New Jersey Administrative Code
*Provided by LexisNexis®*
*Official Publisher of the New Jersey Administrative Code*

Document: 57 N.J.R. 1101(a)

‹ Previous Next ›

# 57 N.J.R. 1101(a)

Copy Citation

VOLUME 57, ISSUE 11, JUNE 2, 2025

**RULE PROPOSALS**

**Reporter**

57 N.J.R. 1101(a)

NJ - New Jersey Register PAW 2025 JUNE JUNE 2, 2025 RULE PROPOSALS LAW AND PUBLIC SAFETY -- DIVISION OF CONSUMER AFFAIRS

▶ Interested Persons Statement

## Agency

LAW AND PUBLIC SAFETY > DIVISION OF CONSUMER AFFAIRS > OFFICE OF CONSUMER PROTECTION

## Administrative Code Citation

**Proposed New Rules: N.J.A.C. 13:45L**

## Text

**Data Privacy**

Authorized By: Cari Fais, Director, Division of Consumer Affairs.

Authority: P.L. 2023, c. 266.

Calendar Reference: See Summary below for explanation of exception to calendar requirement.

Proposal Number: PRN 2025-061.

Submit written comments by August 1, 2025, to:

> Cari Fais, Acting Director
> New Jersey Division of Consumer Affairs
> 124 Halsey Street
> PO Box 45027
> Newark, NJ 07101
> or electronically at:
> http://www.njconsumeraffairs.gov/Proposals/Pages/default.aspx

The agency proposal follows:

## Summary

The Division of Consumer Affairs (Division) proposes new N.J.A.C. 13:45L to implement P.L. 2023, c. 266, also known as the New Jersey Data Privacy Act (NJDPA), enacted on January 16, 2024, and codified at N.J.S.A. 56:8-166.4 et seq. The NJDPA regulates controllers that conduct business in this State or produce products or services that are targeted to residents of this State, and the processors that process personal data on behalf of those controllers. Among other things, the NJDPA grants consumers certain rights regarding their personal data, defined as "any information that is linked or reasonably linkable to an identified or identifiable person" (with exceptions for "de-identified data or publicly available information"). The NJDPA also requires controllers to notify consumers of their personal data rights and provide them with information as to how they may exercise those rights. Additionally, the NJDPA requires controllers that process personal data for purposes of targeted advertising or the sale of personal data to allow consumers to exercise their right to opt out of such processing through a user-selected universal opt-out mechanism.

N.J.A.C. 13:45L-1.1 sets forth the purpose and scope of proposed new Chapter 45L.

N.J.A.C. 13:45L-1.2 defines certain terms and phrases used in the chapter. N.J.A.C. 13:45L-1.2 includes definitions from the NJDPA (with clarifications to the NJDPA's definition of "sale") and provides new definitions for the terms "access request," "correction request," "data broker," "data portability request," "data right," "delete," "deletion request," "essential goods and services," "loyalty program benefit," "loyalty program partner," "opt-out preference signal," and "opt-out request."

Proposed N.J.A.C. 13:45L-1.3 lists exemptions to the provisions of the chapter. The exemptions mirror those at N.J.S.A. 56:8-166.13 through 166.15, with one clarification to the statutory exemptions. N.J.A.C. 13:45L-1.3(d)1 makes clear that pursuant to the exemption at N.J.S.A. 56:8-166.15.b(1), for "internal research," conduct is not "internal research" if: (1)

the data or resulting research is shared with a third party, unless it is de-identified or shared pursuant to N.J.A.C. 13:45L-1.3(c); or (2) the data or resulting research is used to train artificial intelligence, unless the consumer has affirmatively consented to such use.

[page=1102] Proposed N.J.A.C. 13:45L-1.4 sets forth the requirements for disclosures, notifications, and other communications to consumers. Specifically, proposed N.J.A.C. 13:45L-1.4 mandates that disclosures, notifications, and other communications required pursuant to this chapter be: (1) understandable and accessible to a controller's target audience; (2) accessible to consumers with disabilities; (3) available in the languages in which the controller in the ordinary course provides web pages, interfaces, contracts, disclaimers, sale announcements, and other information to consumers, and sent directly to the consumer in the language in which the consumer ordinarily interacts with the controller; (4) available through a readily accessible interface that consumers regularly use in conjunction with the controller's product or service; (5) provided in a readable format on all devices through which consumers regularly interact with the controller; (6) communicated in a manner by which the controller regularly interacts with consumers; (7) accurate, and not written or presented in a way that is unfair, deceptive, or misleading; and (8) available in a format that allows consumers to print a paper copy.

Proposed N.J.A.C. 13:45L-1.5 outlines the principles that controllers must follow when designing and implementing methods for submitting data right requests and obtaining consumer consent. Among other things, N.J.A.C. 13:45L-1.5 requires controllers to design and implement methods that use plain, straightforward language and comply with the requirements for disclosures, notifications, and other communications to consumers as set forth at N.J.A.C. 13:45L-1.4. N.J.A.C. 13:45L-1.5 also prohibits methods that include: (1) language or interactive elements that are confusing to the consumer; (2) manipulative language or visuals to coerce or steer consumer choice or consent; (3) choice architecture that impairs or interferes with the consumer's ability to make a choice; and (4) misleading statements, omissions, affirmative misstatements, or intentionally confusing language in consent choices to obtain consent. In addition, N.J.A.C. 13:45L-1.5 requires controllers to test their methods for submitting data right requests and obtaining consumer consent to ensure they are functional and do not undermine their consumers' choices. Lastly, N.J.A.C. 13:45L-1.5 would make any method for submitting data right requests and obtaining consent that does not comply with its provision, a dark pattern.

Pursuant to N.J.S.A. 56:8-166.6, N.J.A.C. 13:45L-2.1 requires controllers to provide consumers with a privacy notice at or before the point of collection of any personal data. Additionally, N.J.A.C. 13:45L-2.1 specifies that the required privacy notice must: (1) comply with the requirements for disclosures, notifications, and other communications to consumers at N.J.A.C. 13:45L-1.4; (2) be available in a format that allows consumers to print a paper copy; and (3) enable consumers to understand the nature and scope of the controller's processing at or before the point of collection of any personal data. Lastly, if a controller fails to provide the required privacy notice to a consumer, N.J.A.C. 13:45L-2.1 prohibits the controller from collecting personal data from the consumer.

N.J.A.C. 13:45L-2.2 specifies the content of the privacy notice required pursuant to N.J.S.A. 56:8-166.6. Among other things, N.J.A.C. 13:45L-2.2 requires controllers to include the following in their privacy notice: (1) the categories of the personal data that the controller processes; (2) the purpose or purposes for processing personal data; (3) the length of time the controller intends to retain each category of personal data it processes; (4) whether the personal data that the controller processes will be sold to or shared with third parties, and if so, the categories of personal data that the controller sells to, or shares with, third parties and the categories of third parties to which the controller may disclose a consumer's personal data; (5) an explanation of the data rights pursuant to N.J.S.A. 56:8-166.10; and (6) any information necessary for consumers to exercise those data rights. Lastly, N.J.A.C. 13:45L-2.2 requires controllers that process personal data for profiling for decisions that produce legal or similarly significant effects concerning the consumer to make additional disclosures in their privacy notices. Those additional disclosures include: (1) the categories of personal data that will be processed as part of the profiling; (2) the decisions that are made by using profiling; (3) whether the system has been evaluated for accuracy, fairness, or bias; and (4) information about how a consumer may exercise the right to opt out of the processing of personal data for profiling in furtherance of decisions that produce legal or other similarly significant effects.

N.J.A.C. 13:45L-2.3 requires controllers to notify consumers of material changes to their privacy notice in a manner by which the controllers regularly interact with consumers. In addition, N.J.A.C. 13:45L-2.3 provides a non-exhaustive list of material changes that will trigger the notice requirement. Those changes include, but are not limited to, changes to the categories of personal data processed; the categories of third parties with which the controller shares personal data; and the purposes for which personal data is processed. Lastly, if a change to a privacy notice requires a controller to obtain consent prior to processing, sharing, or selling personal data, N.J.A.C. 13:45L-2.3 mandates that consent be obtained pursuant to N.J.A.C. 13:45L-7.2.

N.J.A.C. 13:45L-2.4 requires controllers to provide consumers with a notice of the right to opt out if they sell personal data to third parties or process personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the effect on consumers. N.J.A.C. 13:45L-2.4 also specifies the content of the notice of the right to opt out.

N.J.A.C. 13:45L-2.5 requires controllers that maintain loyalty programs pursuant to N.J.S.A. 56:8-166.8 to provide consumers with a notice of the loyalty program at or before the point of program enrollment, allow consumers to withdraw from the loyalty program at any time, and offer benefits that are reasonably related to the value of the consumer's personal data. In addition, N.J.A.C. 13:45L-2.5 specifies the content of the required notice of the loyalty program and prohibits controllers from conditioning a consumer's participation in a loyalty program on the consumer's consent to process sensitive data unless the sensitive data is required for all loyalty program benefits.

Subchapter 3 addresses business practices for handling consumer requests. N.J.S.A. 56:8-166.6(a)5 requires controllers to include in their privacy notices specific methods through which consumers may submit requests to exercise their data rights. N.J.A.C. 13:45L-3.1 outlines the principles that controllers must follow in providing methods for consumers to submit requests to exercise their right to correct, delete, access, or obtain their personal data in a portable format. Pursuant to N.J.A.C. 13:45L-3.1, the controller's specific methods must: (1) incorporate the ways in which consumers normally interact with the controller; (2) enable consumers to exercise their data rights at times that are reasonably convenient to consumers; (3) be easy for consumers to execute; and (4) use data security measures that comply with the requirements at N.J.A.C. 13:45L-6.4 when exchanging information to facilitate the exercise of data rights. N.J.A.C. 13:45L-3.1 also prohibits controllers from requiring consumers to create new user accounts to exercise their data rights and from collecting personal data from consumers seeking to exercise their data rights unless the personal data is necessary to process or effectuate the request. Lastly, if a consumer seeks to exercise a data right using a method that is not one of the controller's designated methods or that is otherwise deficient in some manner unrelated to the verification process, N.J.A.C. 13:45L-3.1 requires the controller to either treat the request as if it had been submitted in accordance with the controller's designated method of submission or respond to the consumer with information on how to exercise the data right or remedy any deficiencies.

N.J.A.C. 13:45L-3.2 addresses methods for exercising the right to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, and profiling in furtherance of decisions that produce legal or similarly significant effects. Pursuant to N.J.A.C. 13:45L-3.2, a controller that collects personal data from consumers online must allow consumers to exercise their right to opt out through an opt-out preference signal.

N.J.A.C. 13:45L-3.3 outlines the process controllers must follow when responding to consumers' requests to exercise their data rights. Pursuant to N.J.A.C. 13:45L-3.3, no later than 10 business days after receiving a request to exercise a data right, a controller must confirm receipt of the request and provide the consumer with information about how the controller will effectuate the request. In addition, N.J.A.C. 13:45L-3.3 requires a controller to respond to a request to exercise a data right no later than 45 calendar days after the receipt of the verified request; provided, however, that the controller shall comply with a consumer's opt-out request in accordance with N.J.A.C. 13:45L-3.4(a)1 and 2. Lastly, if a [page=1103] controller declines to take action on a consumer's request to exercise a data right, N.J.A.C. 13:45L-3.3 requires the controller to include instructions on how to appeal the denial and the grounds for denial in its response to the consumer.

When a consumer exercises the right to opt out of the processing of personal data for one or more purposes, N.J.A.C. 13:45L-3.4 requires a controller to refrain from processing the consumer's personal data for the opt-out purpose or purposes if the controller has yet to process any of the consumer's personal data. If the controller has already processed or begun to process any of the consumer's personal data, the controller shall cease processing the consumer's personal data for the opt-out purpose or purposes as soon as possible, but not later than 15 days from the date the controller received the request. In addition, when a consumer exercises the right to opt out, N.J.A.C. 13:45L-3.4 requires a controller to: (1) ensure that the processors that process personal data on the controller's behalf stop processing the personal data, as needed, to effectuate the consumer's choice to opt out; (2) 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; and (3) maintain a record of the consumer's choice to opt out and the controller's response. Lastly, N.J.A.C. 13:45L-3.4 requires a controller to wait at least 12 months from the date that a consumer chose to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer before asking the consumer to consent to such processing.

When granting a consumer's access request, N.J.A.C. 13:45L-3.5 requires a controller to confirm whether it processes the consumer's personal data and provide the consumer with any personal data that it has collected that falls within the scope of the request, including any personal data that a processor obtained from the controller in providing services to the controller.

When granting a consumer's correction request, N.J.A.C. 13:45L-3.6 requires the controller to correct the consumer's personal data in its existing systems. N.J.A.C. 13:45L-3.6 also requires a controller to ensure that the processors that process personal data on its behalf make the necessary corrections in their respective systems. In addition, if a consumer seeks to exercise their right to correct personal data and the requested correction could be made by the consumer through the consumer's account setting, N.J.A.C. 13:45L-3.6 allows controllers to respond to the consumer's request to exercise their right to correct personal data by providing instructions on how the consumer may correct the personal data. If a controller has a good faith, reasonable, and documented belief that a customer's requested correction is not accurate, proposed N.J.A.C. 13:45L-3.6 allows the controller to require the consumer to provide documentation to determine whether the personal data, or the consumers' requested corrections to the personal data, are accurate. Lastly, if a controller declines to take action on a consumer's correction request based on the controller's determination that the contested personal data is likely accurate, N.J.A.C. 13:45L-3.6 requires the controller to maintain a record of the consumer's request that includes the reason for the controller's determination that the documentation provided by the consumer was not sufficient to support the consumer's request.

When a consumer exercises the right to deletion, N.J.A.C. 13:45L-3.7 requires the controller to delete the consumer's personal data. When granting a consumer's deletion request, N.J.A.C. 13:45L-3.7 also requires a controller to instruct the processors that process personal data on its behalf to delete the consumer's personal data, and notify all third parties to whom they have sold or with whom they have shared the consumer's personal data of the need to delete the consumer's personal data. In addition, unless prohibited by law, if a controller declines to take action on a consumer's request to delete in whole, or in part, N.J.A.C. 13:45L-3.7 requires the controller to provide the consumer with a detailed explanation of the basis for the denial. If a controller declines to take action on a consumer's request to delete and processes personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, and the consumer has not already chosen to opt out of the processing of personal data for one or more of these purposes. N.J.A.C. 13:45L-3.7 also requires the controller to ask the consumer if the consumer would like to opt out of the processing of personal data for one or more of these purposes. Lastly, N.J.A.C. 13:45L-3.7 would require a controller that has obtained personal data about a consumer from a source other than the consumer to comply with a consumer's deletion request with respect to that personal data by retaining a record of the deletion request and the minimum data necessary to ensure the consumer's data remains deleted from the controller's record, or deleting such personal data.

N.J.A.C. 13:45L-3.8 requires a controller to transfer, to a consumer, the personal data it has collected and maintains about the consumer when the consumer exercises their right to access their personal data in a portable format. In addition, N.J.A.C. 13:45L-3.8 requires the controller to effectuate the transfer through a secure method in a commonly used electronic format that, to the extent technically feasible, allows the consumer to transmit the personal data to another entity without hindrance. Lastly, if a consumer exercises the right to access their personal data in a portable format and the controller determines the manner of response would reveal its trade secrets, proposed N.J.A.C. 13:45L-3.8 requires the controller to provide as much data as possible in a portable format without disclosing trade secrets and to provide access to any additional data in a format or manner which would not reveal trade secrets, such as in a nonportable format.

Subchapter 4 addresses the methods controllers may use to authenticate the identity of consumers seeking to exercise their data rights. N.J.A.C. 13:45L-4.1 requires controllers to use commercially reasonable methods for authenticating the identity of every consumer submitting a deletion request, correction request, data portability request, or access request, and the authority of an authorized agent submitting an opt-out request on behalf of a consumer. N.J.A.C. 13:45L-4.1 also lists the factors that a controller must consider when determining whether an authentication method is commercially reasonable. Those factors include: (1) the type, sensitivity, and value of the personal data collected and maintained about the consumer; (2) the risk of harm to the consumer posed by any unauthorized access, deletion, or correction of the personal data; (3) the likelihood that malicious actors would seek the personal data; (4) whether the personal data to be provided by the consumer to verify their identity sufficiently protects against fraudulent requests; (5) the manner in which the controller interacts with the consumer; and (6) the technologies available for verification. Pursuant to N.J.A.C. 13:45L-4.1, a controller that cannot authenticate a consumer seeking to exercise a data right request using commercially reasonable efforts is not required to grant the consumer's request. In addition, N.J.A.C. 13:45L-4.1 requires controllers to implement security measures consistent with N.J.A.C. 13:45L-6.4 to protect personal data exchanged to authenticate a consumer or to authenticate an authorized agent's authority. Lastly, N.J.A.C. 13:45L-4.1 prohibits controllers from requiring consumers or authorized agents to pay a fee for authentication or requiring consumers to incur costs, unless the controllers compensate the consumers for the cost.

N.J.A.C. 13:45L-4.2 and 4.3 address verification processes for consumers with password-protected accounts and consumers who do not have, or cannot access, a password-protected account, respectively. Pursuant to N.J.A.C. 13:45L-4.2, if a controller suspects fraudulent or malicious activity on, or from, the password-protected account, the controller must not comply with a consumer's deletion, correction, data portability, or access request until further authentication procedures determine that the consumer request is authentic and the requestor is the consumer about whom the controller has collected information or the consumer's authorized agent. N.J.A.C. 13:45L-4.3 requires controllers that receive data right requests from consumers who do not have or cannot access a password-protected account with the controller to verify the identities of the consumers submitting the requests to a reasonable or reasonably high degree of certainty. The level of certainty required is based on the type of request. For example, a controller that receives an access request seeking to know the categories of personal data that the controller collects from the consumer is required to authenticate the identity of the requestor to a reasonable degree of certainty. However, a controller that receives an access request seeking to know specific [page=1104] personal data points is required to verify the identity of the requestor to a reasonably high degree of certainty. Lastly, N.J.A.C. 13:45L-4.3 requires controllers to deny access requests if they cannot authenticate the identity of the requestor.

N.J.A.C. 13:45L-4.4 addresses verification processes for authorized agents. Pursuant to N.J.A.C. 13:45L-4.4, unless an authorized agent has provided the controller with proof that the consumer has given the authorized agent power of attorney pursuant to N.J.S.A. 46:2B-1 et seq., a controller may require the authorized agent to provide proof that the consumer gave the agent signed permission to exercise a data right. N.J.A.C. 13:45L-4.4 also requires an authorized agent to implement and maintain reasonable security procedures and practices to protect the consumer's information. Lastly, N.J.A.C. 13:45L-4.4 prohibits authorized agents from using a consumer's personal data, or any information collected from or about the consumer, for any purpose other than verification, fraud prevention, or fulfilling the consumer's request to exercise a data right.

Pursuant to N.J.S.A. 56:8-166.11(b), a controller that processes personal data for the purposes of targeted advertising or the sale of personal data must allow consumers to exercise the right to opt out of such processing through a user-selected universal opt-out mechanism. N.J.A.C. 13:45L-5.1 addresses how a controller must respond when they receive an opt-out preference signal transmitted through a universal opt-out mechanism, and N.J.A.C. 13:45L-5.2 details the technical specifications universal opt-out mechanisms must meet to comply with the NJDPA. Pursuant to N.J.A.C. 13:45L-5.1, when a controller that collects personal data from consumers online receives or detects an opt-out preference signal from a universal opt-out mechanism that meets the requirements at N.J.A.C. 13:45L-5.2, the controller must treat the opt-out preference signal as a valid choice to opt out of the processing of personal data, as indicated by the universal opt-out mechanism. In addition, pursuant to N.J.A.C. 13:45L-5.1, a controller must continue to comply with an opt-out request transmitted through a universal opt-out mechanism until the consumer consents to the processing of personal data. Lastly, N.J.A.C. 13:45L-5.1 outlines how controllers must respond if an opt-out preference signal conflicts with a consumer's controller-specific privacy setting that allows the controller to sell or share their personal data or with a consumer's participation in a loyalty program that requires the consumer to consent to the sale or sharing of personal data. If an opt-out preference signal conflicts with a consumer's controller-specific privacy setting, the controller must comply with the opt-out preference signal, but the controller may notify the consumer of the conflict and give the consumer an opportunity to consent to the sale or sharing of their personal data. If an opt-out preference signal conflicts with the consumer's participation in a controller's loyalty program, the controller may notify the consumer that complying with the opt-out preference signal would withdraw the consumer from the loyalty program and ask the consumer to affirm that they intend to withdraw from the loyalty program. If the controller does not ask the consumer to affirm their intent to withdraw from the loyalty program, the controller is required to comply with the opt-out preference signal for that browser or device and any consumer profile the controller associates with that browser or device.

N.J.A.C. 13:45L-5.2 requires a universal opt-out mechanism to: (1) allow consumers to automatically communicate their opt-out choice with multiple controllers; (2) clearly describe any limitations that may be applicable to the mechanism; (3) comply with the requirements for disclosures, notifications, and other communications to consumers set forth at N.J.A.C. 13:45L-1.4; (4) store, process, and transmit any consumer personal data using data security measures that comply with N.J.A.C. 13:45L-6.4; (5) not permit its manufacturer to unfairly disadvantage another controller; (6) 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; (7) be as consistent as possible with any other similar platform, technology, or mechanism required by any Federal or State law or regulation; (8) be consumer-friendly, clearly described, and easy to use by the average consumer; and (9) not prevent a controller from determining whether a consumer is a resident of this State or that the universal opt-out mechanism represents a legitimate request to opt out of the processing of personal data. Lastly, N.J.A.C. 13:45L-5.2 requires universal opt-out mechanisms to communicate consumer opt-out preferences by sending opt-out preference signals and prevents universal opt-out mechanisms from using, disclosing, or retaining any personal data collected from a consumer in connection with the sending or processing of a choice to opt out for any purpose other than sending or processing the opt-out preference signal.

Subchapter 6 clarifies the duties that controllers owe to consumers. N.J.A.C. 13:45L-6.1 requires controllers to disclose and describe to consumers the purpose or purposes for which they process personal data before they collect the consumers' personal data. A controller must do this in a level of detail that enables consumers to understand how each category of their personal data is used. If a controller is collecting and processing personal data for more than one purpose, it must specify each purpose with enough detail to allow a consumer to understand each purpose. N.J.A.C. 13:45L-6.1 prohibits controllers from identifying one broad purpose to justify numerous processing activities, specifying one broad purpose to cover potential future processing activities, or identifying so many purposes for which personal data could be processed, that the purpose or purposes become unclear or uninformative.

N.J.A.C. 13:45L-6.2 prohibits a controller from processing personal data for purposes that are neither reasonably necessary to or compatible with the purposes disclosed to the consumer before collection, unless the controller obtains the consumer's consent. N.J.A.C. 13:45L-6.2 also sets forth the factors that a controller must consider when determining whether a new processing purpose is reasonably necessary to or compatible with the purpose disclosed to a consumer at or before the point of collection. The factors include: (1) the expectations of an average consumer concerning how their personal data would be processed once it is collected; (2) the link between the original specified purpose or purposes and the purpose or purposes of further processing; (3) the type, nature, and amount of personal data subject to the new processing purpose; (4) the type and degree of the potential impact to the consumer of the new processing purpose; and (5) the existence of additional safeguards for the personal data.

N.J.A.C. 13:45L-6.3 requires controllers to limit their collection of personal data to what is necessary in relation to the specific purpose or purposes for which such data is processed, as disclosed to the consumer. N.J.A.C. 13:45L-6.3 also prohibits a controller from collecting personal data that does not fall within one or more of the categories of personal data identified in the controller's privacy notice. Pursuant to N.J.A.C. 13:45L-6.3, if a controller intends to collect personal data for a purpose that does not fall within one or more of the categories identified in its privacy notice, the controller must revise its privacy notice and notify consumers of the change pursuant to N.J.A.C. 13:45L-2.3. In addition, to ensure that personal data is not kept longer than necessary, N.J.A.C. 13:45L-6.3 requires controllers to set specific time limits for erasure or for conducting a periodic review.

Proposed N.J.A.C. 13:45L-6.4 requires controllers to establish, implement, update, maintain, and document data security practices to protect the confidentiality, integrity, and accessibility of personal data and to secure personal data during both storage and use from unauthorized acquisition. N.J.A.C. 13:45L-6.4 lists several factors that a controller must consider when determining appropriate data security safeguards. The factors include: (1) applicable industry standards; (2) the sensitivity and amount of personal data; (3) the original source of the personal data; and (4) the risk of harm to consumers resulting from unauthorized or unlawful access, use, or degradation of the personal data. Lastly, N.J.A.C. 13:45L-6.4 specifies that data security measures implemented by controllers must ensure the confidentiality, integrity, accessibility, and availability of personal data; identify and protect against threats to data security; and be designed to protect against unauthorized access, accidental loss, destruction, or damage of personal data and equipment used for processing.

N.J.A.C. 13:45L-6.5 provides the information that controllers must include in their records of data rights requests to comply with the recordkeeping requirement at N.J.S.A. 56:8-166.10(a). The required information includes: (1) the date of the request; (2) a copy of the data right request; (3) the date of the controller's response; and (4) the substance of the controller's response. In addition, N.J.A.C. 13:45L-6.5 requires that the records be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a third party [page=1105] assumes control of personal data to ensure any new controller continues to recognize the consumer's previously exercised data rights. N.J.A.C. 13:45L-6.5 also requires controllers to practice recordkeeping in compliance with N.J.A.C. 13:45L-6.2, 6.3, and 7.3, for as long as the processing activity continues, and for at least 24 months after the conclusion of processing activity. N.J.A.C. 13:45L-6.5 requires controllers to maintain the required records in a readable format, appropriate to the sophistication and size of the controller's business, and to implement and maintain data security measures that comply with N.J.A.C. 13:45L-6.4. Lastly, N.J.A.C. 13:45L-6.5 prohibits controllers from using personal data maintained for recordkeeping purposes for any other purpose, except as necessary for the controller to review and modify its processes for complying with the NJDPA.

Subchapter 7 clarifies the NJDPA's requirements regarding requesting and obtaining consent from consumers prior to processing or selling certain personal data. N.J.A.C. 13:45L-7.1 specifies when a controller needs to obtain consent from a consumer and addresses when consent obtained prior to the effective date of the proposed rules will be considered valid. N.J.A.C. 13:45L-7.2 sets forth what constitutes valid consent. Pursuant to N.J.A.C. 13:45L-7.2, valid consent must: (1) be obtained through the consumer's clear, affirmative action; (2) be freely given by the consumer; (3) be specific; (4) reflect the consumer's unambiguous agreement; and (5) provide the information required pursuant to N.J.A.C. 13:45L-7.3(c). Pursuant to N.J.A.C. 13:45L-7.3, consent must be obtained using a form or mechanism that is simple and readily accessible to the consumer. Requests for consent must also be prominent, concise, and separate and distinct from other terms and conditions, and comply with the design and interface requirements at N.J.A.C. 13:45L-1.5, including the prohibition against using dark patterns. N.J.A.C. 13:45L-7.3 also requires specific information be included on the request interface itself, including the controller's identity; the reason that consent is required explained in plain language; the processing purpose or purposes for which consent is sought; the categories of personal data that the controller will process for that purpose or purposes; the names of any third parties receiving sensitive data through sales; and an explanation of the consumer's right to withdraw consent, including how they can exercise that right.

N.J.A.C. 13:45L-7.4 requires controllers that have actual knowledge that they collect or process the personal data of a consumer younger than 13 to obtain consent from a parent or lawful guardian of the consumer before collecting or processing the consumer's personal data.

N.J.A.C. 13:45L-7.4 then requires controllers that process the personal data of consumers younger than 13 to establish, document, and verify that the person consenting to the collection or processing of the personal data about the consumer is the consumer's parent or lawful guardian. Lastly, when controllers receive consent from a consumer's parent or lawful guardian, N.J.A.C. 13:45L-7.4 requires the controller to inform the parent or guardian of the right to opt out of the processing of personal data and the process for doing so on behalf of the consumer who is less than 13 years old.

Pursuant to N.J.A.C. 13:45L-3.4(f), a controller must wait at least 12 months from the date a consumer exercises their right to opt out before asking the consumer to consent to the processing of personal data. However, pursuant to N.J.A.C. 13:45L-7.5, a controller may request a consumer's consent before the end of the 12-month period if a consumer initiates a transaction or attempts to use a product or service inconsistent with the consumer's choice to opt out, such as signing up for a loyalty program that involves the sale of personal data to a loyalty program partner.

N.J.A.C. 13:45L-7.5 requires controllers to comply with the requirements at N.J.A.C. 13:45L-7.2 and 7.3 when seeking consent from a consumer who has previously opted out of processing of their personal data. Furthermore, a controller seeking consent to process personal data for an opt-out purpose after a consumer has opted out of processing for that purpose is prohibited from making consent unnecessarily confusing or difficult.

N.J.A.C. 13:45L-7.6 requires controllers to allow consumers to refuse or withdraw consent through a mechanism that is at least as accessible and user-friendly as the mechanism by which the consumer provided consent. Additionally, if a consumer withdraws consent for a processing activity, N.J.A.C. 13:45L-7.6 requires controllers to cease that processing activity as soon as practicable, but not later than 15 days after the withdrawal. Lastly, while N.J.A.C. 13:45L-7.6 prohibits detrimental treatment based on a consumer's decision to refuse or withdraw consent, it does not require controllers to provide programs, products, or services if a consumer refuses to consent to, or withdraws consent for, the processing of personal data strictly necessary for the programs, products, or services.

N.J.A.C. 13:45L-7.7 addresses when controllers must refresh consent to continue to process the sensitive personal data of a consumer or the personal data of a consumer at least 13 years of age, but younger than 17 years of age. Pursuant to N.J.A.C. 13:45L-7.7, a controller must refresh consent when a consumer has not interacted with the controller in the prior 24 months or when a processing purpose materially evolves such that the new purpose is not reasonably necessary to the purposes for which such personal data is processed, as disclosed to the consumer.

Subchapter 8 sets forth requirements for controllers carrying out data protection assessments pursuant to N.J.S.A. 56:8-166.12(a)9. N.J.A.C. 13:45L-8.1 requires controllers to conduct and document data protection assessments before engaging in processing activities that present a heightened risk of harm to consumers. N.J.A.C. 13:45L-8.1 also lists the minimum content requirements for data protection assessments, which include risks to the rights of consumers posed by the processing activity; whether the benefits of the processing outweigh the risks; and measures and safeguards the controller will employ to reduce the risks identified.

N.J.A.C. 13:45L-8.2 addresses when controllers must conduct data protection assessments. N.J.A.C. 13:45L-8.2 states that controllers must review and update their data protection assessments, as often as appropriate, throughout the processing activity's life cycle to monitor for harm and adjust safeguards and ensure that data protection and privacy are considered as the data continues to be processed. In addition, N.J.A.C. 13:45L-8.2 requires that data protection assessments regarding the processing of personal data for profiling in furtherance of decisions that produce legal or similarly significant effects be reviewed and updated at least annually. N.J.A.C. 13:45L-8.2 also sets forth criteria for controllers to determine when a new data processing activity has been generated and requires controllers to update data protection assessments when that occurs. Lastly, N.J.A.C. 13:45L-8.2 requires controllers to store data protection assessments in an electronic, transferable form, for as long as the processing activity continues, and for at least three years after the conclusion of the processing activity.

As the Division has provided a 60-day comment period on this notice of proposal, this notice is excepted from the rulemaking calendar requirement pursuant to N.J.A.C. 1:30-3.3(a)5.

## Social Impact

The Division believes the proposed new rules will have a positive social impact because they facilitate the implementation of the NJDPA's provisions. The NJDPA protects consumers from the unauthorized use and sale of their personal data, which can cause substantial economic, physical, emotional, and reputational harm. The NJDPA empowers consumers to take back control of their personal data, including how and when that data is collected, shared, or sold. The proposed new rules will make it easier for consumers to exercise their data rights by specifying how controllers must respond to data right requests, from accepting and verifying the requests, to responding to and complying with the requests.

In addition, to enable consumers to make informed decisions about their data rights, the NJDPA requires controllers to provide consumers with a privacy notice regarding the controllers' personal data processing, selling, and profiling practices. The proposed new rules clarify this requirement by providing controllers with instructions on the requirements of the privacy notice, including the content and form of the notice. The proposed new rules also provide the framework for the universal opt-out mechanism enacted by the NJDPA, which will ensure that consumers have a simple and easy method to exercise their right to opt out with multiple controllers. Furthermore, the proposed new rules clarify the duties the NJDPA imposes on controllers, including the duty to specify the purposes for which controllers process personal data and to refrain from processing personal data for purposes that are neither reasonably necessary to or compatible with the purposes disclosed to a consumer before collection, unless the controller obtains the consumer's [page=1106] consent; the duty to limit the collection of personal data to what is necessary; and a duty of care to protect the confidentiality, integrity, and accessibility of personal data.

To facilitate controllers' compliance with the NJDPA's consent requirements, the proposed new rules clarify when consent is required and how controllers can lawfully solicit and refresh consumer consent. The consent provisions of the proposed new rules also establish additional protections for children under 13 to protect them from harm from the misuse of their personal data. Lastly, the proposed new rules set forth requirements for controllers conducting the data protection assessments required pursuant to the NJDPA to protect consumers from processing activities that present a heightened risk of harm. These data protection assessments will especially help consumers who may face discriminatory harm, such as a violation of Federal, State, or local anti-discrimination laws, from the misuse of their personal data.

### Economic Impact

The proposed new rules impose compliance requirements on controllers and processors. Controllers will incur costs to update their websites and build and maintain internal mechanisms to provide the required notices, enable consumers to exercise their data rights, and request consumer consent. Controllers will also incur costs to establish, implement, and maintain data security measures to protect personal data; comply with the NJDPA's recordkeeping requirements; and perform the data protection assessments required before conducting processing activities that present a heightened risk of harm to consumers. Lastly, processors may incur costs to fulfill their duty to assist controllers in meeting their obligations pursuant to the NJDPA.

The Division believes that the public interest in protecting consumer personal data and facilitating the exercise of the data rights granted by the NJDPA outweighs the costs imposed.

### Federal Standards Statement

The proposed new rules incorporate, but do not exceed, the requirements of the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 et seq., and the regulations promulgated thereto. Accordingly, a Federal standards analysis is not required.

### Jobs Impact

The Division does not believe that the proposed new rules will result in the creation or loss of jobs in the State.

### Agriculture Industry Impact

The proposed new rules will have no impact on the agriculture industry in the State.

### Regulatory Flexibility Analysis

Any controller or processor that is a "business which is resident in this State, independently owned and operated and not dominant in its field, and which employs fewer than 100 full-time employees" constitutes a "small business" within the meaning of the Regulatory Flexibility Act, N.J.S.A. 52:14B-16 et seq. (RFA). N.J.S.A. 52:14B-17. To the extent a controller or processor qualifies as a "small business" pursuant to the RFA, the following analysis applies pursuant to N.J.S.A. 52:14B-19.

The costs of compliance for small businesses are the same as those imposed on businesses generally and are described in the Summary and Economic Impact above. The proposed new rules require controllers to provide methods through which consumers may exercise their data rights and impose notice, consent, data protection, and recordkeeping requirements, as described in the Summary above. As the notification, consent, recordkeeping, data security, and data protection assessment requirements in the proposed new rules are necessary to adequately regulate controllers and processors and enable consumers to exercise the personal data rights granted by the NJDPA, the Division believes that the rules must be uniformly applied to all controllers and processors, and no exemptions are provided based on the size of the controller or processor.

## Housing Affordability Impact Analysis

The proposed new rules will have an insignificant impact on the affordability of housing in New Jersey, and there is an extreme unlikelihood that the rulemaking would evoke a change in the average costs associated with housing because the proposed new rules concern the personal data rights granted by the NJDPA and notification, consent, recordkeeping, and data security requirements for controllers and processors.

## Smart Growth Development Impact Analysis

The proposed new rules will have an insignificant impact on smart growth, and there is an extreme unlikelihood that the rulemaking would evoke a change in housing production in Planning Areas 1 or 2, or within designated centers, pursuant to the State Development and Redevelopment Plan in New Jersey because the proposed new rules concern the personal data rights granted by the NJDPA and notification, consent, recordkeeping, and data security requirements for controllers and processors.

## Racial and Ethnic Community Criminal Justice and Public Safety Impact

The Division has evaluated this rulemaking and determined that it will not have an impact on pretrial detention, sentencing, probation, or parole policies concerning adults and juveniles in the State. Accordingly, no further analysis is required.

**Full text** of the proposed new rules follows:

CHAPTER 45L

DATA PRIVACY RULES

SUBCHAPTER 1. GENERAL PROVISIONS

13:45L-1.1 Purpose and scope

(a) The purpose of this chapter is to implement the provisions at P.L. 2023, c. 266 (the Act). The chapter addresses the obligations of controllers and processors regarding the collection, control, and processing of personal data.

(b) This chapter shall apply to:

1. Controllers that conduct business in this State or produce products or services that are targeted to residents of this State, and that during a calendar year either:

i. Control or process the personal data of at least 100,000 consumers, excluding personal data processed solely for the purpose of completing a payment transaction; or

ii. Control or process the personal data of at least 25,000 consumers and the controller derives revenue, or receives a discount on the price of any goods or services from the sale of personal data; and

2. Processors.

13:45L-1.2 Definitions

The following words and terms, as used in this chapter, shall have the following meanings, unless the context clearly indicates otherwise.

"Access request" or "request to access" means a consumer request that a controller confirms, whether the controller processes the consumer's personal data or that the controller gives the consumer access to such personal data pursuant to N.J.S.A. 56:8-166.10(a)1.

"Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity. For the purposes of this definition, "control" means:

1. The ownership of or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company;

2. The control in any manner over the election of a majority of the directors or individuals exercising similar functions; or

3. The power to exercise a controlling influence over the management or policies of a company.

"Biometric data" means data generated by automatic or technological processing, measurements, or analysis of an individual's biological, physical, or behavioral characteristics, including, but not limited to:

1. Fingerprint;

2. Voiceprint;

3. Eye retinas;

4. Irises;

5. Facial mapping;

6. Facial geometry;

7. Facial templates; or

8. Other unique biological, physical, or behavioral patterns or characteristics that are used, or intended to be used, singularly or in [page=1107] combination with each other or with other personal data, to identify a specific individual.

"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.

"Child" shall have the same meaning as provided in the COPPA.

"Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, or any other unambiguous affirmative action. "Consent" shall not include:

1. Acceptance of general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information;

2. Hovering over, muting, pausing, or closing a given piece of content; or

3. Agreement obtained through the use of dark patterns.

"Consumer" means an identified person who is a resident of this State acting only in an individual or household context. "Consumer" shall not include a person acting in a commercial or employment context. "Acting in a commercial context" means engaging in a business-to-business transaction.

"Controller" means an individual, or legal entity, that alone or jointly with others determines the purpose and means of processing personal data.

"COPPA" means the Federal Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 et seq., and any rules, regulations, guidelines, and exceptions thereto, as may be amended from time to time.

"Correction request" or "request to correct" means a consumer request that a controller correct any inaccuracy in the personal data that the controller and its processors hold about the consumer pursuant to N.J.S.A. 56:8-166.10(2).

"Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, and includes, but is not limited to, any practice the United States Federal Trade Commission refers to as a "dark pattern."

"Data broker" means 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. Examples of a direct relationship include if the consumer is a past or present:

1. Customer, client, subscriber, or user of the person or legal entity's goods or services;

2. Employee, contractor, or agent of the person or legal entity;

3. Investor in the person or legal entity; or

4. Donor to the person or legal entity.

"Data portability request" means a consumer request that a controller provide a copy of the consumer's personal data held by the controller in a portable format and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance pursuant to N.J.S.A. 56:8-166.10(a)4.

"Data right" or "data rights" refers to the rights granted pursuant to N.J.S.A. 56:8-166.10.

"Decisions that produce legal or similarly significant effects concerning the consumer" means decisions, including automated or algorithmic decisions, that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods and services.

"De-identified data" means data that cannot be reasonably used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data:

1. Takes reasonable measures to ensure that the data cannot be associated with an individual;

2. Publicly commits to maintain and use the data only in a de-identified fashion and not to attempt to re-identify the data; and

3. Contractually obligates any recipients of the information to comply with the requirements of this paragraph.

Pseudonymized data that can be used to infer information about, or otherwise be linked to, an identified or identifiable individual or a device linked to such an individual is not de-identified data.

"Delete" means to remove data from all existing systems, such that it is not maintained in a retrievable form and cannot be retrieved in the normal course of business. Existing systems include, but are not limited to, archived or nonactive systems or systems maintained by processors.

"Essential goods and services" means 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.

"Heightened risk of harm" includes, pursuant to N.J.S.A. 56:8-166.12(c): (1) processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of: unfair or deceptive treatment of, or unlawful disparate impact on, consumers; financial or physical injury to consumers; a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns of consumers if the intrusion would be offensive to a reasonable person; or other substantial injury to consumers; (2) selling personal data; and (3) processing sensitive data. This definition applies regardless of whether the risk results from the use of manual, automated, or algorithmic processes.

"Loyalty program benefit" means an offer of a discount or of a superior price, rate, level, quality, or selection of goods or services provided to a consumer through a loyalty program. Such benefits may be provided directly by a controller or through a loyalty program partner.

"Loyalty program partner" means a third party that provides loyalty program benefits to consumers through a loyalty program in partnership with the controller.

"Opt-out preference signal" means a signal that is sent on behalf of the consumer, which communicates the consumer's decision to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legally or similarly significant effects concerning a consumer.

"Opt-out request" or "request to opt out" means a consumer request that a controller refrain from processing or selling the consumer's personal data pursuant to N.J.S.A. 56:8-166.10(a)5, and includes an opt-out preference signal.

"Personal data" means any information that is linked or reasonably linkable to an identified or identifiable person. "Personal data" shall not include de-identified data or publicly available information. Personal data is "reasonably linkable" if it can identify a person or a device linked to a person when aggregated with other data, including, but not limited to, a person's: (1) full name; (2) mother's maiden name; (3) telephone number; (4) IP address or other unique device identifiers; (5) place of birth; (6) date of birth; (7) geographical details (for example, zip code, city, state, or country); (8) employment information; (9) username, email address, or any other account holder identifying information (including, but not limited to, identifying information related to social media accounts); (10) mailing address; and (11) race, ethnicity, sex, sexual orientation, or gender identity or expression.

"Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

"Process" or "processing" means an operation, or set of operations, performed, whether by manual or automated means, on personal data, or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data, and also includes the actions of a controller directing a processor to process personal data.

"Processor" means a person, private entity, public entity, agency, or other entity that processes personal data on behalf of the controller.

"Profiling" means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to [page=1108] an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Publicly available information" means information that is lawfully made available from Federal, State, or local government records, or widely distributed media or information that a controller has a reasonable basis to believe a consumer has lawfully made available to the general public and has not restricted to a specific audience. "Publicly available information" shall not include the scraping of personal data or personal data obtained from data brokers that is not otherwise publicly available.

"Sale" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. "Sale" shall not include the:

1. Disclosure of personal data to a processor that processes the personal data on the controller's behalf, provided that the processor does not use the data for its own purposes;

2. 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;

3. Disclosure or transfer of personal data to an affiliate of the controller, provided that the disclosure or transfer is not for the purpose of circumventing any of the obligations or protections conferred by this chapter;

4. Disclosure of personal data that the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience; or

5. Disclosure or transfer of personal data to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third

party assumes control of all or part of the controller's assets.

"Sensitive data" means personal data revealing:

1. Racial or ethnic origin;

2. Religious beliefs;

3. Mental or physical health condition, treatment, or diagnosis;

4. Financial information, which shall include a consumer's account number, account log-in, financial account, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account;

5. Sex life or sexual orientation;

6. Citizenship or immigration status;

7. Status as transgender or non-binary;

8. Genetic or biometric data that may be processed for the purpose of uniquely identifying an individual;

9. Personal data collected from a known child; or

10. Precise geolocation data.

"Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated Internet websites or online applications to predict such consumer's preferences or interests. "Targeted advertising" shall not include:

1. Advertisements based on activities within a controller's own internet websites or online applications;

2. Advertisements based on the context of a consumer's current search query, visit to an internet website, or online application;

3. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

4. Processing personal data solely to measure or report advertising frequency, performance, or reach.

"Third party" means a person, private entity, public entity, agency, or entity other than the consumer, controller, or affiliate or processor of the controller.

"Trade secret" has the same meaning as section 2 at P.L. 2011, c. 161 (N.J.S.A. 56:15-2).

"Verified request" means the process through which a consumer may submit a request to exercise a right or rights established at P.L. 2023, c. 266, and by which a controller can reasonably authenticate the request and the consumer making the request using commercially reasonable means.

13:45L-1.3 Exemptions

(a) The following are exempt from the provisions of this chapter:

1. Protected health information collected by a covered entity or business associate subject to the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub.L.104-191, and the Health Information Technology for Economic and Clinical Health Act, 42 U.S.C. §§ 17921 et seq.;

2. A financial institution, data, or an affiliate of a financial institution that is subject to Title V of the Federal Gramm-Leach-Bliley Act, 15 U.S.C. §§6801 et seq., and the rules and implementing regulations promulgated thereunder;

3. The secondary market institutions identified at 15 U.S.C. § 6809(3)(D) and 12 CFR 1016.3(l)(3)(iii);

4. An insurance institution subject to P.L. 1985, c. 179 (N.J.S.A. 17:23A-1 et seq.);

5. The sale of a consumer's personal data by the New Jersey Motor Vehicle Commission that is permitted pursuant to the Federal Drivers' Privacy Protection Act of 1994, 18 U.S.C. §§ 2721 et seq.;

6. Personal data collected, processed, sold, or disclosed by a consumer reporting agency, as defined at 15 U.S.C. § 1681a(f), if the collection, processing, sale, or disclosure of the personal data is limited, governed, collected, maintained, disclosed, sold, communicated, or used only as authorized by the Federal Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq., and implementing regulations;

7. Any State agency as defined in section 2 at P.L. 1971, c. 182 (N.J.S.A. 52:13D-13), any political subdivision, and any division, board, bureau, office, commission, or other instrumentality created by a political subdivision; and

8. Personal data that is collected, processed, or disclosed, as part of research conducted in accordance with the Federal Policy for the protection of human subjects pursuant to 45 CFR Part 46 or the protection of human subjects pursuant to 21 CFR Parts 50 and 56.

(b) Nothing in this chapter shall require a controller to:

1. Re-identify de-identified data; or

2. 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.

(c) Pursuant to N.J.S.A. 56:8-166.15, nothing in this chapter shall be construed to restrict a controller's or processor's ability to:

1. Comply with Federal or State law or regulations;

2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by Federal, State, municipal, or other governmental authorities;

3. Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate Federal, State, or municipal ordinances or regulations;

4. Investigate, establish, exercise, prepare for, or defend legal claims;

5. Provide a product or service specifically requested by a consumer;

6. Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

7. Take steps at the request of a consumer prior to entering into a contract;

8. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual, and where the processing cannot be manifestly based on another legal basis;

9. Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action;

10. Engage in public- or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines, or similar independent oversight entities that determine:

i. Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

ii. The expected benefits of the research outweigh the privacy risks; and

[page=1109] iii. Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with re-identification;

11. Assist another controller, processor, or third party with any of the obligations pursuant to this chapter; or

12. Personal data for reasons of public interest in the area of public health, community health, or population health, but solely to the extent that such processing is:

i. Subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and

ii. Under the responsibility of a professional subject to confidentiality obligations pursuant to Federal, State, or local law.

(d) The obligations imposed on controllers or processors pursuant to this chapter shall not restrict a controller's or processor's ability to collect, use, or retain data for internal use to:

1. Conduct internal research to develop, improve, or repair products, services, or technology. Collection, use, or retention of data shall not be considered to be for the purpose of internal research if:

i. The data or resulting research is shared with a third party, unless it is de-identified or shared pursuant to one of the reasons identified at (c) above; or

ii. The data or resulting research is used to train artificial intelligence, unless the consumer has affirmatively consented to such use.

2. Effectuate a product recall;

3. Identify and repair technical errors that impair existing or intended functionality; or

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party. Personal data collected, used, or retained pursuant to this subsection shall, where applicable, take into account the nature and purpose or purposes of such collection, use, or retention. Such data shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to such collection, use, or retention of personal data.

(e) The obligations imposed on controllers or processors pursuant to this chapter shall not apply where compliance by the controller or processor with the provisions of law would violate an evidentiary privilege pursuant to the laws of this State. Nothing in this chapter shall be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege pursuant to the laws of the State as part of a privileged communication.

(f) Personal data that are processed by a controller pursuant to an exception provided by this section:

1. Shall not be processed for any purpose other than a purpose expressly listed in this section; and

2. Shall be processed solely to the extent that the processing is necessary, reasonable, and proportionate to the specific purpose or purposes listed in this section.

(g) If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with the requirements in this section.

(h) Processing personal data for the purposes expressly identified in this section shall not solely make a legal entity a controller with respect to such processing if such entity would not otherwise meet the definition of a controller.

13:45L-1.4 Requirements for disclosures, notifications, and other communications to consumers

(a) The disclosures, notifications, and other communications required by this chapter must be:

1. Understandable and accessible to a controller's target audience (for example, a disclosure, notification, or other communication must use plain, straightforward language and avoid technical or legal jargon);

2. Accessible to consumers with disabilities, including through the use of digital accessibility tools;

3. Available in the languages in which the controller in its ordinary course provides web pages, interfaces, contracts, disclaimers, sale announcements, and other information to consumers, and sent directly to the consumer in the language in which the consumer ordinarily interacts with the controller;

4. Available through a readily accessible interface that consumers regularly use in conjunction with the controller's product or service;

5. 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;

6. Unless otherwise stated in this chapter, communicated in a manner by which the controller regularly interacts with consumers. For instance, if a controller regularly interacts with consumers offline, an offline version must be provided to the consumers;

7. Accurate, and must not be written or presented in a way that is unfair, deceptive, or misleading; and

8. Available in a format that allows consumers to print a paper copy.

(b) Pursuant to (a)2 above, a controller that provides a notice online must, at a minimum, follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.2 of October 5, 2023 (Guidelines), from the World Wide Web Consortium, incorporated herein by reference, or any successor to the Guidelines, as applicable.

(c) Pursuant to (a)2 above, a controller that provides a disclosure, notification, or other communication in a non-online format must provide information on how a consumer with a disability may access the disclosure, notification, or other communication and exercise their data rights.

13:45L-1.5 Requirements related to user interface design, choice architecture, and dark patterns

(a) Controllers shall design and implement methods for submitting data right requests and obtaining consent that incorporate the following principles:

1. The methods shall use plain, straightforward language and comply with the requirements for disclosures, notifications, and other communications to consumers set forth at N.J.A.C. 13:45L-1.4;

2. The methods shall not use language, visuals, or interactive elements that are confusing to the consumer, including the use of double negatives or toggles or buttons that do not clearly indicate the consumer's choice;

3. The methods shall not use language, visuals, or interactive elements to coerce or steer consumer choice or consent, including presenting choices in a way that shames or pressures the user into selecting a specific choice. For example, presenting the choice: "I accept, I want to help defeat cancer" versus "No, I don't care about cancer patients" may violate this provision;

4. The methods shall not impair or interfere with the consumer's ability to make a choice, exercise their choice, or give free, specific, informed, and unambiguous consent; for example:

i. Requiring the consumer to click through disruptive screens before being able to opt out; or

ii. Bundling choices so that the consumer is forced to consent to the use of personal data for any purposes that are incompatible with the context in which the personal data was collected. For example, a controller that provides a location-based service, such as a mobile application that finds gas prices near the consumer's location, shall not require the consumer to consent to incompatible uses (for example, the sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation data for providing the location-based service;

5. The methods shall be easy to execute. The controller shall not add unnecessary burden or friction to the process by which the consumer seeks to exercise opt-out rights. Methods shall be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request, for example:

i. The controller shall not require the 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;

[page=1110] ii. A controller that knows or should know of, but does not remedy, circular or broken links, or nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this paragraph; or

iii. A controller that requires the consumer to wait unnecessarily on a webpage as the controller processes a request may be in violation of this paragraph;

6. Exercising any one option shall not be more time-consuming or difficult than exercising any other option.

i. A choice to opt out or withhold consent shall not be presented with a less prominent size, font, or styling than a choice to opt in or provide consent.

ii. When seeking consent, a website banner that allows consumers to "accept all" in one step must also allow consumers to "decline all" in one step. A choice to opt in that provides "Yes" as an answer must also provide "No";

7. A consumer's silence or failure to take an affirmative action shall not be interpreted as acceptance or consent; for example:

i. A consumer closing a pop-up window that requests consent without first affirmatively selecting the equivalent of an "I accept" button shall not be interpreted as affirmative consent;

ii. A consumer navigating forward on a webpage after a consent choice has been presented without selecting the equivalent of an "I accept" button shall not be interpreted as affirmative consent; and

iii. A consumer continuing to use a "smart" TV, gaming console, or other device without replying the equivalent of "I accept" or "I consent" to a verbal request for consent shall not be interpreted as affirmative consent;

8. Choice options shall not be presented with a preselected or default option;

9. A consumer's expected interaction with a website, application, device, or product shall not be unnecessarily interrupted or intruded upon to request consent. Unnecessary interruptions include, but are not limited to:

i. Interrupting consumers with a request to consent if they have already declined the consent choice offered;

ii. Redirecting consumers away from the content or service they are attempting to interact with because they declined the consent choice offered, unless consent to process the requested data is strictly necessary to provide the website or application content or experience; and

iii. Forcing consumers to navigate through multiple pop-ups which cover or otherwise disrupt the content or service they are attempting to interact with because they declined the consent choice offered;

10. Consent choice options shall not include misleading statements, omissions, affirmative misstatements, or intentionally confusing language to obtain consent; and

11. The vulnerabilities or unique characteristics of the target audience of a product, service, or website shall be considered when deciding how to present choice options. For instance, when the target audience is children or senior citizens, the controller shall ensure that the choice options are appropriate given the vulnerabilities and unique characteristics of that target audience.

(b) A method that does not comply with (a) above shall be considered a dark pattern. The fact that a design or practice is commonly used is not a factor in whether any particular design or practice is a dark pattern.

(c) Any option chosen through the use of dark patterns shall not constitute valid consumer consent.

## SUBCHAPTER 2. CONSUMER DISCLOSURES

### 13:45L-2.1 Privacy notice required

(a) The purpose of the privacy notice required by this section is to provide consumers with a comprehensive description of a controller's online and offline information practices. The privacy notice shall inform consumers about the rights they have regarding their personal data and provide any information necessary for them to exercise those rights.

(b) A controller is not required to provide a separate New Jersey-specific privacy notice or section of a privacy notice, as long as the controller's privacy notice meets all requirements of this subchapter.

(c) A privacy notice shall:

1. Comply with the requirements for disclosures, notifications, and other communications to consumers at N.J.A.C. 13:45L-1.4;

2. Be available in a format that allows a consumer to print a paper copy; and

3. Enable a consumer to understand, at or before the point of collection of any personal data, the nature and scope of the controller's processing operations.

(d) A controller shall make the privacy notice required pursuant to (a) above readily available where consumers will encounter it at or before the point of collection of any personal data.

(e) If a controller does not give the privacy notice required pursuant to (a) above to the consumer at or before the point of collection of the consumer's personal data, the controller shall not collect personal data from the consumer.

(f) A controller's privacy notice shall comply with the requirements at N.J.A.C. 13:45L-2.2.

13:45L-2.2 Privacy notice content

(a) The privacy notice required pursuant to N.J.A.C. 13:45L-2.1 shall include a comprehensive description of the controller's online and offline personal data processing practices, including, but not limited to, the following:

1. The categories of the personal data that the controller processes. Categories shall be described in a level of detail that enables consumers to understand the type of personal data processed. For example, descriptions of personal data that are sufficiently granular to enable consumers to understand the type of personal data processed include "telephone number," "email address," "mailing address," "government issued identification numbers," "payment information," "IP address," "device ID," "username," "location," or "browsing history," "data revealing religious affiliation," or "medical data";

2. The purpose or purposes for processing personal data, consistent with the requirements set forth at N.J.A.C. 13:45L-6.1, and described in a level of detail that gives consumers a meaningful understanding of how each category is used when provided for that purpose. For example, descriptions of purposes for processing personal data that give consumers a meaningful understanding of how each category of personal data is used include "targeted advertising," "credit profiling," or "AI modeling";

3. The length of time the controller intends to retain each category of personal data identified at (a)1 above;

4. Whether the personal data identified at (a)1 above will be sold to or shared with third parties. If so:

i. The categories of personal data that the controller sells to or shares with third parties; and

ii. The categories of third parties to which the controller may disclose or sell a consumer's personal data. Categories of third parties must be described in a level of detail that enables the consumer to understand the type of, business model of, and processing conducted by the third party. For example, descriptions of third parties that are sufficiently granular to enable consumers to understand the type of third parties to which the controller may disclose a consumer's personal data include "analytics companies," "data brokers," "third-party advertisers," "payment processors," "lenders," and "government agencies";

5. A statement regarding whether the controller knowingly sells or shares the personal data of consumers under 16 years of age;

6. An explanation of the data rights at N.J.S.A. 56:8-166.10;

7. An explanation of how consumers may exercise their data rights, including:

i. Clear and conspicuous instructions as to the manner in which a consumer may exercise each data right, including any available links to an online form or portal for exercising data rights;

ii. Clear and conspicuous instructions on how an authorized agent may opt out of the processing of personal data on a consumer's behalf pursuant to N.J.S.A. 56:8-166.11(a);

iii. A description of the commercially reasonable process, which complies with the requirements at N.J.A.C. 13:45L-4.1(c), that the controller uses to authenticate the identity of a consumer exercising a data right or to authenticate the authority of an authorized agent exercising the right to opt out on a consumer's behalf;

[page=1111] iv. An explanation of how opt-out preference signals sent through universal opt-out mechanisms will be processed; and

v. How a consumer may appeal a controller's decision regarding the consumer's exercise of data rights;

8. The controller's contact information, including an active electronic mail address or other online mechanism that the consumer may use to contact the controller; and

9. The process by which the controller notifies consumers of material changes to the privacy notice required to be made available pursuant to N.J.A.C. 13:45L-2.3, along with the effective date of the notice.

(b) In addition to (a) above, a controller that processes personal data for profiling for a decision that produces legal or similarly significant effects concerning the consumer and subject to N.J.S.A. 56:8-166.10(a)5 shall include, at a minimum, the following in the privacy notice required at N.J.A.C. 13:45L-2.1:

1. The decisions to be made using profiling;

2. The categories of personal data that were or will be processed as part of the profiling in furtherance of decisions that produce legal or other similarly significant effects;

3. A plain language explanation of how the profiling software works;

4. A plain language explanation of how profiling is used in the decision-making process, including the role of human involvement, if any;

5. If the system has been evaluated for accuracy, fairness, or bias, including the impact of the use of sensitive data, and the outcome of any such evaluation;

6. The consequences of a decision based on profiling; and

7. Information about how a consumer may exercise the right to opt out of the processing of personal data for profiling in furtherance of decisions that produce legal or other similarly significant effects.

(c) Nothing at (b) above shall be construed to require a controller to provide information to a consumer in a manner that would disclose the controller's trade secrets.

13:45L-2.3 Changes to a privacy notice

(a) A controller shall notify consumers of material changes to a privacy notice. Such changes to a privacy notice shall be communicated to consumers in a manner by which the controller regularly interacts with consumers. Material changes include, but are not limited to, changes to:

1. Categories of personal data processed;

2. The purposes for which personal data is processed;

3. The name or ownership of the controller;

4. The act of or policies concerning the sharing of personal data with third parties;

5. Categories of third parties with whom personal data is shared; or

6. Methods by which consumers may exercise their data rights.

(b) If a change to a privacy notice triggers the consent requirements at N.J.A.C. 13:45L-7.1, the controller shall:

1. Obtain valid consent pursuant to N.J.A.C. 13:45L-7.2 prior to processing, sharing, or selling, as applicable, personal data collected before the change to the privacy notice, regardless of whether the consumer has previously consented to the processing, sharing, or sale of personal data; and

2. Otherwise comply with N.J.A.C. 13:45L-7.

13:45L-2.4 Notice of right to opt out

(a) A controller that sells personal data to third parties or processes personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer shall provide consumers a notice of their right to opt out, which shall comply with all requirements for disclosures and communications to consumers set forth at N.J.A.C. 13:45L-1.4.

(b) A controller shall provide the notice to opt out required at (a) above at or before the point of collection of personal data.

(c) A controller shall include the following in its notice of the right to opt out:

1. An explanation of the consumer's right to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects; and

2. Instructions on how the consumer can opt out.

i. If notice is provided online, include the interactive form by which the consumer can opt out, as required at N.J.A.C. 13:45L-3.2(c); or

ii. If the controller does not operate online, the notice shall explain the offline method by which the consumer can submit their request to opt out.

13:45L-2.5 Loyalty program notice

(a) Pursuant to N.J.S.A. 56:8-166.8, a controller may offer consumers discounts, loyalty programs, or other incentives for the processing or sale of the consumer's personal data, or to provide different services to consumers that are reasonably related to the value of the consumers' personal data.

(b) A controller maintaining a loyalty program pursuant to N.J.S.A. 56:8-166.8 shall:

1.Provide a notice of loyalty program at or before the point of program enrollment, either directly, or in the form of a link that takes the consumer directly to the specific section containing the information required at (e) below;

2. Allow consumers to withdraw from the loyalty program at any time; and

3. Offer loyalty program benefits that are reasonably related to the value of the consumer's personal data.

(c) The notice of loyalty program required at (b)1 above shall comply with all requirements for disclosures, notifications, and other communications to consumers provided at N.J.A.C. 13:45L-1.4.

(d) Pursuant to (b)3 above, if a controller is unable to calculate a good-faith estimate of the value of a consumer's personal data that forms the basis for offering a loyalty program benefit, or cannot show that the loyalty program benefit is reasonably related to the value of the consumer's personal data, the controller shall not offer the loyalty program benefit.

(e) A controller shall include the following in its notice of loyalty program:

1. A statement that the offered discounts, programs, incentives, or services include the sale or processing of personal data that the consumer may opt out of if the consumer chooses not to participate in the loyalty program;

2. An explanation of how the price or service difference associated with participating in the loyalty program is reasonably related to the value of the consumer's personal data, including:

i. A good-faith estimate of the value of the consumer's personal data that forms the basis for offering the price or service difference; and

ii. A description of the method or methods the controller used to calculate the value of the consumer's personal data;

3. The categories of personal data collected through the loyalty program, provided in the level of detail described at N.J.A.C. 13:45L-2.2(a)1 that will be sold or processed, if any;

4. Any third parties that will receive the consumer's personal data, provided in the level of detail described at N.J.A.C. 13:45L-2.2(a)4, including whether personal data will be provided to data brokers;

5. A statement that the consumer has the right to withdraw from the loyalty program at any time and how the consumer may exercise that right;

6. A list of any loyalty program partners, and the loyalty program benefits provided by each loyalty program partner;

7. A link to the controller's privacy notice pursuant to N.J.A.C. 13:45L-2.2;

8. If a controller claims that a consumer's decision to delete personal data makes it impossible to provide a loyalty program benefit, explain why the deletion of personal data makes it impossible to provide a loyalty program benefit; and

9. If a controller claims that a consumer's sensitive data is required for a loyalty program benefit, explain why the sensitive data is required for a loyalty program benefit.

(f) If a consumer refuses to consent to the processing of sensitive data necessary for a loyalty program benefit, the controller is not obligated to provide that loyalty program benefit. However, the controller shall provide any available loyalty program benefit for which the sensitive data is not necessary.

[page=1112] SUBCHAPTER 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

13:45L-3.1 Submitting requests to correct, access, and delete personal data, and data portability requests

(a) The privacy notice required pursuant to N.J.S.A. 56:8-166.6 must include specific methods through which a consumer may submit requests to exercise their data rights.

(b) Any method specified by a controller pursuant to N.J.S.A. 56:8-166.6(a)5 must:

1. Incorporate the ways in which consumers normally interact with the controller:

i. A controller shall provide two or more designated methods for submitting data right requests. One of those methods must be a toll-free telephone number;

ii. If a controller maintains a website, mobile application, or other digital presence, the controller shall allow consumers to submit requests through its website, mobile application, or digital interface, such as through a webform or online portal for submitting data portability requests and requests to correct, access, and delete personal data, or a link or button that consumers can click on that immediately effectuates the consumer's right to delete personal data; and

iii. If a controller interacts with consumers in person, the controller shall provide an in-person method, such as a printed form that the consumer can submit in person or send by mail; a tablet or computer portal that allows the consumer to complete and submit an online form; or a telephone that the consumer can use to call the controller's toll-free number;

2. Enable consumers to exercise their data rights at times that are reasonably convenient to the consumers; for example:

i. 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; or

ii. At any time if the controller uses a website, mobile application, or digital interface (such as a webform);

3. Comply with requirements for disclosures, notifications, and other communications to consumers provided at N.J.A.C. 13:45L-1.4;

4. Use data security measures that comply with N.J.A.C. 13:45L-6.4 when exchanging information to facilitate the exercise of a data right, considering the volume, scope, and nature of personal data that may be exchanged; and

5. Be consumer-friendly, clearly established, and easy to use by the average consumer, requiring the minimum number of steps necessary.

(c) The method of exercising a data right does not have to be specific to New Jersey, provided the method meets the requirements of this subchapter.

(d) A controller shall not require a consumer to create a new user account to exercise a data right; provided, however, that a controller may require a consumer to use an existing account to submit a verified request.

(e) A controller may only collect personal data in connection with a consumer's exercise of a data right if the personal data is necessary to effectuate the request.

(f) If a consumer seeks to exercise a data right using a method that is not one of the controller's designated methods or that is otherwise deficient in some manner unrelated to the verification process, the controller shall either:

1. Treat the attempt to exercise a data right as if it had been attempted in accordance with the controller's designated method or methods of submission; or

2. Respond with information on how to exercise the data right or remedy any deficiencies, as applicable, within the time frames set forth at N.J.A.C. 13:45L-3.3 and 3.4, as applicable.

(g) Data rights requests for a consumer under the age of 13 must be submitted by a parent or guardian. A controller shall establish, document, and comply with a reasonable method, in accordance with the methods set forth at N.J.A.C. 13:45L-7.4(c), for determining that a person exercising their right to delete, access, make portable, or correct the personal data of a consumer under the age of 13 on behalf of the consumer is the parent or guardian of that consumer. If, by employing this reasonable method, a controller cannot determine that the person submitting the request is the parent or guardian of the consumer under the age of 13, the controller shall not allow the person to exercise the data right on the consumer's behalf.

13:45L-3.2 Exercising the right to opt out

(a) A controller that processes personal data from consumers for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer shall allow consumers to opt out of the processing of personal data:

1. For the purposes of targeted advertising and the sale of personal data through an opt-out preference signal; and

2. For the purpose of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer through an opt-out preference signal, to the extent such technology exists.

(b) In addition to allowing consumers to exercise their right to opt out through an opt-out preference signal as required pursuant to (a) above, a controller that processes personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects must provide at least two clear and conspicuous methods for exercising the right to opt out.

(c) Acceptable methods for exercising the right to opt out of the processing of personal data required may include an interactive form accessible through a clear and conspicuous link on the controller's website or mobile application, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, or a universal opt-out preference signal.

(d) If a link is used pursuant to (c) above, the link must:

1. Be prominently displayed outside the controller's privacy notice;

2. Take a consumer directly to the opt-out method; and

3. Provide a clear understanding of its purpose, for example "Limit the Use of My Personal Data," "Do Not Sell or Share My Personal Data," "Your Privacy Choices," or "Your New Jersey Privacy Choices."

(e) A controller that interacts with consumers in person and online shall provide an in-person method for exercising the right to opt out of the processing of personal data for each of the purposes for which the controller processes personal data, in addition to the requirements at (b) above.

(f) A controller's methods for opting out of the processing of personal data shall comply with the requirements at N.J.A.C. 13:45L-1.5.

13:45L-3.3 Responding to consumer requests

(a) No later than 10 business days after receiving a request to exercise a data right, a controller who has not yet effectuated the request shall confirm receipt of the request and provide information about how the controller will effectuate the request. The information provided shall:

1. Describe the controller's verification process; and

2. State when the consumer should expect a response, except in instances where the controller has already granted or denied the request.

(b) A controller shall respond to a request to exercise a data right no later than 45 calendar days after the receipt of the verified request; provided, however, that the controller shall comply with a consumer's opt-out request in accordance with N.J.A.C. 13:45L-3.4(a)1 and 2. A controller may extend the response period for an access, correction, data portability, or deletion request by up to 45 additional days, where reasonably necessary, considering the number and complexity of the consumer's request, provided that the controller:

1. Informs the consumer of any such extension within the initial 45-day response period;

2. Explains the reason for the extension; and

3. If applicable, provides the requested information for all disclosures of personal data that occurred in the prior 12 months.

(c) If a controller declines to take action on a consumer's request to exercise a data right, the controller shall respond to the consumer without undue delay, but not later than 45 days after receipt of the request, with instructions on how to appeal the denial pursuant to N.J.S.A 56:8-166.7(f) and the grounds for denial, including:

1. If the controller relied on an exception at N.J.S.A. 56:8-166.15, a description of the exception;

2. If the controller was unable to authenticate the consumer's identity, the reasons why the controller was unable to do so;

[page=1113] 3. Any factual basis for the controller's good-faith, reasonable, and documented belief that compliance is impossible; or

4. Any factual basis for a good-faith, reasonable, and documented belief that the request is fraudulent or abusive.

(d) If a controller denies a consumer request based on its inability to authenticate the request, the controller must describe in the documentation required pursuant to N.J.A.C. 13:45L-6.5, its reasonable efforts to authenticate the request and explain why it was unable to do so.

(e) Pursuant to N.J.S.A. 56:8-166.16(b)1, when a controller complies with a consumer's data right request, the controller shall also use technical, organizational, or other measures or processes set forth in the contract required pursuant to N.J.S.A. 56:8-166.16(e), to instruct the processors that process personal data on the controller's behalf to fulfill requests relating to personal data held by the processors.

(f) Information provided in response to a consumer request shall be provided by a controller, free of charge, once per consumer during any 12-month period.

(g) If requests from a consumer are manifestly unfounded, excessive, or repetitive, a controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller shall bear the burden of demonstrating that the request is manifestly unfounded, excessive, or repetitive. For the purpose of this section, "reasonable fee" means the fee charged does not exceed the actual cost to the controller of providing information or taking the requested action, provided such cost is reasonable and the controller has taken reasonable efforts to mitigate the actual cost. When determining the actual cost of compliance, a controller shall be limited to those expenses that would generally be recognized as ordinary and necessary to comply with a request, such as:

1. Compensation of employees' time specifically related to complying with the request;

2. Computer system expenses specifically related to complying with the request; and

3. Costs of material acquired, consumed, or expended specifically for the purpose of complying with the request.

(h) Controllers must maintain all documentation required pursuant to N.J.A.C. 13:45L-6.

13:45L-3.4 Right to opt out

(a) When a consumer exercises the right to opt out, a controller shall:

1. Refrain from processing the consumer's personal data for the opt-out purpose, or purposes, if the controller has yet to process any of the consumer's personal data;

2. Cease processing the consumer's personal data for the opt-out purpose, or purposes, as soon as possible, but no later than 15 days from the date the controller receives the request, and delete any of the consumer's personal data processed for the opt-out purpose, or purposes, after the consumer exercised the right to opt out;

3. Use technical, organizational, or other appropriate measures or processes set forth in the contract required pursuant to N.J.S.A. 56:8-166.16(e) to ensure that the processors that process personal data on the controller's behalf stop processing the personal data, as needed, to effectuate the consumer's choice to opt out;

4. 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; and

5. Maintain a record of the consumer's choice to opt out and the controller's response, in compliance with N.J.A.C. 13:45L-6.5.

(b) After receiving an online opt-out request from a consumer, a controller may request additional information from the consumer if it is necessary to opt the consumer out of the processing of offline or other personal data. The controller must comply with N.J.A.C. 13:45L-4.1 and 5.1 when requesting the additional information.

(c) If a consumer submits a request to exercise more than one data right and a controller is able to fulfill the opt-out request in a more timely manner than other data right requests, the controller shall complete the opt-out request prior to any other data right request.

(d) A controller may deny an opt-out request if the controller has a good faith, reasonable, and documented belief that such request is fraudulent. If a controller denies an opt-out request because the controller believes such request is fraudulent, the controller shall send a notice to the person who made such request, stating the following:

1. The controller believes the request is fraudulent;

2. Why the controller believes the request is fraudulent; and

3. That the controller shall not comply with the request.

(e) A consumer may use an authorized agent to opt out on the consumer's behalf if the consumer expressly confirms that the authorized agent may act on the consumer's behalf. A controller may deny a request from an authorized agent if the agent does not provide to the controller the consumer's express permission demonstrating that the consumer has authorized the agent to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made through an opt-out preference signal.

(f) A controller shall wait at least 12 months from the date that a consumer choses to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer before asking the consumer to consent to such processing.

13:45L-3.5 Right of access

(a) When granting a consumer's access request, the controller shall confirm whether it processed the consumer's personal data and provide the consumer with any personal data that it has collected that falls within the scope of the request, including any personal data that a processor obtained from the controller in providing services to the controller; provided that nothing in this section shall require a controller to provide data to the consumer in a manner that would reveal the controller's trade secrets.

(b) Personal data provided in response to an access request must:

1. Be provided in a form that is concise, transparent, and easily intelligible and in an appropriate, commonly used electronic format;

2. Be available in the language in which the consumer interacts with the controller;

3. Avoid internal codes and include explanations that would allow the average consumer to make an informed decision of whether to exercise their right to portability, deletion, correction, or opt out; and

4. Be in compliance with the requirements for disclosures, notifications, and other communications provided at N.J.A.C. 13:45L-1.4.

(c) In responding to an access request, a controller shall not be required to disclose a consumer's government-issued identification number, financial account number, health insurance or medical identification numbers, account password, security questions and answers, biometric data, or biometric identifiers. The controller shall, however, inform the consumer that it has collected the type of information that is the subject of the access request.

(d) A controller shall implement and maintain data security measures that comply with N.J.A.C. 13:45L-6.4 in processing any documentation relating to a consumer's access request.

### 13:45L-3.6 Right to correct

(a) When granting a consumer's correction request, the controller shall correct the consumer's personal data in its systems. The controller shall also use technical, organizational, or other appropriate measures or processes set forth in the contract required pursuant to N.J.S.A. 56:8-166.16(e) to ensure that the processors that process personal data on the controller's behalf make the necessary corrections in their respective systems.

(b) If a consumer seeks to exercise their right to correct personal data and the requested correction could be made by the consumer through the consumer's account settings, a controller may respond to the consumer's request by providing instructions on how the consumer may correct the personal data, so long as:

1. The correction process is not unduly burdensome to the consumer;

2. The instructions meet all requirements at N.J.A.C. 13:45L-1.4;

3. The controller's response is compliant with the timing requirements set forth at N.J.A.C. 13:45L-3.3; and

[page=1114] 4. The process described in the instructions enables the consumer to make the requested correction.

(c) A controller may require a consumer to provide documentation, if necessary, to determine whether the personal data, or the consumer's requested correction to the personal data, is accurate if the controller has a good faith, reasonable, and documented belief that the correction is not accurate. When requesting documentation, the controller must explain to the consumer why the documentation is necessary.

(d) A controller shall not process any documentation provided by a consumer in connection with the consumer's correction right for any purpose other than determining the accuracy of the consumer's personal data or requested correction. The controller shall delete such documentation immediately after determining the accuracy of the consumer's personal data or requested correction.

(e) A controller shall implement and maintain data security measures that comply with N.J.A.C. 13:45L-6.4 in processing any documentation relating to the consumer's correction request.

(f) If the controller did not receive the personal data directly from the consumer and has inadequate documentation to support the accuracy of the personal data, the consumer's assertion of inaccuracy shall be sufficient to establish that the personal data is inaccurate.

(g) A controller may decide not to act upon a consumer's correction request only if the controller has exhausted the step at (c) above and determined that the contested personal data is likely accurate.

(h) If a controller declines to take action upon a consumer's correction request based on the controller's determination that the contested personal data is likely accurate, the controller must describe in the documentation required pursuant to N.J.A.C. 13:45L-6.5(a):

1. The consumer's requested correction to the personal data;

2. Any documentation requested from and provided by the consumer in support of the correction request; and

3. The reason for the controller's determination that the consumer's documentation provided pursuant to (c) above was not sufficient to support the consumer's position.

13:45L-3.7 Right to deletion

(a) When a consumer exercises the right to deletion, the controller shall:

1. Delete the consumer's personal data;

2. Using technical, organizational, or other measures or processes set forth in the contract required pursuant to N.J.S.A. 56:8-166.16(e), instruct the processors that process personal data on the controller's behalf to delete the consumer's personal data held by the processors; and

3. Notify 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.

(b) A processor shall, with respect to personal data that it holds pursuant to a written contract with the controller and upon notification by the controller, comply with a request to delete.

(c) In responding to a request to delete, a controller shall inform the consumer whether it has complied with the consumer's request. The controller shall also 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 pursuant to N.J.S.A. 56:8-166.10(b)(1).

(d) If a controller declines to take action on a consumer's request to delete, in whole or in part, the controller shall:

1. Unless prohibited from doing so by law, provide the consumer with a detailed explanation of the basis for the denial, including whether the controller relied on an exception at N.J.S.A. 56:8-166.15;

2. If the controller relied on an exception at N.J.S.A. 56:8-166.15:

i. Delete the consumer's personal data that is not subject to the applicable exception; and

ii. Refrain from using the consumer's personal data for any purpose other than that provided for by the applicable exception; and

3. Instruct the processors that process personal data on the controller's behalf to delete the consumer's personal data that is not subject to the applicable exception and to refrain from using the consumer's personal data retained for any purpose other than the purpose provided for by the applicable exception.

(e) If a controller denies a consumer's request to delete, and processes personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer, and the consumer has not already chosen to opt out of the processing of personal data for one or more of these purposes, the controller shall:

1. Ask the consumer if the consumer would like to opt out of the processing of personal data for one or more of these purposes; and

2. Include either the contents of, or a link to, the notice of right to opt out of the processing of the consumer's personal data for one or more of these purposes in accordance with N.J.A.C. 13:45L-2.4.

(f) A controller that has obtained personal data about a consumer from a source other than the consumer shall comply with a consumer's deletion request with respect to that personal data pursuant to N.J.S.A. 56:8-166.10(b) by:

1. Retaining a record of the deletion request and the minimum data necessary to ensure the consumer's personal data remains deleted from the controller's records, provided that such data shall not be used for any other purpose; or

2. Deleting such personal data.

13:45L-3.8 Right to data portability

(a) To comply with a data portability request, a controller shall transfer to a consumer the personal data it has collected and holds about the consumer through a secure method in a commonly used electronic format that, to the extent technically feasible, allows the consumer to transmit the personal data to another entity without hindrance.

(b) In responding to a data portability request, a controller is not required to provide personal data to a consumer in a manner that would disclose its trade secrets. When complying with a request to access personal data in a portable format, controllers must provide as much data as possible in a portable format without disclosing the trade secret.

(c) If a consumer exercises the right to access their personal data in a portable format pursuant to N.J.S.A. 56:8-166.10(a)4 and the controller determines that the manner of response would reveal the controller's trade secrets, the controller shall provide access to that information in a format or manner which would not reveal trade secrets, such as in a nonportable format.

SUBCHAPTER 4. VERIFICATION OF REQUESTS

13:45L-4.1 General rules regarding verification

(a) A controller shall use commercially reasonable methods for authenticating the identity of every consumer submitting a request to delete, request to correct, data portability request, or access request, and the authority of an authorized agent submitting an opt-out request on behalf of a consumer pursuant to N.J.S.A. 56:8-166.11(a).

(b) A controller shall not require a consumer to authenticate their identity to opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. A controller may ask the consumer for information necessary to effectuate the right to opt out; however, it shall not be unduly burdensome to the consumer. For example, a controller may ask the consumer for their username, but it shall not require the consumer to submit their driver's license, together with a photo of themselves.

(c) To determine if an authentication method is commercially reasonable, the controller shall consider:

1. The type, sensitivity, and value of the personal data collected and maintained about the consumer;

2. The risk of harm to the consumer posed by any unauthorized deletion, correction, or access to their personal data. A greater risk of harm to the consumer by unauthorized deletion, correction, or access shall warrant a more stringent verification process;

3. The likelihood that malicious actors would seek the personal data. The higher the likelihood, the more stringent the verification process shall be;

4. Whether the personal data to be provided by the consumer to verify their identity sufficiently protects against fraudulent requests;

[page=1115] 5. The manner in which the controller interacts with the consumer (for example, whether the controller interacts with the consumer online or over the phone); and

6. Available technology for verification.

(d) In addition to (c) above, in determining the method by which a controller will authenticate a consumer's identity, a controller shall:

1. Match the identifying information provided by the consumer to the personal data of the consumer already maintained by the controller, or use an identity verification service that complies with this subchapter;

2. Avoid authentication methods that place an unreasonable burden on the consumer seeking to exercise their data rights, or on an authorized agent opting out on behalf of a consumer; and

3. Refrain from requesting additional personal data to authenticate a consumer unless the controller cannot authenticate the consumer using the personal data already maintained by the controller or its processors.

(e) Personal data obtained to authenticate a consumer may only be used to authenticate the consumer submitting the data right request, or to authenticate an authorized agent's authority, and must be deleted as soon as practicable after processing the consumer's request, except as required pursuant to N.J.A.C. 13:45L-6.5, or as otherwise required.

(f) A controller shall implement security measures, consistent with N.J.A.C. 13:45L-6.4, to protect personal data exchanged to authenticate a consumer or to authenticate an authorized agent's authority, considering the type, value, sensitivity, and volume of information exchanged and the level of possible harm improper access or use could cause to the consumer submitting a data right request.

(g) A controller shall implement security measures to detect fraudulent identity-verification activity and prevent the unauthorized deletion, correction, or access of a consumer's personal data.

(h) Except as provided at N.J.A.C. 13:45L-3.3(g), a controller shall not require the consumer or authorized agent to pay a fee for authentication, or require the consumer to incur a cost (such as, for example, the cost of a notarized affidavit) unless the controller compensates the consumer for the cost.

(i) For requests to correct, a controller shall use best efforts to authenticate the consumer, based on personal data that is not the subject of the request to correct.

(j) If a controller cannot authenticate the consumer seeking to exercise a data right using commercially reasonable efforts pursuant to (c) above, the controller shall not be required to grant the consumer's request, and the controller shall:

1. Inform the consumer that their identity could not be authenticated; and

2. Provide information on how the consumer can remedy any deficiencies.

(k) A controller who cannot authenticate the consumer seeking to exercise a data right using commercially reasonable efforts pursuant to (c) above may request additional personal data, if necessary to authenticate the consumer.

13:45L-4.2 Verification for password-protected accounts

If a controller suspects fraudulent or malicious activity on or from a password-protected account, the controller shall not comply with a consumer's request to delete, request to correct, data portability request, or access request until further authentication procedures determine that the consumer request is authentic and the requestor is the consumer about whom the controller has collected information or the consumer's authorized agent. The controller shall use the procedures set forth at N.J.A.C. 13:45L-4.3 to further verify the identity of the consumer.

13:45L-4.3 Verification for non-account holders

(a) This section shall apply only when a consumer does not have or cannot access a password-protected account with a controller, in which case, the controller shall comply with this section and with N.J.A.C. 13:45L-4.1, or when a controller seeks to verify the identity of a consumer pursuant to N.J.A.C. 13:45L-4.2.

(b) A controller who receives an access request seeking to know categories of personal data shall authenticate the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty shall include matching at least two data points provided by the consumer with data points maintained by the controller for the purpose of authenticating the consumer. The controller shall determine that the data points provided by the consumer and the data points maintained by the controller are reliable before using the data points for this purpose.

(c) A controller who receives an access request requesting to know specific personal data points shall verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty shall include matching at least three pieces of personal data provided by the consumer with personal data maintained by the controller for the purpose of authenticating the consumer. The controller shall determine that the personal data provided by the consumer and the personal data maintained by the controller are reliable before using them for this purpose.

(d) A controller who receives a request to delete or a request to correct data shall verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal data and the risk of harm to the consumer posed by unauthorized deletion or correction.

(e) A controller shall deny an access request if it cannot authenticate the identity of the requestor pursuant to this section.

(f) If there is no reasonable method by which a controller can authenticate the identity of a consumer to the degree of certainty required by this section, the controller shall state as much in response to any request and explain why there is no reasonable method by which it can authenticate the identity of the requestor. The controller shall evaluate and document whether such a reasonable method exists at least once every 12 months.

13:45L-4.4 Authorized agents

(a) If a consumer uses an authorized agent to exercise a data right, a controller may require the authorized agent to provide proof that the consumer gave the agent signed permission to do so.

(b) Notwithstanding (a) above, when a consumer has provided the authorized agent with power of attorney pursuant to N.J.S.A. 46:2B et seq., the controller shall not require the authorized agent to provide proof of signed permission to submit a request; provided, however, that a controller shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

(c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.

(d) An authorized agent shall not use a consumer's personal data, or any information collected from or about the consumer, for any purpose other than verification, fraud prevention, or fulfilling the consumer's request.

SUBCHAPTER 5. UNIVERSAL OPT-OUT MECHANISM

13:45L-5.1 Universal opt-out mechanism requests

(a) Pursuant to N.J.S.A. 56:8-166.11(b), a controller that processes personal data for the 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.

(b) A controller that processes personal data for the purposes of targeted advertising or the sale of personal data shall comply with the choice to opt out of such processing that is transmitted through a universal opt-out mechanism that meets the requirements at N.J.A.C. 13:45L-5.2.

(c) When a controller that collects personal data from consumers online receives or detects an opt-out preference signal from a universal opt-out mechanism that meets the requirements at N.J.A.C. 13:45L-5.2:

1. The controller shall treat the opt-out preference signal 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 browser, network, or device(s), and any consumer profile associated with that browser, network, or device(s), including pseudonymous profiles. The controller shall not:

i. Charge a fee or require any valuable consideration for complying with the opt-out preference signal;

ii. Change the consumer's experience with the product or service offered by the controller. For example, a consumer who uses an opt-out preference signal shall have the same experience with regard to how the [page=1116] controller's product or service functions compared to a consumer who does not use an opt-out preference signal; and

iii. Display a notification, pop-up, text, graphic, animation, sound, video, or any other interstitial content that degrades or obstructs the consumer's experience on the controller's web page or application in response to the opt-out preference signal.

2. The controller shall not require additional personal data beyond that which is strictly necessary to:

i. Authenticate that a consumer is a resident of New Jersey; or

ii. Determine that the opt-out preference signal represents a legitimate request to opt out of the processing of personal data as permitted pursuant to N.J.S.A. 56:8-166.11(b).

3. If the opt-out preference signal conflicts with a consumer's controller-specific privacy setting that allows the controller to sell or share their personal data, the controller shall comply with the opt-out preference signal to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or both; provided, however, that the controller may notify the consumer of the conflict and give the consumer an opportunity to consent to the sale or sharing of their personal data. The controller shall comply with N.J.A.C. 13:45L-7.1 in obtaining the consumer's consent to the sale or sharing of personal data. The controller's notification must clearly inform the consumer that the consumer does not need to provide consent in order to continue receiving a good or service. If the consumer consents to the sale or sharing of personal data after being notified, the controller may ignore the opt-out preference signal unless the consumer withdraws such consent; and

4. If the opt-out preference signal conflicts with the consumer's participation in a controller's loyalty program that requires the consumer to consent to the sale or sharing of personal data, the controller may notify the consumer that complying with the opt-out preference signal to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or both, would withdraw the consumer from the loyalty program and ask the consumer to affirm that they intend to withdraw from the loyalty program.

i. If the consumer affirms that they intend to withdraw from the loyalty program, the controller shall comply with the opt-out preference signal to opt out of the processing of personal data for purposes of targeted advertising, the sale of personal data, or both.

ii. If the controller asks whether the consumer intends to withdraw from the loyalty program, and the consumer does not affirm their intent to withdraw, the controller may ignore the opt-out preference signal with respect to that consumer's participation in the loyalty program for as long as the consumer is known to the controller.

iii. If the controller does not ask the consumer to affirm their intent to withdraw from the loyalty program, the controller shall comply with the opt-out preference signal to opt out of the processing of personal data for purposes of targeted advertising, or the sale of personal data, or both, for that browser, network, or device(s) and any consumer profile the controller associates with that browser, network, or device(s).

(d) Notwithstanding (c)2 above, a controller shall give the consumer an option to provide additional personal data to extend the recognition of the consumer's use of the universal opt-out mechanism across platforms, devices, or offline.

1. Any information provided by the consumer for this purpose shall not be used, disclosed, or retained for any purpose other than extending the recognition of the consumer's use of the universal opt-out mechanism across platforms, devices, or offline; and

2. If the consumer does not respond, the controller shall process the opt-out preference signal as a valid request to opt out of processing for that browser, network, or device(s) and any consumer profile the controller associates with that browser, network, or device(s), including pseudonymous profiles.

(e) After receiving a valid opt-out signal through the use of a universal opt-out mechanism, a controller shall continue to comply with the signal until the consumer consents to the processing of personal data for purposes of targeted advertising or the sale of personal data, as specified at N.J.A.C. 13:45L-7.5.

13:45L-5.2 Technical specification

(a) A universal opt-out mechanism must:

1. Allow for consumers to automatically communicate their opt-out choice with multiple controllers;

2. Clearly describe any limitations that may be applicable to the mechanism, including, for example, that the mechanism:

i. Allows a consumer to exercise the opt-out right for one specific purpose only (that is, either targeted advertising or the sale of personal data); or

ii. Applies only to a single browser or device;

3. Comply with the requirements for disclosures, notifications, and other communications to consumers as set forth at N.J.A.C. 13:45L-1.4;

4. Store, process, and transmit any consumer personal data using data security measures that comply with N.J.A.C. 13:45L-6.4;

5. Not prevent the controller from determining:

i. Whether a consumer is a resident of this State; or

ii. That the universal opt-out mechanism represents a legitimate request to opt out of the processing of personal data;

6. Not permit its manufacturer to unfairly disadvantage another controller;

7. 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;

8. Be consumer-friendly, clearly described, and easy to use by the average consumer; and

9. Be as consistent as possible with any other similar platform, technology, or mechanism required by any Federal or State law or regulation.

(b) A universal opt-out mechanism must communicate a consumer's opt-out preference by sending an opt-out preference signal. The signal must be in a format commonly used and recognized by controllers.

(c) A universal opt-out mechanism shall not use, disclose, or retain any personal data collected from a consumer in connection with the sending or processing of a choice to opt out for any purpose other than sending or processing the opt-out preference signal.

SUBCHAPTER 6. DUTIES OF CONTROLLERS

13:45L-6.1 Purpose specification

(a) Pursuant to N.J.S.A. 56:8-166.12(a)8, a controller shall specify the purposes for which it processes personal data.

(b) The purpose must be disclosed before the collection of a consumer's personal data.

(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.

(d) If personal data is collected and processed for more than one purpose, a controller must specify each purpose with enough detail to allow consumers to understand each purpose. 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.

13:45L-6.2 Restrictions on the use of personal data

(a) Pursuant to N.J.S.A. 56:8-166.12(a)2, except as otherwise provided in the Act, a controller shall not process personal data for purposes that are neither reasonably necessary to or compatible with the purposes disclosed to a consumer before collection, unless the controller obtains the consumer's consent as required pursuant to N.J.A.C. 13:45L-7.

(b) When considering whether a new processing purpose is reasonably necessary to or compatible with the purposes disclosed to a consumer at or before the point of collection, a controller shall consider the following, as applicable:

1. The expectations of an average consumer concerning how their personal data would be processed once it was collected;

2. The link between the original specified purpose or purposes for which the data was collected and the purpose or purposes of further processing;

3. The relationship between the consumer and the controller and the context in which the personal data was collected;

[page=1117] 4. The type, nature, and amount of the personal data subject to the new processing purpose;

5. The type and degree of possible consequence or impact to the consumer of the new processing purpose;

6. The identity of the entity conducting the new processing purposes, for example, the same or different controller, or a third party; and

7. The existence of additional safeguards for the personal data, such as encryption or pseudonymization.

13:45L-6.3 Data minimization

(a) Pursuant to N.J.S.A. 56:8-166.12(a)1, a controller shall 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.

(b) As part of its compliance with N.J.S.A. 56:8-166.12(a)(1), a controller shall, at a minimum, document its efforts to:

1. Consider each processing purpose and determine the minimum personal data that is necessary for the specific purpose or purposes, as disclosed to the consumer;

2. Create, establish, update, and maintain a data inventory documenting the types of data that the controller possesses, where the data is stored, and who has access to the data;

3. Keep the consumer's personal data in a form which allows for the identification of consumers for no longer than is necessary for the processing purpose or purposes;

4. Delete, and instruct any processors with which the controller has shared the personal data, to delete any personal data that is no longer necessary for the specific processing purpose or purposes;

5. At least once a year, assess 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 held by a controller is still necessary for the specific processing purpose or purposes, and document such assessment consistent with N.J.A.C. 13:45L-8;

6. After a consumer revokes consent to process the consumer's personal data, immediately delete sensitive data concerning the consumer for which the controller no longer has consent to process, control, possess, sell, or share; and

7. If collecting, using, or retaining personal data pursuant to N.J.S.A. 56:8-166.15(b), assess why the collection, use, or retention of such data is covered pursuant to N.J.S.A. 56:8-166.15(b).

(c) A controller shall not collect personal data unless it falls within one or more of the categories of personal data identified in the privacy notice pursuant to N.J.A.C. 13:45L-2.2(a)1. If a controller intends to collect personal data that does not fall within one or more of those categories of personal data, it shall revise the privacy notice and notify consumers of the change pursuant to N.J.A.C. 13:45L-2.3.

(d) A controller shall not collect personal data for any purpose other than the purpose or purposes for processing personal data identified in the privacy notice pursuant to N.J.A.C. 13:45L-2.2(a)2. If a controller intends to collect personal data for a purpose other than the purpose or purposes identified in the privacy notice, it shall revise the privacy notice and notify consumers of the change pursuant to N.J.A.C. 13:45L-2.3.

(e) A controller shall not retain personal data for longer than the length of time identified in the privacy notice pursuant to N.J.A.C. 13:45L-2.2(a)3. If a controller intends to retain personal data for longer than that length of time, it shall revise the privacy notice and notify consumers of the change pursuant to N.J.A.C. 13:45L-2.3.

(f) To ensure that the personal data is not kept longer than necessary, a controller shall set reasonable, specific time limits for erasure or for conducting a periodic review.

(g) A controller shall not require a consumer who exercises a data right to provide any information that is not necessary to locate the consumer's personal data in the controller's data systems.

13:45L-6.4 Duty of care

(a) Pursuant to N.J.S.A. 56:8-166.12(a)3, controllers must establish, implement, update, maintain, and document data security practices to protect the confidentiality, integrity, and accessibility of personal data and to secure personal data during both storage and use from unauthorized acquisition.

(b) When determining appropriate data security safeguards, controllers shall consider:

1. Applicable industry standards and frameworks;

2. The nature, size, and complexity of the controller's organization;

3. The sensitivity and amount of personal data;

4. The original source of personal data (for example, whether the data came directly from a consumer or from a third-party data broker); and

5. The risk of harm to consumers resulting from unauthorized or unlawful access, use, or degradation of the personal data.

(c) When determining appropriate data security safeguards, controllers may consider the burden or cost of safeguards to protect personal data.

(d) Appropriate data security safeguards shall be designed to:

1. Protect against access without authorization or in excess of authorization to personal data, servers, networks, hardware, and software used for processing;

2. Protect against accidental loss, destruction, or damage of personal data and equipment used for processing;

3. Ensure the confidentiality, integrity, accessibility, and availability of personal data collected, stored, and processed;

4. Identify and protect against threats to data security and the integrity and confidentiality of personal data; and

5. Oversee compliance with data security policies by the controller and processors through reasonable requirements.

13:45L-6.5 Recordkeeping

(a) A controller shall maintain records of all data rights requests made pursuant to N.J.S.A. 56:8-166.10(a) for at least 24 months. Such records shall include, at a minimum, each of the following:

1. The date of the request;

2. A copy of the data rights request;

3. The data rights request type;

4. The date of the controller's response;

5. The substance of the controller's response;

6. If a request is denied in whole, or in part, the basis for the denial of the request; and

7. The existence and resolution of any consumer appeal to a denied request.

(b) For requests to delete personal data that the controller has lawfully obtained from a source other than the consumer, a controller shall either:

1. Retain a record of the request and the minimum necessary information listed at (a) above; or

2. Delete such personal data pursuant to N.J.S.A. 56:8-166.10(b)(2).

(c) Records made pursuant to (a) above shall be made available at the completion of a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of personal data to ensure any new controller continues to recognize the consumer's previously exercised data rights.

(d) A controller shall maintain records sufficient to demonstrate compliance with N.J.A.C. 13:45L-6.2, 6.3, 6.4, and 7.3 for as long as the processing activity continues, and for at least 24 months after the conclusion of processing activity.

(e) Required records shall be maintained in a readable format, appropriate to the sophistication and size of the controller's business.

(f) Personal data maintained pursuant to this subchapter, where that information is not used for any other purpose, shall not be subject to data rights requests.

(g) Personal data maintained for recordkeeping purposes shall not be used for any other purpose except as necessary for the controller to review and modify its processes for complying with the Act and this chapter. Personal data maintained for recordkeeping purposes shall not be shared with any third party, except as necessary to comply with a legal obligation or as part of a merger, acquisition, bankruptcy, or other transaction in which a third party assumes control of personal data.

(h) Other than as required pursuant to (a) above and N.J.A.C. 13:45L-3.6, a controller is not required to retain personal data solely for the purpose of fulfilling a data rights request made pursuant to the Act.

[page=1118] (i) The controller shall implement, update, and maintain data security measures that comply with N.J.A.C. 13:45L-6.4 in maintaining all required records.

## SUBCHAPTER 7. CONSENT

### 13:45L-7.1 Consent required

(a) Pursuant to N.J.S.A. 56:8-166.12(a), a controller must obtain valid consent prior to:

1. Processing a consumer's sensitive data;

2. Processing personal data for purposes that are neither reasonably necessary to, nor compatible with, the purposes for which such personal data is processed, as previously

disclosed to the consumer;

3. Processing the personal data of a consumer for purposes of targeted advertising, the sale of the consumer's personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer, where the controller has actual knowledge, or willfully disregards, that the consumer is at least 13 years of age, but younger than 17 years of age; and

4. Selling a consumer's personal data, processing a consumer's personal data for targeted advertising, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer after the consumer has exercised the right to opt out of the processing for those purposes.

(b) A controller may rely upon valid consent obtained prior to (the effective date of this rulemaking), to continue to process a consumer's previously collected personal data collected before (the effective date of this rulemaking). Consent obtained before (the effective date of this rulemaking), shall be considered valid only if it would comply with the requirements set forth in this subchapter.

(c) If a controller has collected personal data prior to (the effective date of this rulemaking), and the processing purpose changes after (the effective date of this rulemaking), such that the new purpose is neither reasonably necessary to, nor compatible with, the purposes for which such personal data was processed, as disclosed to the consumer, the controller must obtain valid consent before the time the processing purpose changes to continue to process the previously collected personal data.

13:45L-7.2 Requirements for valid consent

(a) Valid consent must:

1. Be obtained through the consumer's clear, affirmative action:

i. For purposes of this section, "clear, affirmative action" means a consumer's consent is communicated either through deliberate and clear conduct, or through a selection that clearly indicates acceptance of the proposed processing or sale of their personal data. A blanket acceptance of general terms and conditions, silence, inactivity or inaction, pre-ticked boxes, and other negative option opt-out constructions that require intervention from the consumer to prevent agreement are not clear, affirmative actions for the purposes of valid consent;

2. Be freely given by the consumer. Consent is freely given when consumers may refuse consent without detriment and withdraw consent without undue burden at any time. Consent is not freely given when:

i. It reflects acceptance of general terms of use that contain descriptions of personal data processing together with unrelated information;

ii. The performance of a contract depends on consent to process personal data that is not necessary to provide the goods or services contemplated by the contract; or

iii. The controller denies goods, services, discounts, or promotions to a consumer who chooses not to provide consent, unless the personal data is necessary to the provision of those goods, services, discounts, or promotions or the consent is otherwise required in connection with a consumer's voluntary participation in a loyalty program;

3. Be specific:

i. When controllers request consent to process personal data for more than one processing purpose, and those processing purposes are not reasonably necessary to one another, consumers must have the ability to consent or not consent to each purpose separately;

ii. Controllers may request consent to process personal data for multiple processing purposes that are not reasonably necessary to or compatible with one another using a single consent request only if there is also an option for a more granular consent within the same consent interface;

iii. Consent to process personal data for one purpose does not constitute valid consent to process personal data for other purposes; and

iv. Consent to the sale of sensitive data to one specific party does not imply consent to the sale of sensitive data to any other party;

4. Reflect the consumer's unambiguous agreement; and

5. Provide the information required pursuant to N.J.A.C. 13:45L-7.3(c).

13:45L-7.3 Request for consent

(a) Pursuant to N.J.S.A. 56:8-166.12, a controller shall provide a simple form or mechanism to enable a consumer to provide consent. Such form or mechanism shall be readily accessible to the consumer and comply with the requirements of this subchapter.

(b) Requests for consent shall be prominent, concise, and separate and distinct from other terms and conditions, and shall comply with all requirements for disclosures and communications to consumers as set forth at N.J.A.C. 13:45L-1.5.

(c) A controller's request for consent must provide the following information:

1. The controller's identity;

2. The reason that consent is required explained in plain language;

3. The processing purpose or purposes for which consent is sought which shall comply with the requirements set forth at N.J.A.C. 13:45L-6.1;

4. The categories of personal data that the controller shall process to effectuate the processing purpose or purposes;

5. The names of any third parties receiving sensitive data through sale; and

6. An explanation of the consumer's right to withdraw consent for the processing purpose or purposes at any time in accordance with N.J.A.C. 13:45L-7.6 and an explanation of the method or methods through which the consumer may exercise that right.

(d) A controller must provide the disclosures required pursuant to (c) above on the request interface itself.

13:45L-7.4 Consumers under the age of 13

(a) A controller that has actual knowledge that it collects or processes the personal data of a consumer younger than 13, or that directs its activities at children and collects personal data from children, must obtain consent from the parent or lawful guardian of the consumer before collecting or processing the consumer's personal data. For instance, a controller must obtain consent from a parent or lawful guardian when the controller:

1. Engages in processing activities involving the collection and processing of personal data from a consumer younger than 13; or

2. Operates a website or business directed to consumers younger than 13.

(b) A controller that processes the personal data of consumers younger than 13 must make reasonable efforts to ensure that a parent or legal guardian of a child receives notice of the controller's personal data collection, use, processing, and disclosure and obtain consent from the child's parent or legal guardian for personal data collection, use, processing, and disclosure before personal data is collected from that child.

(c) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:

1. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the controller by postal mail, facsimile, or electronic scan;

2. Requiring a parent or guardian, 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;

3. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

4. Having a parent or guardian connect to trained personnel through video-conference;

[page=1119] 5. Having a parent or guardian communicate in person with trained personnel; and

6. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, provided the parent or guardian's identification is promptly deleted by the controller from its records after such verification is complete.

(d) When a controller receives consent to the collection or processing of personal data pursuant to (a) above, the controller shall inform the parent or guardian of the right to opt out of the processing of personal data and of the process for doing so on behalf of the consumer who is less than the age of 13.

(e) Any personal data collected for the purpose of verifying the identity of a parent or legal guardian may not be used for any other purpose.

(f) A controller may satisfy the requirements of this section by following a set of self-regulatory guidelines regarding consent for the collection or processing of personal data for consumers under the age of 13 that have been approved by the Federal Trade Commission in accordance with 16 CFR 312.11 and 15 U.S.C. § 6503.

13:45L-7.5 Consent after opt out

(a) A consumer's decision to consent to the processing of personal data from which the consumer has previously opted out is subject to the requirements for consent pursuant to N.J.A.C. 13:45L-7.2 and 7.3. Pursuant to N.J.A.C. 13:45L-3.4(f), a controller shall wait at least 12 months from the date of the consumer's opt-out request before asking a consumer to consent to the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

(b) A controller seeking consent to process personal data for a purpose after the consumer has opted out of processing for that purpose shall not make consent unnecessarily confusing or difficult, including by using interface dominating cookie banners, high frequency requests, cookie walls, pop-ups, or any other interstitials that degrade or obstruct the consumer's experience on the controller's web page or application.

(c) A controller may request consent to process personal data for a purpose after the consumer has opted out by providing a link to a privacy settings page, menu, or similar interface, or comparable offline method, that enables the consumer to consent to the controller processing the personal data for the opt-out purpose, provided the request for consent meets all other requirements for valid consent pursuant to N.J.A.C. 13:45L-7.2 and 7.3.

(d) If a consumer has opted out of the processing of personal data, and then initiates a transaction or attempts to use a product or service inconsistent with the request to opt out, such as signing up for a loyalty program that also involves the sale of personal data to a loyalty program partner, the controller may request the consumer's consent to process the consumer's personal data for that purpose, provided the request for consent meets the requirements for valid consent pursuant to N.J.A.C. 13:45L-7.2 and 7.3.

13:45L-7.6 Refusing or withdrawing consent

(a) Pursuant to N.J.S.A. 56:8-166.12(a)6, a controller shall provide an effective mechanism for a consumer to revoke the consumer's consent that is at least as accessible and user-friendly as the mechanism by which the consumer provided consent.

(b) If consent is obtained through an electronic interface, the consumer shall be able to refuse or withdraw consent through the same or a similar electronic interface.

(c) There shall be no detriment to a consumer for refusing or withdrawing consent, consistent with N.J.S.A. 56:8-166.6(c)2.

(d) Notwithstanding (c) above, if a consumer refuses to consent to, or withdraws consent for, the processing of personal data strictly necessary for a program, product, or service, the controller is no longer obligated to provide that program, product, or service.

(e) If a consumer withdraws consent for a processing activity, the controller shall cease that processing activity as soon as practicable, but not later than 15 days after the receipt of such request. The controller shall provide the consumer with instructions on how to exercise the right to deletion by providing a link to exercise the right to deletion, or informing the consumer that information regarding the right to delete their personal data can be found in the controller's privacy notice.

13:45L-7.7 Refreshing consent

(a) When a consumer has not interacted with a controller in the prior 24 months, the controller shall refresh consent in compliance with all requirements of this subchapter to continue processing sensitive data concerning a consumer or personal data concerning a known child pursuant to N.J.S.A. 56:8-166.12(a)4, or, pursuant to N.J.S.A. 56:8-166.12(a)7, to continue processing the personal data of a consumer for purposes of targeted advertising, the sale of the consumer's personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer when the controller has actual knowledge, or willfully disregards, that the consumer is at least 13 years of age, but younger than 17 years of age.

(b) If a processing purpose materially evolves such that the new purpose is not reasonably necessary to the purposes for which such personal data is processed, as disclosed to the consumer, the consumer's original consent is no longer valid, and the controller must obtain new consent pursuant to this subchapter before continuing to process the consumer's personal data.

## SUBCHAPTER 8. DATA PROTECTION ASSESSMENTS

### 13:45L-8.1 Minimum content

(a) Pursuant to N.J.S.A. 56:8-166.12(a)9, when processing presents a heightened risk of harm, as defined at N.J.S.A. 56:8-166.12(c), to a consumer, a controller shall, prior to the processing, conduct and document a data protection assessment of each processing activity that involves personal data acquired on or after (the effective date of this rulemaking).

(b) A data protection assessment shall include the following information:

1. A summary of the processing activity;

2. The categories of personal data to be processed and whether they include sensitive data, including personal data obtained from activities directed at children or from a consumer the controller has actual knowledge is under the age of 13;

3. The relationship between the controller and the consumers whose personal data will be processed, and the reasonable expectations of those consumers;

4. The elements of the processing activity, including:

i. Sources of personal data;

ii. Technology to be used;

iii. Processors to be used;

iv. Names or categories of personal data recipients, including third parties, affiliates, and processors that will have access to the personal data, the processing purpose for which the personal data will be provided to those recipients, and compliance processes that the controller uses to ensure the security of personal data shared with such recipients;

v. Operational details about the processing, including planned processes for personal data collection, use, storage, retention, and sharing; and

vi. Specific types of personal data to be processed;

5. The purposes of the processing activity, as well as any benefits of the processing that may flow, directly or indirectly to the controller, consumer, other stakeholders, or the public;

6. The risks to the rights of consumers posed by the processing activity. Risks to the rights of consumers that a controller may consider in a data protection assessment include, for example:

i. Constitutional harms, such as speech harms or associational harms;

ii. Data security harms, such as unauthorized access or adversarial use;

iii. Discrimination harms, such as a violation of Federal antidiscrimination laws or antidiscrimination laws of any state or political subdivision thereof;

iv. Unfair, unconscionable, or deceptive treatment;

v. A negative outcome or decision with respect to an individual's eligibility for a right, privilege, or benefit related to financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services;

[page=1120] vi. Financial injury or economic harm;

vii. Physical injury, harassment, or threat to an individual or property;

viii. Privacy harm, including both physical and non-physical intrusion upon the solitude or seclusion or the private affairs or concerns of consumers, stigmatization, or reputational injury;

ix. Psychological harm, including anxiety, embarrassment, fear, and other mental trauma; or

x. Other detrimental or negative consequences that affect an individual's interest in exercising rights protected by law, private life, private affairs, or private family matters or similar concerns, including actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data or other data will not be collected, observed, or used;

7. Measures and safeguards the controller will employ to reduce the risks identified by the controller pursuant to (b)6 above, including the following, as applicable:

i. The use of de-identified data;

ii. Measures taken pursuant to the controller duties at N.J.S.A. 56:8-166.12(a)3, including an overview of data security practices the controller has implemented, any data security assessments that have been completed pursuant to N.J.S.A. 56:8-166.12(a)9, and any measures taken to comply with the consent requirements at N.J.A.C. 13:45L-7.1; and

iii. Measures taken to ensure that consumers have access to the rights provided at N.J.S.A. 56:8-166.10;

8. An analysis as to whether the benefits of the processing outweigh the risks identified pursuant to (b)6 above, as mitigated by the safeguards identified pursuant to (b)7 above, including:

i. Contractual agreements in place to ensure that personal data in the possession of a processor or other third party remains secure; and

ii. Any other practices, policies, or trainings intended to mitigate processing risks;

9. Relevant internal actors and external parties contributing to the data protection assessment;

10. Any internal or external audit conducted in relation to the data protection assessment, including the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process; and

11. When the data protection assessment was reviewed and approved, and the names, positions, and signatures of the individuals responsible for the review and approval.

13:45L-8.2 Timing

(a) A controller shall conduct and document a data protection assessment before initiating a processing activity that presents a heightened risk of harm to a consumer, as defined at N.J.S.A. 56:8-166.12(c).

(b) A controller shall review and update the data protection assessment, as often as appropriate, considering the type, amount, and sensitivity of personal data processed and level of risk presented by the processing, throughout the processing activity's lifecycle in order to:

1. Monitor for harm caused by the processing and adjust safeguards, accordingly; and

2. Ensure that data protection and privacy are considered as the controller makes new decisions with respect to the processing.

(c) Data protection assessments that address the processing of personal data for profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer shall be reviewed and updated at least annually.

(d) A new data processing activity is generated when existing processing activities are modified in a way that materially changes the level of risk presented. When a new data processing activity is generated, a data protection assessment must reflect changes to the pre-existing activity and additional considerations and safeguards to offset any heightened risk.

1. Modifications that may materially change the level of risk of a processing activity may include changes to any of the following:

i. The way that existing systems or processes handle personal data;

ii. The purpose or purposes of processing;

iii. Personal data processed or sources of personal data;

iv. Method of collection of personal data;

v. The recipients of the personal data;

vi. Processor roles or processors;

vii. The algorithm applied;

viii. Software or other systems used for processing; or

ix. Changes in security methods or protocols.

(e) Data protection assessments, including prior versions that have been revised when a new data processing activity is generated, shall be stored for as long as the processing activity continues, and for at least three years after the conclusion of the processing activity. Data protection assessments shall be held in an electronic, transferable form.

(f) Data protection assessments shall be required for activities created or generated after (the effective date of this rulemaking).

‹ Previous

Next ›

PLEASE NOTE:

In order to ensure your comments are received, please send your comments concerning any rule proposals via email to DCAProposal@dca.lps.state.nj.us.

Please include the following in your email:

- **Email Subject Line:** Rule Proposal Subject
- **Email Body:** Comments to the Rule Proposal, Name, Affiliation, and Contact Information *(email address and telephone number)*.