September 2, 2025

By Electronic Mail

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

RE: Public Comment on New Jersey Data Privacy Law Rulemaking

To Whom It May Concern:

The Entertainment Software Association ("ESA") submits these comments regarding the rules proposed by the New Jersey Division of Consumer Affairs (the "Division") implementing the New Jersey Data Privacy Act (the "Act").[1]

ESA is the U.S. trade association for the video game industry. Our members are the innovators, creators, publishers, and business leaders reimagining entertainment and transforming how America plays video games on consoles, handheld devices, and personal computers. With over 120 video game companies in the state of New Jersey and an economic impact of more than $300 million in the state,[2] ESA's members support the statutory goals of promoting the privacy and security of consumers' personal data. ESA urges the Division, however, to make the following revisions to the Proposed Rules to help ensure the rules are consistent with the statutory text and focus on concrete, rather than speculative, consumer harms:

- **Align the Proposed Rules with the language of the Act by eliminating provisions that are unsupported by or conflict with the statutory text;**
- **Harmonize the Proposed Rules with existing U.S. state privacy laws to promote a rational legal framework that facilitates compliance; and**
- **Eliminate vague provisions that provide no meaningful benefits to consumers.**

These points are discussed further in Sections I through III below.

* * *

[1] 57 N.J.R. § 1101(a) (June 2, 2025) (hereinafter "Proposed Rules").

[2] Entertainment Software Association, *Impact of the Video Game Industry*, New Jersey, https://www.theesa.com/video-game-impact-map/state/new-jersey.

I. THE PROPOSED RULES MUST BE REVISED TO AVOID INCONSISTENCIES AND OVERREACH WITH THE TEXT OF THE ACT.

The Proposed Rules diverge from the language of the Act in multiple respects, exceeding the Division's rulemaking authority.

A. Aggregated Data Must Be Excluded from the Definition of "Personal Data" to Avoid Conflicts with the Act.

The Proposed Rules stipulate that "[p]ersonal data is 'reasonably linkable' if it can identify a person or a device linked to a person *when aggregated with other data*."[3] This provision creates ambiguity by suggesting that aggregated data can be personal data. An interpretation treating aggregated data as "personal data" would be inconsistent with the statutory text, which excludes de-identified data from the definition of "personal data." Aggregated data, such as the statistic that 28% of video game players in the U.S. are age 50 or older,[4] cannot identify a specific person and is therefore de-identified data excluded from the definition of "personal data." If the Proposed Rules are intended to address the concept of *combining* (as opposed to *aggregating*) data, then this should be clarified in the Proposed Rules.

In addition, the Proposed Rules must be clarified to state that data will be "reasonably linkable" only if the combined data can *reasonably* identify a person or device linked to a person. Treating information as personal data where someone using unreasonable methods could theoretically identify a person or device inappropriately ignores the "reasonably" in "reasonably linkable."

The definition of "personal data" also conflicts with the Act's stipulation that "[n]othing in [the Act] shall require a controller to . . . re-identify de-identified data" or "collect, retain, use, link, or combine personal data concerning a consumer that it would not otherwise collect, retain, use, link, or combine in the ordinary course of business."[5] For example, information that *theoretically could be* linked with other information to identify an individual but that the business *does not* link or combine in the ordinary course of business cannot be "personal data" with respect to that business because such an interpretation would require the controller to re-identify or otherwise link or combine data in order to comply with the Act's requirements, in conflict with the statutory text.

To align the Proposed Rules with the language of the Act, the Division should eliminate the reference to aggregated data in the definition of "personal data" and re-iterate the statute's language that controllers are not required to re-identify de-identified data or otherwise link or combine personal data that it would not otherwise link or combine in the ordinary course of business.

---

[3] Proposed Rules § 13:45L-1.2 (emphasis added).

[4] *See* ESA, *Essential Facts*, https://www.theesa.com/resources/essential-facts-about-the-us-video-game-industry/2025-data.

[5] N.J. Stat. Ann. § 56:8-166.14.

B. The Proposed Requirements for "Valid Consent" Clash with the Language of the Act.

The statute defines "consent" in clear, unambiguous language, and it does not grant the Division rulemaking authority to expand or otherwise alter this definition. As a result, it is concerning that the Proposed Rules go beyond this statutory text by imposing additional, prescriptive conditions in order for consent to be valid. To avoid this overreach, the Division must eliminate all additional conditions and instead incorporate and defer to the statutory definition of "consent." For example:

- The Proposed Rules provide that consent is invalid if "[t]he controller denies goods, services, discounts, or promotions to a consumer who chooses not to provide consent," except where the personal data "is necessary" to the provision of the goods or a loyalty program.[6] Not only is this limitation absent from the statutory text, but also it conflicts with language in the Act providing that controllers may "provide different services to consumers that are reasonably related to the value of the relevant data" depending on whether a user opts out of processing, subject to making certain disclosures.[7]

- The Proposed Rules require granular, purpose-by-purpose consent for processing purposes that are "not reasonably necessary to one another."[8] Again, this restriction does not appear anywhere in the Act, and imposing such a prescriptive requirement is likely to confuse and overwhelm consumers.

- The Proposed Rules require that if a consumer has not interacted with a controller in the prior 24 months, the controller must "refresh" consent to continue processing the consumer's personal data in certain contexts. This requirement is inconsistent with the statutory text, which treats consent as valid unless and until it is withdrawn by the consumer.[9] Had the legislature intended to have consent expire after a specified time, it would have so stated.[10] With respect to personal data concerning a known child, the requirement also is inconsistent with the Act's directive that obtaining consent "in accordance with COPPA" is sufficient, because verifiable parental consent under COPPA does not expire unless and until it is withdrawn.[11]

---

[6] Proposed Rules § 13:45L-7.2(a)(2)(iii).

[7] N.J. Stat. Ann. § 56:8-166.8.

[8] Proposed Rules § 13:45L-7.2(a)(3)(i).

[9] *See* N.J. Stat. Ann. § 56:8-166.12(6).

[10] *Compare with* Video Privacy Protection Act, 18 U.S.C § 2710(b)(2)(B)(ii)(II) (specifying that "informed, written consent" may be given "at the time the disclosure is sought" or "in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner").

[11] *See* Proposed Rules § 13:45L-7.7(a); N.J. Stat. Ann. § 56:8-166.12(a)(4).

- The Proposed Rules include a section on consent for "consumers under the age of 13" that mischaracterizes the COPPA statute and the COPPA Rule's provisions in important respects.[12] For example, the proposed text does not incorporate recently adopted amendments to the COPPA Rule and restates only select portions of the applicable COPPA language.[13] This creates unnecessary confusion and inconsistency with the Act's statement that processing personal data from children consistent with COPPA satisfies the Act's requirements. ESA urges the Division to strike section 13:45L-7.4 of the Proposed Rules and instead rely on the existing cross-reference to COPPA's requirements under the Act, which would eliminate this confusion.[14]

Moreover, the additional conditions imposed by the Proposed Rules create practical challenges that could have unintended consequences for consumers. For example, a prohibition on further processing unless a consumer refreshes their consent every two years imposes a substantial and undue burden on consumers, who might lose access to products, services, and features they requested (some of which they might have even paid for) simply because they did not refresh their consent in time. In addition, the provision could have the unintended consequence of requiring controllers to collect and maintain more personal data than they otherwise would in order to determine whether consent must be refreshed and to seek such consent. Because the provision contemplates that the consumer has become inactive on the service, the controller will need to collect and maintain contact information, such as email, phone number, or direct mailing address, to be able to communicate with the consumer outside the service to inform them that their consent is about to expire and request that they update consent. A video game company might not otherwise collect and maintain this information if, for instance, they communicate with the consumer primarily through the player's account within the game.

For these reasons, the Division should remove all provisions imposing additional conditions for consent to be valid and, instead, defer to the statutory text.

C. The Proposed Limitation on Training AI Models Exceeds the Statutory Authority and Would Harm Innovation.

The Act expressly and unequivocally states that the statute shall not be interpreted to restrict a controller's ability to "collect, use, or retain data for internal use to . . . conduct internal research to develop, improve, or repair products, services, or technology."[15] Notwithstanding this clear directive, the Proposed Rules would require affirmative consumer consent in order to

---

[12] *See* Proposed Rules § 13:45L-7.4.

[13] *See* 90 Fed. Reg. 16918, 16951 (Apr. 22, 2025), *codified at* 16 CFR § 312.5(b)(2)(ii) (striking "monetary" from the COPPA Rule's prior provision permitting an operator to obtain verifiable parental consent by "[r]equiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder").

[14] *See* Proposed Rules § 13:45L-7.4(c)(2).

[15] N.J. Stat. Ann. § 56:8-166.15(b)(1).

collect, use, or retain data used to train AI under the internal research exception. This restriction, which is arbitrary and capricious and in direct conflict with the statute, must be removed.[16]

This unsupported narrowing of the internal research exemption is particularly concerning given that the Act does not even mention "AI," much less provide the Division any authority to regulate this specific technology. Moreover, neither the Act nor the Proposed Rules define "AI," creating uncertainty about when, specifically, affirmative consent would be required. It is not at all clear how revoking consent could work in the context of AI models, where information often cannot be removed from a model after it has been used to train the model.

The proposed limitation also would significantly disrupt AI-related innovation in the video gaming industry with serious consequences for consumers. For example, video game companies may use AI models to create in-game dialogue or to personalize the difficulty level of a game to the player's capabilities. The use of gameplay data to train such models does not pose any meaningful risks to consumers' privacy or security and yields significant consumer benefits by making game experiences richer. Many video game companies also use AI to perform content moderation and detect and prevent fraud and abuse by players. The Proposed Rules would have the effect of cutting off access to training data used to develop and maintain these systems — particularly because bad actors are unlikely to consent to the use of their data for model training. To align with the statute and avoid these adverse outcomes, the Division should eliminate the Proposed Rules' AI carveout to the statute's unlimited internal research exemption.

D. The Requirement to Pass Deletion Requests on to Third Parties Is Inconsistent with the Statute and Should Be Removed.

The Proposed Rules create an entirely new requirement to pass deletion requests on to third parties that has no basis in the Act's text and should therefore be removed. The Proposed Rules state that when a consumer exercises the right to delete, the controller "shall . . . [n]otify all third parties to whom the controller has sold or with whom the controller has shared the consumer's personal data of the need to delete the consumer's personal data."[17] While some other state comprehensive privacy laws require certain consumer requests to be passed through to third parties, this requirement is generally limited to only specific types of sharing, such as sharing for cross-context behavioral advertising.[18] Accordingly, the Proposed Rules would greatly expand the scope of such a requirement to pass on deletion requests to third parties, with no basis in the Act's text, and this provision should be removed.

E. Consistent with the Act, the Requirements for Correction Requests Should Allow Controllers to Protect against Fraudulent Requests.

As drafted, the Proposed Rules provide controllers with only a limited ability to defend against fraudulent correction requests by allowing controllers to require a consumer to provide documentation to support the request only if the controller has a good faith, reasonable, and

[16] Proposed Rules § 13:45L-1.3(d)(1)(ii).

[17] *See id.* § 13:45L-3.7(a)(3).

[18] Cal. Code Regs. tit. 11, § 7022(b)(3).

documented belief that the correction is not accurate.[19] However, the Act explicitly provides that it should not be construed as restricting a controller's ability to "prevent, detect, protect against . . . fraud, harassment, malicious or deceptive activities, or any illegal activity. . . ."[20] Consistent with this mandate, the Proposed Rules should explicitly acknowledge that controllers have additional flexibility in defending against fraudulent or abusive correction requests.

In the experience of ESA's members, fraudsters and other bad actors can abuse correction rights to try to evade detection, gain unauthorized access to an account, or otherwise facilitate their unlawful or malicious conduct. For example, a video game player who has been banned from an online game for harassing other players or cheating in violation of the game's terms of use might attempt to request "correction" of their IP address, username, or other personal data in order to try to circumvent the game company's anti-fraud, anti-cheat, and other detection systems that prevent such players from attempting to create new accounts. Malicious actors may also exploit the correction right to aid in gaining unauthorized access to another user's account or regain access to an account the company had previously suspended under suspicion of fraud.

To discourage such efforts, in addition to allowing controllers to request supporting documentation when they have a good faith belief a correction request is not accurate, the Proposed Rules should also allow a controller to deny a correction request in order to prevent fraud when the controller has a good faith belief that the particular consumer is attempting to abuse the correction right for malicious purposes.

F. The Proposed Rules Introduce New Notice Obligations Related to Deletion Requests that Are Not Based in the Act.

The Proposed Rules improperly expand a controller's duties with respect to a deletion request by requiring controllers to (1) "inform the consumer whether it has complied with the consumer's [deletion] request," and (2) "inform the consumer whether it retained a record of the deletion request and the minimum data necessary to ensure the consumer's personal data that is lawfully obtained from a source other than the consumer remains deleted."[21] These new requirements should be eliminated as they have no basis in the Act and impose burdensome paperwork requirements and costs with no demonstrated consumer benefit.

The Act sets forth a clear and specific process that a controller must follow when responding to a deletion request.[22] Specifically, this process outlines the timeframes for response, requirements for justification in the case of denial, and the right to appeal. Nowhere does the Act require a controller to notify a consumer when a deletion request has been completed, let alone whether it retained a record of that request or the retention of certain data.

In addition to lacking a statutory basis, these novel requirements also introduce significant ambiguity. The requirement to inform the consumer whether the controller has "complied" with a deletion request is vague and lacks a workable standard. Determining whether

---

[19] *See* Proposed Rules § 13:45L-3.6(c).

[20] N.J. Stat. Ann. § 56:8-166.15(a)(9).

[21] Proposed Rules § 13:45L-3.7(c).

[22] N.J. Stat. Ann. § 56:8-166.7.

a deletion request has been "complied with" is inherently technical and context-specific, particularly for businesses managing backup storage or archived systems. Similarly, the proposed requirement to disclose whether the controller retained a record of the deletion request and the "minimum data necessary" to prevent reintroduction of deleted data is confusing. While the Act permits such minimal data retention for internal compliance purposes, the obligation to affirmatively disclose this information to consumers — without clear guidance on the form, scope, or content of such disclosure — would likely confuse consumers. For example, telling a consumer that her data has been deleted, but also that a subset of data has been retained, could undermine trust in the company's data management practices and risk creating unnecessary concern.

G. The Proposed Rules Improperly Expand the Scope of "Biometric Information" Beyond the Text of the Act.

The Proposed Rules would improperly expand the definition of regulated "biometric data" to include "[d]ata generated from a digital or physical photograph, or an audio or video recording, [that] is generated to identify a specific individual if the generated data relates to a specific individual's biological, physical, or behavioral characteristics."[23] This language deviates from the text of the Act.

First, the Act expressly excludes "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" from its definition of "biometric data."[24] Instead of aligning with the statute's mandate, the Proposed Rules stretch beyond the bounds of the Division's authority by introducing a new, vague, and overbroad standard, effectively scoping in *any* data that may relate to an individual's biological, physical, or behavioral characteristics (even if such data would not otherwise be considered biometric data). For example, in the video game context, a developer may allow users to create avatars by uploading a photograph, which the software would use to model features like hair color, eye color, or skin tone. Neither the Act nor any other state privacy law would consider this use case to involve biometric data.[25] However, it's unclear how this would be treated under the Proposed Rules, because the data used comes from a photograph that "relates to a specific individual's . . . physical . . . characteristics."

This misalignment is further compounded by the Proposed Rules' data minimization provisions, which would require controllers to "assess whether biometric identifiers, *photographs depicting one or more persons, audio or voice recordings containing the voice of one or more*

---

[23] Proposed Rule § 13:45L-1.1.

[24] N.J. Stat. Ann. § 56:8-166.4.

[25] *Id.* § 56:8-166.4 (defining "biometric data" to expressly exclude "any data generated from a digital or physical photograph or an audio or video recording"); 4 CCR 904-3 Rule 2.02 (substantially same); Del. Code 6 § 12D-102(3) (substantially same); Fla. Stat. § 501.702(4) (substantially same); Ind. Code Ann. § 24-15-2-4(b) (substantially same); Iowa Code Ann. § 715D.1(4) (substantially same); Mont. Code Ann. § 30-14-2801(2)(3)(b) (substantially same); OR SB 619 § 1(3)(b) (substantially same); Tenn. Code Ann. § 47-18-3201(3)(B) (substantially same); Tex. Bus. & Com. Code § 541.001.3 (substantially same); Utah Code Ann. § 13-61-101(6)(c) (substantially same); RCW § 19.375.010(1) (substantially same).

persons, or any personal data generated from a photograph or an audio or video recording held by a controller is still necessary for the specific processing purpose or purposes."[26] As explained above, photos, audio recordings, and video recordings are not biometric data under the Act, and including them in this context improperly suggests that the information should be subject to heightened compliance obligations notwithstanding the legislature's explicit directive to the contrary.

Accordingly, ESA urges the Division to revise the definition of "biometric data" as follows:

"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 revision brings the Proposed Rules in alignment with the Act, as well as other state comprehensive privacy laws.

H. The Proposed "Notice of Right to Opt Out" Requirements Lack a Basis in the Act and Create Practical Implementation Challenges.

The Proposed Rules require controllers to provide a separate "notice of right to opt out" presented "at or before the point of collection of personal data" that includes an explanation of the consumer's right to opt out of certain types of processing, as well as instructions on how to exercise that right.[27] This requirement contravenes the Act and must be removed.

The Act only references one notice that must be provided proactively to all consumers — the privacy notice.[28] Within this notice, a controller must provide a description of the consumer's rights — including the right to opt out of targeted advertising, the sale of personal data, and profiling in furtherance of significant decisions — along with clear information about how to exercise those rights. Nothing in the Act requires a real-time, point-of-collection disclosure solely focused on the opt-out right. Because the Proposed Rules require proactive opt-out notices that are in conflict with the statutory text, the notice of right to opt out provisions must be removed from the Proposed Regulations.

Moreover, the Proposed Rules are unclear as to how this new "notice of right to opt out" can be implemented. The Proposed Rule does not clarify whether a controller can satisfy the rule through a controller's privacy notice, or whether it must be presented as a distinct, standalone mechanism at each data collection point. In practice, a standalone notice mechanism would be difficult to implement. For example, video games often collect personal data across multiple channels and interfaces, such as during account creation and through multiplayer features. Requiring a separate opt-out notice at each of these collection points would interfere with the gameplay experience, degrade the user experience, and increase the

[26] Proposed Rules § 13:45L-6.3(a)(5) (emphasis added).

[27] *Id.* § 13:45L-2.4.

[28] *See* N.J. Stat. Ann. § 56:8-166.6.

risk of notice fatigue. It may also be technically infeasible to present such notices in fast-moving, immersive environments like online multiplayer games or virtual reality applications.

ESA urges the Division to remove this provision, in alignment with the Act. At a minimum, the final rule should clarify that controllers may satisfy this requirement through a privacy notice, which would ensure that consumers are informed in a meaningful and accessible manner while preserving flexibility for diverse business models and user experiences.

I. The Novel Requirement to Provide an Opt-Out After a Denial of a Deletion Request Lacks a Basis in the Act.

The Proposed Rules would require a controller that denies a consumer's deletion request — and continues to process the consumer's data for targeted advertising, sale, or profiling — to (1) ask the consumer whether they would like to opt out of such processing, and (2) provide the contents of, or a link to, the notice of the right to opt out. This is novel requirement that has no basis in the Act and is not seen in any other comprehensive privacy statute.

The Act already includes language explaining what a controller must do if it denies a consumer request. Specifically, if a controller declines to take action regarding the consumer's request, the controller must inform the consumer of "the justification for declining to take action and instructions for how to appeal the decision."[29] The Act does not require or even suggest that the controller must also offer the consumer an opportunity to opt out of certain processing activities as a condition of denying a deletion request. Thus, by attempting to impose this additional requirement, the Division exceeds its delegated authority and creates obligations not grounded in the statutory text. Accordingly, the Division must remove this language from the final rule.

II. THE PROPOSED RULES SHOULD BE HARMONIZED WITH EXISTING U.S. STATE COMPREHENSIVE PRIVACY FRAMEWORKS.

Some provisions of the Proposed Rules are significantly misaligned with requirements in other U.S. states' comprehensive privacy laws. A lack of harmonization around key provisions risks confusing consumers and creating unnecessary compliance burdens for controllers without providing consumers any meaningful additional benefits.

A. The Proposed Rules' Definition of Personal Data Is Out of Step with U.S. State Privacy Laws.

The Proposed Rules' expanded definition of personal data, discussed in greater detail above, is out of step with every other state comprehensive privacy law. While every other state comprehensive privacy law includes some version of the "reasonably linkable" qualifier in its definition of "personal data," no state's law interprets that qualifier as covering any data that theoretically "can identify a person or a device linked to a person when aggregated with other data." Several laws' definitions of personal data include pseudonymous data, but only insofar as it "*is used by a controller or processor* in conjunction with additional information that reasonably

[29] *Id.* § 56:8-166.7(e).

links the data to an identified or identifiable individual."[30] The definition in the Proposed Rules lacks this important qualification.

The Division should eliminate the overinclusive and unworkable proposed interpretation of the phrase "reasonably linkable." Retaining that interpretation would put the Act severely out of step with other state comprehensive privacy laws, creating substantial uncertainty regarding what qualifies as personal data.

B. Consistent with Other U.S. State Privacy Laws, the Proposed Rules Should Recognize a Broad Exemption for Trade Secrets.

To align with other state consumer privacy law frameworks, the Division should clarify the Proposed Rules to recognize broader protections for trade secrets in the form of a trade secret exemption to controller obligations.[31] Such an exemption would enable controllers to protect their legal rights without limiting the rights afforded to consumers under the Act. For example, the Act provides that if a controller declines to comply with a consumer's request, the controller must inform the consumer of the justification for declining to take action.[32] In the context of a deletion request by a video game player who has violated the controller's anti-cheat policy, disclosing that a controller could not comply by deleting certain information could risk disclosing trade secrets related to how the controller detects cheating behavior. As another example, the Act's privacy notice requirements should not require controllers to describe the "purpose for processing personal data"[33] in such detail that it would expose a trade secret — for example, by requiring a video game developer to disclose how personal data is processed to prevent players from cheating. This approach would protect controllers' trade secrets without compromising consumer rights, and it would align the Proposed Rules with other state consumer privacy laws.

C. The Deletion Requirements Are Impractical and Inconsistent with Other U.S. State Privacy Laws.

The Proposed Rules define "delete" in an unprecedented and expansive manner that will create compliance difficulties for controllers. Specifically, "delete" means "to remove data from *all existing systems*," which include "archived or nonactive systems."[34] Removing personal data from archived or nonactive systems imposes a significant burden on controllers due to cost and difficulty of taking personal data out of archived systems in order to effectuate data deletion. This burden comes without any added benefit to consumers, as personal data in archived or nonactive systems is unlikely to be accessed by the controller in the ordinary course of business and may in fact be more secure when remaining in the archive than when being taken out of the archive. Indeed, the California Consumer Privacy Act ("CCPA") regulations recognize this

---

[30] *See* Fla. Stat. § 501.702(19); Neb. Rev. Stat § 87-1102(20)(a); Tex. Bus. & Com. Code § 541.001(19) (emphasis added).

[31] *See, e.g.*, Cal. Civ. Code § 1798.100(f); Utah Code § 13-61-304(5); Fla. Stat. § 501.716(4); Tex. Bus. & Com. Code § 541.201(d); Iowa Code § 715D.7(9).

[32] *See* N.J. Stat. Ann. § 56:8-166.7(c).

[33] *See id.* § 56:8-166.6(a)(2).

[34] *See* Proposed Rules § 13:45L-1.2.

practical reality and exempt "archived or backup systems" from the requirement to completely and permanently delete personal data from "existing systems."[35] Relatedly, COPPA defines "delete" narrowly to mean removal of personal data "such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business."[36] These frameworks strike the appropriate balance between honoring consumer deletion rights and addressing the technical realities of archive and backup systems. ESA encourages the Division to adopt a similar approach to its deletion requirements.

Furthermore, to ease burdens on controllers without jeopardizing the safety of consumers' personal data, the Proposed Rules should explicitly confirm that anonymization, deidentification, or aggregation that renders data no longer "linked or reasonably linkable to an identified or identifiable person"[37] satisfies any deletion requirement. This would be consistent with the statutory text which recognizes that personal data "shall not include de-identified data"[38] or otherwise require controllers to link or combine data that is not otherwise linked or combined in the ordinary course of business.[39]

D. The Proposed Privacy Notice Requirements Are Overly Prescriptive and Out of Step with U.S. State Privacy Laws.

The Proposed Rules would impose granular requirements for privacy notices that depart significantly from the statute and other U.S. privacy laws. For example, the Proposed Rules would require a controller to include "the length of time the controller intends to retain each category of personal data" identified in the policy.[40] While the Act requires controllers to disclose "the categories of the personal data that the controller processes" and "the purpose for processing personal data," it notably does not require controllers to include the retention policy for each data type contemplated by the privacy policy.

This requirement is out-of-step with other U.S. state privacy laws. No other state comprehensive privacy law requires such granular retention disclosures within their privacy notice requirements, recognizing that rigid, category-specific timelines are often impractical and misaligned with how businesses actually manage data.[41] Businesses typically retain and dispose of information on the basis of the business purpose and not discrete data categories, and as such, a particular category of data may be subject to multiple different retention periods within a company. Indeed, even the CCPA regulations permit businesses to disclose "the criteria used to determine the period of time it will be retained" in the event it cannot identify the specific

---

[35] *See* Cal. Code Regs. tit. 11, § 7022(b)(1).

[36] 16 C.F.R § 312.2.

[37] N.J. Stat. Ann. § 56:8-166.4.

[38] *Id.*

[39] *Id.* § 56:8-166.14(b).

[40] Proposed Rules § 13:45L-2.2(a)(3).

[41] *See, e.g.*, Va. Code Ann. § 59.1-578(C); Iowa Code § 715D.4(5); Mont. Code § 30-14-2812(5); Colo. Rev. Stat. § 6-1-1308(1)(a).

retention period for each category of personal data included within a notice at collection.[42] In addition, mandating public disclosures of detailed retention schedules could also present significant security risks. For example, such disclosures could inadvertently aid threat actors, who could exploit the retention criteria to time malicious activities — such as impersonation attempts or fraudulent claims — after data associated with prior interactions has been deleted.

The ESA urges the Division to remove this requirement that controllers disclose the specific length of time for which each category of personal data will be retained. As an alternative, the Division should align the rule with the CCPA and other laws by allowing controllers to disclose the criteria used to determine the retention period for personal data. This approach ensures consumers are informed about the controller's data practices while preserving operational flexibility and minimizing unnecessary security risks.

III. THE PROPOSED RULES MUST AVOID BURDENSOME REQUIREMENTS THAT PROVIDE NO MEANINGFUL BENEFIT TO CONSUMERS.

The Proposed Rules must avoid implementing "paperwork exercises" and highly prescriptive compliance steps that impose significant cost and complexity on controllers without providing meaningful benefits to consumers.

A. Requiring that Controllers Provide a Toll-Free Number for Consumer Rights Requests Would Burden Controllers Without Benefitting Consumers.

The Proposed Rules' requirement that "one of [the] methods" a controller provides by which consumers can submit rights requests "must be a toll-free telephone number" staffed during business hours would impose undue burdens on controllers that operate principally or entirely online.[43]

As a threshold matter, the Proposed Rules are self-contradictory as to whether a toll-free number is required: another provision states that "***If*** the controller uses an in-person or telephone method, the method must, at a minimum, be available during the hours the controller is open for business."[44] Positioning a toll-free number as one option among many aligns with the approach taken in the Act, which provides controllers with flexibility by simply requiring that controllers describe in a privacy notice "how consumers may exercise their consumer rights, including the controller's contact information and how a consumer may appeal a controller's decision with regard to the consumer's request."[45]

Requiring controllers to permit consumers to submit rights requests through a toll-free number that is staffed during business hours would force substantial investments in a rights

---

[42] Cal. Code Regs. tit. 11, § 7012(e)(4).

[43] Proposed Rules § 13:45L-3.1(b)(1)(i).

[44] *Id*. § 13:45L-3.1(b)(2)(i).

[45] N.J. Stat. Ann. § 56:8-166.6(5). The Act only refers to toll-free numbers in its definition of a "[d]esignated request address." Though that definition is not used in the Act, it refers to "an electronic mail address, Internet website, or toll-free telephone number that a consumer may use to request the information required to be provided [in the privacy notice.]" *See id.* at § 56:8-166.4.

request method that consumers do not want or expect. Businesses — and particularly smaller businesses — that operate principally or exclusively online typically communicate with consumers by email or other electronic methods rather than by phone. For example, a video game player seeking to submit a consumer rights request in connection with personal data collected through a multiplayer online roleplaying game would generally want to do so through the game's interface or a website. Given the rise of voice spoofing technologies used by fraudsters to impersonate consumers over the phone, requiring a toll-free telephone number also could inadvertently make it easier for bad actors to gain unauthorized access to consumers' personal data.[46] Other comprehensive privacy frameworks have recognized the importance of permitting controllers to tailor their rights request methods to the manner in which they interact with consumers. For example, the CCPA includes an express exemption from its toll-free telephone number requirement for businesses that are based online.[47] While it would be most in keeping with the Act to eliminate the toll-free phone number requirement entirely, the Division should, at a minimum, limit the requirement to "controllers that primarily interact with consumers in person."

B. The Proposed Data Minimization Documentation Requirements Create a Paperwork Exercise for Controllers Without Creating Benefits for Consumers.

Like other state privacy law frameworks, the Proposed Rules require a controller to limit personal data collection to "what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer."[48] But unlike other frameworks, the Proposed Rules would impose a number of burdensome documentation requirements related to this data minimization requirement.[49] These highly prescriptive requirements have no basis in the Act and would transform the statute's principles-based data minimization standard into a paperwork exercise for controllers without adding benefit to consumers.

The Proposed Rules contemplate no fewer than *seven* data minimization measures that controllers must document and retain records for at least 24 months after the conclusion of processing activity.[50] Yet it is unclear how this burdensome paperwork requirement will result in a benefit to consumers beyond the protections provided by the Act's existing data minimization principles.[51] ESA urges the Division to reconsider these documentation requirements for the following reasons:

---

[46] Federal Communications Commission, *Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot* (June 8, 2024), https://www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot.

[47] Cal. Civ. Code § 1798.130(a)(1)(A).

[48] Proposed Rules § 13:45L-6.3(a).

[49] *Id.* § 13:45L-6.3(b).

[50] *Id.*; *id.* § 13:45L-6.5(d).

[51] N.J. Stat. Ann. § 56:8-166.12(a)(1).

- The requirements to (1) document efforts to keep consumer's personal data in a form which allows for identification "for no longer than necessary,"[52] (2) document efforts to reevaluate whether biometric identifiers are necessary for the specific processing purpose at least once a year,[53] and (3) document efforts to "immediately delete sensitive data" after a consumer revokes consent[54] contain no foundation in the statutory text and should therefore be removed. Furthermore, the requirement to document efforts to "immediately delete sensitive data" once a consumer revokes consent directly conflicts with a separate provision of the Proposed Rules, which requires processing to cease as soon as practicable after consent is withdrawn, but in any event no longer than 15 days after receiving a withdrawal request.[55]

- The requirements to (1) document that the controller has considered each processing purpose and determined the minimum amount of personal data necessary for such purpose[56] and (2) document the controller's assessment of why collection, use, or retention of data is covered pursuant to Section 56:8-166.15(b) of the Act[57] will force controllers to create and file away documents containing these analyses without adding any substantive value given the Act's existing requirements.

- The requirement to create, establish, update, and maintain a data inventory[58] needlessly imposes a prescriptive methodology for maintaining personal data. Controllers should be given flexibility to determine how to capture and organize the data maps and other information they need to comply with the substantive requirements of the statute.

Notably, these documentation requirements effectively require controllers to conduct an assessment for *every* data processing activity that is nearly as lengthy as a data protection assessment under the Proposed Rules,[59] despite the fact that data protection assessments are only required for processing activities that present a "heightened risk of harm" to consumers.[60] ESA urges the Division to remove these documentation requirements that add no additional protections for consumers and instead align the Proposed Rules with the Act's principles-based data minimization requirements.

---

[52] Proposed Rules § 13:45L-6.3(b)(3).

[53] *Id.* § 13:45L-6.3(b)(5).

[54] *Id.* § 13:45L-6.3(b)(6).

[55] *Id.* § 13:45L-7.6(e).

[56] *Id.* § 13:45L-6.3(b)(1).

[57] *Id.* § 13:45L-6.3(b)(7).

[58] *Id.* § 13:45L-6.3(b)(2).

[59] *See id.* § 13:45L-8.1(b).

[60] N.J. Stat. Ann. § 56:8-166.12(a)(9).

C. The Proposed Rules' Recordkeeping Obligations Create a Box-Ticking Exercise with No Meaningful Benefit to Consumers.

The Proposed Rules would require controllers to maintain records "sufficient to demonstrate compliance" with the statute "for as long as the processing activity continues, and for at least 24 months after the conclusion of the processing activity."[61] This requirement, which has no basis in the Act, imposes a rigid and unnecessary obligation that serves to turn compliance into a box-ticking exercise with no clear benefit to consumers.

The Proposed Rules offer no guidance as to what constitutes "sufficient" documentation, leaving business uncertain about the scope and depth of documentation required. By contrast, most state privacy laws either do not impose a specific record retention period or tie such obligations to narrow, well-defined activities like responding to consumer rights requests. Accordingly, the Division should remove these recordkeeping requirements from the final rule.

D. The Proposed Rules Wrongly Limit Children under Thirteen Years of Age from Controlling Their Own Data.

The Proposed Rules provide that "[d]ata rights requests for a consumer under the age of 13 must be submitted by a parent or guardian."[62] This limitation significantly limits young users' control over the processing of their personal data, and is out of step with developing global norms regarding children's consumer rights. The Division should clarify that a consumer under the age of 13 *or* their parent may submit a rights request, which would alleviate burdens on parents and support children's autonomy.

E. The Vague Regulations on "Dark Patterns" Must Be Clarified to Create a Workable Framework for Compliance.

The Proposed Rules introduce a number of novel requirements regarding so-called "dark patterns" that are vague and impracticable. The ESA urges the Division to clarify or eliminate these provisions to ensure all guidance is clear and actionable for controllers.

For example, the Proposed Rules would prohibit controllers from "requiring the consumer to click through disruptive screens" to exercise an opt-out right.[63] However, what constitutes a "disruptive screen" is not defined. This vague requirement creates confusion for controllers that will need to comply with the Proposed Rules, particularly for members of the video game industry that may have platforms that are more complex than a simple website. For example, if a player has started gameplay, it is unclear if a modal requiring the user to affirmatively agree to exit out of an in-progress game before being able to navigate to opt-out interface would be considered a "disruptive screen," despite providing important information or features to the player (*e.g.*, the opportunity to save).

The Proposed Rules would also prohibit "requir[ing] the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for

---

[61] Proposed Rules § 13:45L-6.5(d).

[62] *Id.* § 13:45L-3.1(g).

[63] *Id.* § 13:45L-1.5(a)(4)(i).

submitting an opt-out request."[64] However, the Act and other consumer privacy laws specifically require controllers to explain how a consumer can exercise their data rights in the privacy policy,[65] and it is thus standard practice for controllers to include information on submitting opt-out requests in the privacy policy. The Proposed Rules thus create tension with the requirements of the Act and make it unclear how controllers should avoid this "dark pattern" that appears in virtually every privacy policy published today.

Similarly, the Proposed Rules create a presumption of engaging in a dark pattern if a controller that knows *or should know of* and does not remedy broken links or "nonfunctional" email addresses, such as those that are not monitored or aggressively screen out emails from the public.[66] First, the constructive knowledge standard imposed under this rule is unworkable. Unless the controller has actual knowledge of a broken link or "nonfunctional" email address the controller cannot be expected to take action to remedy the problem. Video game companies often have numerous websites, apps, and other surfaces where they may provide links for consumers. Second, due to the volume of consumer requests, many controllers must use automated tools to filter out spam emails so that legitimate consumer requests may receive proper attention. The Proposed Rules are unclear as to what types of automated filtering would be considered so "aggressive" as to constitute a dark pattern.

In addition, the statute's inclusion of "any practice the United States Federal Trade Commission ('FTC') refers to as a 'dark pattern,'" in its definition of a dark pattern is unworkably vague.[67] The Division should take this rulemaking as an opportunity to clarify what "references" to a "dark pattern" by the FTC would fall within the definition. ESA encourages the Division to make clear that only legally binding rulemaking should qualify as "references" under the definition. Informal references, such as links or references to third-party research or academic articles on dark patterns or non-binding staff guidance do not have the same authority as a formal determination by the full Commission that a particular practice is an unlawful dark pattern. Informal materials are not reliable indicia of the FTC's policy positions and should not be considered "dark patterns" for purposes of the Act.

---

[64] *Id.* § 13:45L-1.5(a)(5)(i).

[65] *See* N.J. Stat. Ann. § 56:8-166.6(a)(5).

[66] Proposed Rules § 13:45L-1.5(a)(5)(ii) (emphasis added).

[67] N.J. Stat. Ann. § 56:8-166.4.

entertainment software association

* * *

ESA and its members remain steadfastly committed to providing consumers with online experiences in a safe and privacy-protective manner. We appreciate the opportunity to provide this feedback.

Sincerely,

Maya McKenzie
Senior Counsel, Tech Policy
Entertainment Software Association