeted advertising to efficiently reach potential customers with limited marketing resources. Requiring them to wait 12 months before re-engaging consumers who might be willing to interact sooner than the 12-month requirement significantly constrains their outreach strategies and ignores how consumer preferences may evolve over time. To that end, the Division should replace the 12-month waiting period with a requirement that controllers wait a reasonable amount of time between consent requests to prevent a repetitive pattern of solicitation.

Fourth, while the requirement to authenticate non-account holders' identities in response to consumer requests in N.J.A.C. 13:45L-4.3 is worthwhile, the Division should remove the requirement for controllers to annually evaluate and document whether reasonable methods exist. In order to comply with this documentation requirement, small businesses would have to divert limited resources away from core functions, such as hiring, product development, and other areas critical to growth, and towards administrative tasks that do not meaningfully advance consumer privacy protection.

Fifth, the Division should strike or modify the requirements in N.J.A.C. 13:45L-2.2 and 13:45L-6.1 that controllers disclose and describe the purpose for which data is processed in sufficient detail for consumers to understand how each category of their data is used, as well as the length of time controllers intend to retain data. This level of granularity imposes a substantial administrative burden on small businesses, which must draft, maintain, and update compliant language across all categories of data. Articulating use purposes and timing in such a specific manner may also require specialized legal or technical expertise that many small businesses may not have. For example, App Association member company TechNeed, a Hopewell-based digital product studio, built a data collection platform for their client, Easy, a digital health company. The platform, with integrated APIs, enabled value-based care by streamlining data collection from patients and providers, giving doctors faster access to better data and allowing patients to easily access and share their health information. None of these activities involve selling user data or assigning it a dollar value, yet under the proposed rule, TechNeed could be required to articulate granular justifications for data collection and retention that don't align with their model. For organizations working at the intersection of technology and community care, this kind of requirement adds complexity without improving transparency, diverting limited resources from the people they serve. Moreover, it is unclear whether this level of detail offers meaningful benefit to consumers, particularly when higher-level descriptions or an explanation of retention criteria can still effectively inform their decisions.

Sixth, the Division should remove the requirement in N.J.A.C. 13:45L-6.3 that controllers annually assess and document the necessity of retaining biometric identifiers, photographs, audio or video recordings, or data generated from such recordings. Mandating this evaluation and documentation imposes a significant administrative burden on small businesses, which often collect such data in the course of operations and to support essential functions like customer service, fraud prevention, and workplace security. Requiring annual reassessments and documentation is unlikely to change these legitimate business needs, lead to a meaningful reduction in data retention, or offer practical benefit to consumers.

For example, App Association Member company Sheer Health, a New Jersey-born health tech startup, provides secure communication tools between patients and care teams, handling sensitive health-related data on a daily basis. Despite having a team of fewer than 50 employees, they invest heavily in compliance with the Health Insurance Portability and Accountability Act (HIPAA) to ensure the security and accuracy of patient information, while also working to simplify complex medical billing and claims issues for consumers. Under the proposed rule, Sheer Health would be required to reassess and document its biometric data retention practices at least annually, even though its health data processing, which may include biometric identifiers, is already closely governed by HIPAA. For a small team, this overlapping effort doesn't just strain resources; it disrupts

ongoing development and imposes legal obligations on top of a framework that already mandates secure, privacy-protective practices. Rather than enhancing privacy, this kind of layered redundancy risks disproportionately burdening small innovators that already invest heavily in consumer protection.

Seventh, the Division should strike requirements in N.J.A.C. 13:45L-2.5(e)2 for controllers to calculate the value of consumers' personal data in connection with loyalty programs. Estimating such value would impose a significant burden on small businesses, particularly given the absence of a standard methodology for such calculations. Assessing factors such as operational savings from personalization, data monetization potential, or market value benchmarks requires analytical resources and expertise that small businesses may lack. Moreover, many small businesses rely on third-party service providers to operate loyalty programs and may not have sufficient access to the underlying data or processing logic to produce even good-faith valuations.

Finally, the Division should prioritize creating guidance for small businesses that includes clear instructions or illustrative examples on how to comply with the rule. In particular, identifying and formally recognizing opt-out preference signals that satisfy the requirement in N.J.A.C. 13:45L-5.2 to be in a "format commonly used and recognized by controllers" would significantly ease compliance burdens. Such guidance would enable small businesses to better comply with the law without needing to hire legal counsel or navigate the rule's intent on their own.

Clarifying Regulatory Scope, Definitions, and Requirements

As written, the proposed rule introduces uncertainty through inconsistent analysis, overly broad definitions, and ambiguous regulatory requirements. To facilitate compliance, particularly for small businesses, the Division should revise and clarify three key provisions.

First, while the regulatory flexibility analysis accompanying the proposed rule states that the Division believes the rule must be applied to all controllers, regardless of size, this position appears to conflict with the rule's scope, which incorporates statutory applicability thresholds. To avoid confusion and ensure clarity regarding regulatory intent, the Division should reconcile this discrepancy and clarify whether those thresholds effectively exempt small businesses from compliance. As currently written, this inconsistency may create unnecessary uncertainty about whether small businesses fall within its scope.

Further, in N.J.A.C. 13:45L-1.2, the Division should revise the definition of "data broker" to better capture persons or legal entities engaged in the business of selling consumer data. As currently drafted, the rule defines a data broker as any person or entity that "collects, purchases, or sells" the personal data of consumers they do not know. This overly broad language could inadvertently classify many businesses as data brokers, including those that collect or purchase data solely for internal use and do not engage in selling it. To avoid imposing disproportionate compliance obligations on businesses that

do not engage in data brokering as commonly understood, the Division should narrow the focus of the definition to only entities that sell consumer data.

Finally, in N.J.A.C. 13:45L-5.1(c), the Division should reconsider the obligation that controllers treat opt-out preference signals as a directive to opt out of processing consumer profiles associated with a "network." It is unclear what constitutes a network, which creates significant ambiguity for controllers and leaves them without clear guidance on how to apply opt-out signals in practice. Moreover, the ambiguity is likely to result in overcompliance, imposing technical and operational demands that many small businesses may be unable to meet due to infrastructure costs, implementation challenges, or reliance on third-party service providers. The Division should either clarify the scope and intent of this provision or strike the network-based obligation altogether.

Practical Challenges in Operationalizing Consumer Rights

The rule rightly emphasizes consumers' rights to control their personal data. However, to make the section more effective, the Division should prioritize three changes that would reduce operational burdens while preserving meaningful consumer protections.

To that end, the Division should strike requirements in N.J.A.C. 13:45L-3.4(a)4 and 13:45-3.7(a)3 that obligate controllers to notify third parties of a consumer's opt-out or deletion requests. Flowing down such requests may impose significant burdens on small businesses, which often lack the data mapping capabilities to comprehensively and effectively comply with this requirement. It would also increase administrative overhead, as small businesses would be required to verify and coordinate these requests with vendors or other third parties. This challenge is compounded by the fact that many small businesses do not have the leverage to negotiate custom data processing agreements that could facilitate compliance. Moreover, automatically forwarding such requests may not reflect the consumer's intent in every case and could result in unintended consequences.

For example, App Association member company Harbor Technology Group, based in Hopewell, New Jersey, is a cybersecurity firm serving small and mid-sized businesses. They frequently manage data protection protocols for clients with complex vendor ecosystems. Under the proposed rule, controllers like Harbor Technology Group (and their clients) would be required not only to honor consumer opt-out requests but also notify every third party with access to that data and ensure those third parties pass the request along to others in the chain. For small firms already navigating multiple compliance frameworks, this is not just a resource burden; it's a logistical impossibility.

In N.J.A.C. 13:45L-3.3(c)4, the Division should clarify that controllers do not have to disclose specific fraud detection methods when explaining the factual basis for determining a request is fraudulent or abusive. Disclosing fraud detection methods in detail could enable bad actors to circumvent existing controls or craft fraudulent requests designed to evade detection. Under N.J.A.C. 13:45L-3.3(c)4's requirement to disclose detection methods, Harbor Technology Group could be limited in their ability to protect

users, leaving them vulnerable to future fraudulent requests. The Division should modify this provision to allow controllers to withhold sensitive details about their fraud detection methods while still offering a good-faith explanation for denying a request. Otherwise, these ambiguities force small companies into a lose-lose scenario: either risk noncompliance or compromise their security posture.

Advancing Responsible Research and Third-Party Data Practices

The rule's requirements regarding data sharing and third-party relationships aim to strengthen consumer privacy but may also create compliance challenges for small businesses that rely on third-party tools, partners, or vendors. To ensure the rule is both effective and practical, the Division should clarify or revise provisions that affect third-party relationships and the responsible use of personal data for research and innovation.

First, the Division should revise the definition of "sale" in N.J.A.C. 13:45L-1.2. As currently drafted, the rule exempts disclosures of personal data to third parties if the third party processes the data on behalf of the controller or to provide a product or service requested by the consumer and does not use the data for their own purposes. However, this narrow framing may inadvertently hamper the ability of third parties to deliver requested goods or services to consumers, especially when doing so involves limited internal use of data, such as for analytics or operational improvements, outside of immediate service delivery. This provision may also disadvantage small businesses in particular, as they often do not have the legal and technical resources to negotiate complex data use agreements that clearly delineate own-purpose uses from service-related processing. As a result, small businesses may face uncertainty about compliance, increased regulatory exposure, and pressure to work primarily with traditional service providers, while their larger counterparts retain flexibility to structure compliant agreements with favorable terms.

For example, App Association Member company Fool Me Once, based in Spring Lake, New Jersey, develops AI-driven solutions that depend on integrations with third-party analytics tools, cloud services, and research partners. These relationships allow the company to improve its offerings without ever selling or misusing user data. Yet under the proposed rule, Fool Me Once could be subject to complex and potentially burdensome compliance requirements when sharing data with third parties, even when those interactions are secure, service-related, and not monetized. For companies like Fool Me Once, the rule's treatment of third-party data flows creates a compliance thicket that risks stalling innovation without providing meaningful privacy gains for consumers. The Division should strike the latter part of the exemption to allow disclosures of personal data to third parties when necessary to provide a requested product or service, regardless of whether the third party uses the data for its own purposes.

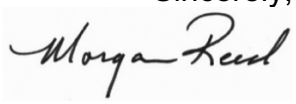
Further, the Division should modify the internal research exemption in N.J.A.C. 13:45L-1.3 to allow controllers to use personal data for internal AI system training and to share resulting research with third parties, without imposing additional restrictions. As

currently drafted, the requirement to obtain affirmative consent for AI training or share research only after de-identifying data or limit it to specific purposes places undue constraints on innovation and research. While protecting consumer data is essential, the rule already includes meaningful safeguards and mechanisms for consumer control. Imposing additional restrictions on internal research is unlikely to offer significant privacy benefits but would create substantial burdens for businesses and hinder innovation in New Jersey's science and technology sectors.

Finally, the Division should revise N.J.A.C. 13:45L-2.1(e) to account for situations in which a third party collects personal data but cannot provide direct notice to the consumer at or before the point of collection. This requirement creates significant challenges for third parties that lack a direct relationship with the consumer and have no practical means of delivering a notice. In particular, small businesses may face compliance uncertainty, especially where they rely on third-party tools or services, and may be unable to ensure that consumers receive disclosures with the appropriate information at or before the point of collection. The Division should clarify how notice obligations apply in these indirect collection scenarios or provide flexibility for both parties.

We appreciate your consideration of the above views and welcome any opportunity to provide additional commentary as the process advances.

Sincerely,



Morgan Reed
President
ACT | The App Association