Response by the Centre for Information Policy Leadership to the Proposed Rules for the New Jersey Data Privacy Act

Submitted September 2, 2025

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to respond to the New Jersey Division of Consumer Affairs' (Division) proposed rules for the New Jersey Data Privacy Act (NJDPA or Act). CIPL commends this effort to clarify the scope and application of key concepts included in the Act. The NJDPA and these proposed rules represent significant steps towards strengthening privacy protections for New Jersey residents while signalling the state's engagement in shaping a modern, risk-focused data governance framework.

CIPL respectfully offers these comments to further assist the Division in ensuring that the proposed rules are clear, workable, and aligned with practical implementation considerations. Our comments aim to identify areas where further specificity may be beneficial, where harmonization with other state privacy laws could reduce compliance burdens for organizations of all sizes, and where adjustments may be necessary to enable technological innovation while supporting consumers' privacy.

Our key recommendations below highlight opportunities to further strengthen the rules by utilizing a risk-based approach grounded in the concepts of organizational accountability[2]:

- As a general matter, lawmakers and regulators should encourage organizations to invest in accountability and recognize the use of demonstrated accountability measures as a mitigating factor in enforcement.

- Organizations need consistency in terminology and definitions in order to build cohesive and effective data protection assessment and compliance programs.

- To enable beneficial development and use of AI and other emerging technologies in the modern information age, laws and regulatory guidance should facilitate lawful mechanisms for the use of personal data in AI model training. Lawmakers and regulators should avoid legal

---

[1] **The Centre for Information Policy Leadership (CIPL)** is a global privacy and data policy think tank within the Hunton law firm that is financially supported by 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] For more than a decade, CIPL has pioneered organizational accountability as a key building block of effective data privacy regulation and its corresponding implementation within companies. See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

interpretations that are unduly restrictive regarding the use of personal data in AI model training, development, and deployment.

- Regulations addressing the use of sensitive data, including biometric data, should contain obligations tailored to the level of risk. The rules should acknowledge that certain technical or governance measures can reduce or mitigate risks to acceptable levels, and reserve heightened requirements or outright bans for high-risk use cases where safeguards are not available.

- The purposes, uses, application, and capabilities of processing personal data should be the focus of the rules rather than the nature of the data, with a view to not impeding deployment of low-risk processing.

- Data minimization principles should be interpreted so as to enable the collection and use of personal data that is necessary and appropriate for ensuring accuracy and preventing bias in AI models and ensuring robust customer experiences for data-enabled products and services.

While rules in New Jersey ordinarily take effect immediately upon the publication of a Notice of Adoption, CIPL urges the Division to provide at least a 24-month grace period between the finalization of the rules and the commencement of enforcement, given the complexity and extensive nature of these rules.

We provide more granular comments on the regulations below across four topic areas: (I) General Comments, (II) Artificial Intelligence, (III) Biometric Data, and (IV) Consumer Requests and Disclosures.

TABLE OF CONTENTS

I. GENERAL COMMENTS

CIPL submits that the following changes could be helpful for sharpening the focus of the obligations in connection with New Jersey's consumer privacy mandate and providing businesses with necessary clarity:

- **N.J.A.C. 13:45L-1.2: Limit definition of data broker to those who "sell or license."**

The proposed rules adopt a broad definition of "data broker" as "a person or legal entity, including a controller, that knowingly, collects, purchases, or sells to third parties the personal data of a consumer with whom the person or legal entity does not have a direct relationship." The proposed definition does not limit the definition of data brokers to persons or entities that sell or license customer data to third parties. As such, it creates an unprecedented expansion of the concept of a data broker to include persons or entities that merely collect or purchase data from third parties, regardless of whether they actually sell or license the data. Such a broad definition would drastically impact the business model of many businesses, including small businesses, that rely on third-party data for product development and marketing purposes.

Data broker provisions are usually written to regulate intermediaries who fall outside the scope of general privacy laws. A more narrow definition of a "data broker" that focuses on the sale or licensing of data would address intermediaries who are not subject to general data privacy laws while avoiding overly burdensome and overlapping regulations.

- **N.J.A.C. 13:45L-1.2: Narrow definition of "essential goods and services."**

The definition of "essential goods and services"—any objects, wares, goods, commodities, services, or anything that is consumed or used to preserve, protect, or sustain the life, health, safety, or comfort of persons or their property—is very broad and could be interpreted to include almost anything. Because this concept is nested within the definition of "Decisions that produce legal or similarly significant effects concerning the consumer," the proposed definition takes on even greater significance. For example, a controller who processes personal data in order to profile likely consumers of running shoes would arguably need to comply with any provision related to decisions that produce "legal or similarly significant effects," because running shoes are arguably "goods" used to "preserve" the "health" or "comfort" of persons. Clearly, running shoes are not "essential goods and services," and a decision to purchase a pair should not be considered one that produces "legal or similarly significant effects."

- **N.J.A.C. 13:45L-1.2: Clarify definition of "personal data"**

The proposed rule expands the statutory definition of "personal data" in a way that creates significant confusion about what data is in scope. In particular, it is unclear whether the list of 11 types of data—including IP addresses and other unique device identifiers—are data types that themselves are inherently "reasonably linkable" to a person, or if they are examples of "other data," which, when aggregated with some other, unknown data, renders that other, unknown data "reasonably linkable."

- **N.J.A.C. 13:45L-1.2: Exclude reference to third parties not using data for their own purposes from definition of "sale."**

The proposed rules indicate that a "sale" shall not include the disclosure of personal data to a third party for the purposes of providing a product or service requested by the consumer, "***provided the third party does not use the data for its own purposes.***" This language expands the statutory definition of a "sale"[3] and is inconsistent with the purpose of this exception, which is to allow a consumer to use products and services that permit third-party integrations. For example, a smart stereo system may permit a consumer to connect with a music streaming service. If a consumer consents and directs the stereo system to pass a song request to the streaming service to play on the stereo, then the streaming service should be able to use that request for its own purposes, such as to customize the next song to play.

- **N.J.A.C. 13:45L-1.2: Limit the application of "revealing" in definition of "sensitive data."**

While the proposed regulation defines "sensitive data" with text that largely tracks the statutory language, the formatting used in the proposed rule highlights a problematic use of the modifier "revealing." The proposed rule defines "sensitive data" as "personal data ***revealing*** …," followed by a colon and a numbered list of attributes, but some of the items in that list refer to types of data that, standing alone, are sensitive in and of themselves. For example, "personal data collected from a known child" is sensitive on its face. As such, the regulation should not be read to include personal data ***revealing*** that certain data was *collected* from a known child. The same could be said about "genetic or biometric data that may be processed for the purpose of uniquely identifying an individual." The genetic or biometric data is itself sensitive, but not data *revealing* that it may be *processed* …." (or intended to be used for the purpose of uniquely identifying an individual[4]).

- **N.J.A.C. 13:45L-2.3(a): For changes to a privacy notice, modify language to note that material changes "*may*" include ….**

N.J.A.C. 13:45L-2.3(a) provides a non-exhaustive list of material changes that will trigger the notice requirement. We suggest clarifying that the examples in this section are illustrative rather than prescriptive—by adding the word "may" before "include"—thereby enabling flexibility in situations where the specified changes are not material, as materiality is fact- and context-specific. This approach would help prevent consumers from being overwhelmed with constant notifications of updates.

Moreover, we seek clarification on the example pertaining to "the act of or policies concerning the sharing of personal data with third parties" listed under N.J.A.C. 13:45L-2.3(a)(4). As written, it is unclear what sorts of "acts" or "policies" would fall within scope.

- **N.J.A.C. 13:45L-3.6; N.J.A.C. 13:45L-6.3(b)(6): In the context of deletion obligations, replace "immediately" with "as soon as practicable."**

"Immediately" is not always a reasonable standard given that data can be stored across various systems, including archived ones. The requirement for immediate deletion would be particularly

---

[3] N.J. Rev. Stat. § 56:8-166.4: "'Sale' means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party."

[4] See our comments below about modifying the definition of "sensitive data" to clarify that "genetic or biometric data" must be *used or intended to be used* for the purpose of uniquely identifying an individual.

challenging for organizations, especially where, as here, the definition for "delete" calls for removal from "existing systems," which includes "archived or nonactive systems or systems maintained by processors." See N.J.A.C. 13:45L-1.2. Deletion from backups is particularly challenging, as data may persist until overwritten, depending on each controller's circumstances, retention policies, and available technical solutions.

- **N.J.A.C. 13:45L-6.3(b): Modify data inventory documentation requirements.**

N.J.A.C. 13:45L-6.3(b)(2) requires controllers to "create, establish, update, and maintain a data storage inventory documenting the types of data that the controller possesses, ***where*** the data is stored, and ***who*** has access to the data." (Emphasis added). This data inventory requirement presents data security concerns and goes beyond similar requirements under existing data protection laws. While some comprehensive privacy laws require documentation of the categories of personal data, they do not require such specific inventory as to document ***where data is stored*** and ***who has access***.

More generally, the proposed regulation would create records of processing requirements not tied to the risk of the processing (which is separately covered by DPIAs). This will significantly increase business compliance costs, as the proposed rule would mandate prescriptive documentation efforts for each type of processing activity.

This section also appears to regulate the substance of requirements that are otherwise addressed in other sections of the rule, which will create compliance confusion. For example, subsection (b)(6) requires *immediate* deletion of sensitive data after consent is withdrawn, but Section 13:45L-7.6(e) allows for 15 days.

CIPL suggests deleting subsection (b) in its entirety.

- **N.J.A.C. 13:45L-7.4: Simplify requirements relating to consumers under the age of 13**

N.J.A.C. 13:45L-7(f) permits a controller to satisfy the requirements of this section by following regulatory guidelines "that have been approved by the Federal Trade Commission in accordance with 16 CFR 312.11 and 15 U.S.C. § 6503." Those specific regulatory and statutory references, however, could be updated or changed by Congress and/or the FTC. To avert any potential conflict with these specific references, we suggest including language that says that complying with the notice and consent requirements under COPPA are sufficient for purposes of New Jersey.

- **N.J.A.C. 13:45L-8.1(b): Take a less prescriptive approach to the requirements of data protection assessments.**

N.J.A.C. 13:45L-8.1(b) lists the minimum content requirements for data protection assessments, which include disclosing relevant internal actors and external parties contributing to the data protection assessment. These requirements are quite prescriptive compared to many other state privacy laws and could force organizations operating across multiple states to develop standalone data protection assessments for New Jersey, resulting in duplicative processes and inefficient use of resources and time that could instead be devoted to putting in place meaningful privacy protections. We suggest the following edits:

> (b) A data protection assessment shall include ~~the following information:~~
>
> ~~1. A~~ a summary of the processing activity that takes into account information such as:
>
> ~~2.~~ 1. The categories of personal data to be processed ….

Moreover, we encourage the Division to add:

> *"If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section."*
>
> *"A controller may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy."*

II. ARTIFICIAL INTELLIGENCE

Generative AI ("GenAI") tools have recently become available for broad public use and have been adopted by individuals and organizations around the world. GenAI systems are trained on vast amounts of data to achieve a variety of purposes. From these large and diverse datasets, GenAI models can recognize statistical relationships between words and other data—such as images, videos, and audio—and make probabilistic predictions that generate useful outputs.

Evaluating the use of personal data in GenAI development requires careful contextual and risk-based analysis. For example, model developers often use personal data in training datasets to address potential algorithmic biases. To ensure proper model functioning and reduce the potential for unintended harms, lawmakers and regulators should avoid overly restrictive and broad requirements that exclude the use of personal data from datasets used for GenAI model development. They should also ensure that lower-risk AI systems are able to use personal data in a manner that enables development and deployment of societally beneficial technologies and use cases.

To advance these goals, we recommend the following changes to the regulations:

- **N.J.A.C. 13:45L-1.3(d): Permit use of personal data to train artificial intelligence models without the need for affirmative consent.**

  As proposed, N.J.A.C. 13:45L-1.3(d)(1) allows for the processing of personal data to conduct **internal research** to develop, improve, or repair products, services or technology. However, data used to train artificial intelligence shall not be considered to be for the purpose of internal research "unless the consumer has affirmatively consented to such use." N.J.A.C. 13:45L-1.3(d)(1)(ii).

  Given that many model developers use personal data to train GenAI systems to reduce the risk of biased outputs and otherwise improve the functionality and quality of models, the collection and use of such data should be recognized as a critical part of an organization's internal research to develop, improve, or repair products, services, or technology and not be hampered by an affirmative consent requirement.[5]

[5] See CIPL Discussion Paper – Applying Data Protection to Generative AI: Practical Approaches for Organization and Regulators (December 6, 2024), available at

The proposed limitations placed on internal research also limit the ability to create or access legitimate non-personal data or synthetic data that are critical to developing accurate and privacy-protecting AI tools. Access to good quality data is critical to the development of good quality AI technologies that are privacy-protective. The language within the draft rules broadly restricts both the legitimate uses of personal data and non-personal data in internal research. The language also broadly restricts instances where "[t]he data or *resulting research* is used to train artificial intelligence." (Emphasis added.) The provision fails to recognize that such "resulting research" will in most cases *exclude* personal data, given that the scope of data used in training AI often includes aggregated or deidentified data, or publicly available information which is excluded from the Act's scope of personal data. "Resulting research" may also include synthetic data, which is important in enabling privacy protection when developing AI tools in scenarios where personal data is inaccessible or unlawful.

The draft rules require companies to disclose whether a "system has been evaluated for accuracy, fairness, or bias (see N.J.A.C. 13:45L-2.2(b)(5)). However, synthetic data resulting from internal research is often required particularly to conduct bias testing, given that sensitive personal information such as race, national origin, and other key data are unavailable. Companies will also be limited as to the scope of data they can use to train AI if even "resulting data" must be excluded, which will stifle the development of more robust and accurate tools, which in turn does not protect consumers from harms such as inaccuracies and bias.

GenAI models are intended to be deployed for a wide range of applications, and many of these applications will be unknown at the time of development. Organizations should be provided with a certain degree of flexibility when it comes to purpose specification so they have room to explore the development of innovative applications. Furthermore, GenAI model training cannot be seen as a singular, unrepeating stage, as developers may need to collect, retain, and use data beyond the initial training to continue to improve the technology. A consent requirement in this context potentially puts organizations in the difficult position of excluding personal data from training datasets to the detriment of the performance of the model where such consent is not obtainable, for example.[6] Therefore, lawmakers should enable the use of personal data for the purpose of training of AI models as a part of the internal research process as long as other accountability measures and safeguards are sufficiently in place.

- **N.J.A.C. 13:45L-1.2: Remove reference to "automated or algorithmic decisions" from definition of "decisions that produce legal or similarly significant effects concerning the consumer"**

N.J.A.C. 13:45L-1.2 defines "decisions that produce legal or similarly significant effects concerning the consumer" to include "automated or algorithmic decisions." The reference to "automated or algorithmic decisions" could be interpreted as rendering any form of automated profiling and any form of processing by automated means as producing "legal or similarly significant effects" and therefore should be removed. Any automated or algorithmic decisions that do produce legal or similarly significant effects would already be included by the other elements of the definition.

---

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf.

6 *Id*.

- **N.J.A.C. 13:45L-1.2: Remove "scraping of personal data" from the exclusions under publicly available information.**

The proposed regulations exclude "publicly available information" from the definition of personal data, so the processing of publicly available information is not within the scope of the regulations. However, the regulations specify that "publicly available information" does not include "the scraping of personal data." The exclusion of scraped data thus brings public information collected by search engines and other companies that index such information within the scope of the regulations.

The scraping of publicly available information is a common practice for AI developers to gather the large and diverse datasets necessary to train GenAI models so that they generate reliable and fair results. Publicly available personal data on the Internet is therefore critical to the functioning of many AI models. The Division can mitigate potential risks from the use of publicly available information scraped from the Internet by requiring that scraping be done in a responsible way, with the establishment of appropriate guardrails to respect data minimization and accountable processing principles. Responsible web scraping of personal data goes hand in hand with proper limitations to ensure data minimization and accountable processing.[7]

III. BIOMETRIC DATA

The definition of "biometric data" **as formatted** in the rules creates an unintended expansion of the definition found in the NJDPA. Although the wording largely tracks the wording found in the statute, N.J.A.C. 13:45L-1.2 enumerates a list of seven physical characteristics—fingerprint, voiceprint, eye retinas, irises, facial mapping, facial geometry, or facial templates—but the numbering of those characteristics separates them from the purpose limitation language (found in the catchall clause under heading #8) that such data must be **used for the purpose of identifying a specific individual**. As formatted, the purpose limitation does not apply to the seven characteristics listed prior to the catchall, but only to the catchall, i.e., "other unique biological, physical, or behavioral patterns or characteristics."

CIPL believes that regulations pertaining to biometric data should address the purposes, uses, applications, and capabilities of biometric-based technologies rather than solely the underlying nature of the data. A risk-based approach ensures that low-risk applications of biometric technology, especially those with societal and economic benefits, can be deployed without undue restraints, and that higher or high-risk applications be deployed with appropriate protections and mitigation measures. This approach also encourages the use of risk mitigation measures that are proportionate and tailored to the specific use case, requiring more rigorous safeguards for uses posing greater risks.

[7] For more discussion of responsible approaches to web scraping, see CIPL, Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators (December 6, 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_genai_dec24.pdf.

Significant regulatory oversight should be reserved for high-risk uses where alternative effective safeguards are not available.[8]

- **N.J.A.C. 13:45L-1.2: Modify definition of "biometric data" to ensure that uses of such data relate to the identification of a specific individual.**

To ensure that the purpose limitation found in the catchall provision applies to **all of the listed examples** of biometric identifiers, we propose modifying the definition to say:

> *"Biometric data" means data generated by automatic or technological processing, measurements, or analysis of an individual's biological, physical, or behavioral characteristics, that are used, or intended to be used, singularly or in combination with each other or with other personal data, to identify a specific individual including, but not limited to…*

This change would ensure that the definition of "biometric data" is consistent not only with the NJDPA, but also with other state, federal, and international definitions of "biometric data."

- **N.J.A.C. 13:45L-1.2: Modify carve-out to definition of "biometric data"**

Remove the sentence formatted with ~~strikethrough~~ from the current carve-out to the definition of "biometric data":

> "Biometric data" shall not include: a digital or physical photograph; an audio or video recording; or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual. ~~Data generated from a digital or physical photograph, or an audio or video recording, is generated to identify a specific individual if the generated data relates to a specific individual's biological, physical, or behavioral characteristics.~~

This sentence could be interpreted to lower the threshold for defining "biometric data" from data that identifies a specific individual to data that ***relates*** to a specific individual.

- **N.J.A.C. 13:45L-1.2: Modify definition of "sensitive data" to clarify that "genetic or biometric data" must be used or intended to be used for the purpose of uniquely identifying an individual.**

As currently drafted, "sensitive data" is defined as including "genetic or biometric data that ***may be processed*** for the purpose of uniquely identifying an individual." To align with our suggested modification of the definition of "biometric data," we suggest that the "sensitive data" definition be modified to say "genetic or biometric data that ***is used or intended to be used*** for the purpose of uniquely identifying an individual."

- **N.J.A.C. 13:45L-6.3(b)(5): Modify requirement for documentation of biometric identifiers.**

N.J.A.C. 13:45L-6.3(b)(5) requires controllers to assess annually "whether biometric identifiers, photographs depicting one or more persons, audio or voice recordings containing the voice of one or more persons, or any personal data generated from a photograph or an audio or video recording

---

[8] CIPL White Paper – Enabling Beneficial and Safe uses of Biometric Technology Through Risk-Based Regulations (April 24, 2024), available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_safe_and_effective_biometric_tech_april_24.pdf.

held by a controller is still necessary for the specific processing purpose, and document such assessment."

This provision, as drafted, does not limit the assessment to biometric data that is used for purposes of identifying a specific individual. Without such a qualifier, the provision creates an unnecessary compliance burden for companies, requiring that they assess and report even low-risk processing of biometric data. This provision is also inconsistent with the stated definition of "biometric data," which does not include "a digital of physical photograph; an audio or video recording; or any data generated from a digital or physical photograph, or an audio or video recording, ***unless such data is generated to identify a specific individual."***

IV. CONSUMER REQUESTS AND DISCLOSURES

- **N.J.A.C. 13:45L-1.4(a)(5), -1.5(a)(5), and -2.4(c): Add a reasonableness or feasibility limitation to the requirements for user-interface design.**

N.J.A.C. 13:45L-1.4(a)(5) requires that all consumer communications be provided "in a readable format on all devices through which consumers normally or regularly interact with the controller, including on smaller screens and through mobile applications, if applicable[.]"

N.J.A.C. 13:45L-1.5(a)(5) requires controllers to design and implement methods for submitting data right requests and obtaining consent via methods that are easy to execute, expressly prohibiting methods that would require a consumer "to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting an opt-out request[.]"

N.J.A.C. 13:45L-2.4(c) requires controllers to provide a notice of the right to opt out that includes, inter alia, "the interactive form by which the consumer can opt out" if the notice is provided online.

As proposed, design-based requirements such as these may be technically challenging for organizations to implement while creating little benefit for consumers. CIPL suggests adding language such as "if reasonable or feasible" to give organizations flexibility to determine how best to ensure the visibility of notices and mechanisms for data rights requests across a range of devices.

- **N.J.A.C. 13:45L-1.4(b): Recast accessibility requirements to ensure reasonable compliance.**

Proposed rule N.J.A.C. 13:45L-1.4(b) requires a controller to "***follow*** *generally recognized industry standards*" when providing notifications and other communications online. Given that accessibility issues are already addressed by laws such as the Americans with Disabilities Act, the regulation should be recast to require controllers to ***"ensure reasonable compliance with applicable accessibility laws and/or*** *generally recognized industry standards* …."

- **N.J.A.C. 13:45L-1.5: Add exception to consent requirement**

The proposed rules should also incorporate language reaffirming that controllers are not required to obtain consent when the collection, use, or retention of personal data is essential to provide the service the consumer requests, for statistical purposes about the use of the controller's service, or to adapt functions in line with the consumer's preferences. Non-exhaustive examples include retaining the consumer's language preferences, such as those chosen on a multilingual website, understanding how the consumer accesses the controller's service (e.g. device types and browser or operating system versions), or A/B testing.

- **N.J.A.C. 13:45L-2.2(a)(3): Modify privacy notice requirements to specify the criteria used to determine how long data will be retained, rather than the "length of time" it will be kept.**

N.J.A.C. 13:45L-2.2(a)(3) requires the controller to specify the "length of time" the controller intends to retain each category of personal data that the controller processes. Rather than requiring the controller to specify a length of time, we suggest modifying the language to specify "*the criteria used to determine the period of time it will be retained*." This language would provide controllers flexibility for instances where they may not know with certainty how long they will retain the data.

- **N.J.A.C. 13:45L-2.2(a)(4), (5): Provide definition for the term "share" to avoid ambiguity.**

N.J.A.C. 13:45L-2.2(a) requires a privacy notice to include a statement regarding whether personal data will be "shared with third parties" (subsection 2.2(a)(4)) or whether the controller knowingly "shares the personal data of consumers under 16 years of age" (subsection 2.2(a)(5)). CIPL recommends the Division to define the term "share."

- **N.J.A.C. 13:45L-2.2(b)(5): Delete requirement to disclose the outcome of evaluations for "accuracy, fairness, and bias."**

N.J.A.C. 13:45L-2.2(b)(5) requires a controller who processes personal data for profiling to disclose the results of an evaluation of a system "if the system has been evaluated for accuracy, fairness, or bias." This obligation does not appear to be included in the notice obligations of the NJDPA. Although the obligation does not appear to be mandatory given that the disclosure is required "if" evaluation has taken place, the failure to make such a disclosure would give the impression that an organization has not evaluated its systems in contravention of a rule that does not appear to be in line with the statute. Furthermore, N.J.A.C. 13:45L-8.1 already sets forth detailed obligations for completion of a data protection impact assessment, which is required for processing that presents a "heightened risk of harm," which includes profiling in furtherance of decisions that produce legal or similarly significant effects.

- **N.J.A.C. 13:45L-3.1(f): Modify requirements pertaining to non-standard methods of exercising rights.**

If a consumer seeks to exercise a data right using a method that is not one of the controller's designated methods, N.J.A.C. 13:45L-3.1(f) requires a controller to treat the attempt "as if it had been attempted in accordance with the controller's designated method." CIPL cautions the Division against creating a de facto incentive that consumers can lodge complaints through any available channel, potentially including non-privacy-related resources. This raises uncertainty for the controllers when managing individual requests outside of those methods designated for submitting privacy requests.

- **N.J.A.C. 13:45L-3.1(g): Allow children as well as adults to make data rights requests.**

As proposed, this element is more restrictive than many other jurisdictions, which grant children the ability to exercise data subject rights on their own, in addition to granting parents the ability to do so on their children's behalf.

- **N.J.A.C. 13:45L-3.2: Clarify that UOOM does not apply to profiling.**

The NJDPA limits the universal opt-out mechanism (UOOM) to targeted ads and the sale of data.[9] From a substantive perspective, the nature of the risk associated with profiling varies by use case, and subjecting profiling to the universal opt-out mandate could create situations where consumers would opt-out to avoid certain high-risk use cases while simultaneously and inadvertently blocking beneficial, low-risk use cases.

- **N.J.A.C. 13:45L-3.2(d)(3): Remove reference to sharing of data in the context of the opt-out link.**

For controllers that provide an opt-out link pursuant to N.J.A.C. 13:45L-3.2(c), subsection (d)(3) requires such controllers to provide "a clear understanding of its purpose, for example … "Do Not Sell ***or Share*** My Personal Data …." However, the NJDPA grants consumers the right to opt out only of "the processing of personal data for the purposes of (a) targeted advertising; (b) the **sale** of personal data; or (c) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."[10] As there is no right to opt out of ***sharing*** personal data, the reference to *sharing* should be removed.

- **N.J.A.C. 13:45L-3.4(a)(4): Strike obligation to forward opt-out requests to third parties.**

When a consumer exercises the right to opt out, N.J.A.C. 13:45L-3.4(a)(4) requires controllers to "notify all third parties to whom the controller has sold or with whom the controller has shared the consumer's personal data of the consumer's choice to opt out and direct them to comply with the consumer's choice and forward the request to any other person to whom the third party has made the personal data available during that time period." Automatic flow-down of the opt-out request to third parties may not be aligned with users' intent in all circumstances.

N.J.A.C. 13:45L-3.7(c): Strike requirement to notify consumer of compliance.

N.J.A.C. 13:45L-3.7(c) requires a controller to inform the consumer whether it has complied with the consumer's deletion request. The proposed language is similar to a Florida requirement that has already proven difficult to implement. It is unclear what level of deletion must be achieved to reasonably be able to tell the consumer the controller has "complied" with their deletion request. For example, must a controller simply notify the consumer that the request was received and processed, or must the controller have a high level of certainty that the individual's information was actually deleted across the entire company? New Jersey's proposed text goes beyond the obligation in Florida because it requires the controller to tell the consumer about the minimum data kept to comply with the deletion request. This is likely to spur consumer confusion.

- **N.J.A.C. 13:45L-4.3(c)(1): Modify OOPS requirement related to browsers and devices.**

N.J.A.C. 13:45L-5.1(c)(1) requires a controller "treat the opt-out preference signal [OOPS} as a valid choice to opt out of the processing of personal data for purposes of targeted advertising, sale of personal data, or both, as indicated by the universal opt-out mechanism, ***for the associated***

---

[9] N.J. Rev. Stat. § 56:8-166.11(b)(1): "Beginning not later than six months following the effective date of P.L. 2023, c. 266 (C.56:8-166.4 et seq.), a controller that processes personal data for purposes of targeted advertising, or the sale of personal data shall allow consumers to exercise the right to opt out of such processing through a user-selected universal opt-out mechanism."

[10] N.J. Rev. Stat. § 56:8-166.10(a)(5).

browser, network, or device(s), and any consumer profile associated with that browser, network, or device(s), including pseudonymous profiles."

CIPL notes that this requirement could prove technically difficult to implement, e.g., with respect to verification. If preserved, CIPL suggests rewording and limiting the bolded language as follows: ***"for the associated browser session or device, and if known, the consumer."*** Such a change would avoid triggering an opt out for the profiles of all consumers that may use the device. In addition, such language would better respect consumer choice by applying the opt out only to the consumer who has requested the opt out.

- **N.J.A.C. 13:45L-5.1(c)(4): Do not apply OOPS to loyalty programs.**

The regulations should not extend the OOPS to cover participation in a loyalty program. Unlike targeted ads or the sale of data, a consumer must ***enroll*** in a loyalty program. That affirmative step should supersede the impact of an OOPS, which a consumer may enable without considering its impact on a specific program that benefits the consumer. For instance, a consumer who wants to turn off targeted ads may inadvertently disable a pharmacy or grocery store program and delete their accumulated coupons. This is even more likely since other state privacy laws do not extend OOPS to such programs. New Jersey would therefore be an outlier in this regard, increasing consumer confusion.

- **N.J.A.C. 13:45L-5.2(a)(7): Modify phrasing of default settings in technical specification.**

N.J.A.C. 13:45L-5.2(a)(7) provides that a UOOM must not make use of a default setting that **opts a consumer *into* the processing** of personal data for purposes of targeted advertising or sale of personal data. We suggest alignment with the language from other states, i.e., a prohibition of opt-out signals that by default do not reflect a clear consumer intent to opt-out.

- **N.J.A.C. 13:45L-5.2(b): Permit UOOMs approved by other state AGs.**

N.J.A.C. 13:45L-5.2(b) provides that a UOOM signal "must be in a format commonly used and recognized by controllers." CIPL suggests adding a reference to lists of UOOMs recognized by sister states (like Colorado).

- **N.J.A.C. 13:45L-6.1(d): Modify purpose specification requirements to delete unnecessary detail.**

When personal data is collected and processed for more than one purpose, **the opening sentence** of N.J.A.C. 13:45L-6.1(d) requires a controller to **specify each purpose with enough detail to allow consumers to understand each purpose**. The express prohibitions outlined in the text that follows—*"A controller shall not: 1. Identify one broad purpose to justify numerous processing activities; 2. Specify one broad purpose to cover potential future processing activities; or 3. Specify so many purposes for which personal data could potentially be processed that the purpose or purposes becomes unclear or uninformative"*—**are unnecessary**, given the directive already set out in the opening sentence of subsection (d), as well as the directive in subsection (c): *"A controller must disclose and describe the purpose or purposes for which personal data is processed in a level of detail that enables consumers to understand how each category of their personal data is used."*

- **N.J.A.C. 13:45L-6.3(b)(4): Remove requirement to document the deletion of personal data that is no longer necessary for the specific processing purpose(s).**

The consumer deletion right described under 13:45L-3.7 sets out detailed requirements for controllers (and processors based on controllers' instructions) to delete consumer personal data. The data minimization rule under 3:45L-6.3(b)(4) additionally requires controllers to document their efforts "to delete any personal data that is no longer necessary for the specific processing purpose or purposes."

The data minimization provision is inconsistent with the requirements of NJDPA, which requires a controller to "limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, *as disclosed to the consumer*." N.J. Stat. §56:8-166.12 (emphasis added).

If a consumer has not requested deletion of personal data, and processing of such data is otherwise relevant and reasonably necessary for processing purposes as disclosed to the consumer, there should be no further requirement to delete such data.