

# STATE OF NEW YORK

8149--A

2023-2024 Regular Sessions

## IN ASSEMBLY

October 13, 2023

Introduced by M. of A. ROZIC, REYES, SHIMSKY, MAGNARELLI, HEVESI, BUTTENSCHON, FAHY, DICKENS, McMAHON, GLICK, DE LOS SANTOS, DURSO, McDONOUGH, GANDOLFO, SIMON, ZACCARO, DeSTEFANO, WALLACE, BERGER, BURDICK, SEAWRIGHT, McDONALD, BEEPHAN, SMULLEN, MANKTELOW, J. A. GIGLIO, SLATER, ARDILA, SILLITTI, DARLING, K. BROWN, EPSTEIN, LEVENBERG, WEPRIN, BICHOTTE HERMELYN, LUPARDO, MIKULIN, PAULIN, SOLAGES, SANTABARBARA, L. ROSENTHAL, DAVILA, BURGOS, CHANDLER-WATERMAN, TAYLOR, ZEBROWSKI, JENSEN, KIM, RIVERA, ZINERMAN, MAHER, WALKER, CUNNINGHAM, CONRAD, CLARK, JACKSON, DAIS, RAJKUMAR, FALL, LUNSFORD, FORREST, LEE, GIBBS, ANDERSON, LAVINE, STERN, BRAUNSTEIN, DINOWITZ, JEAN-PIERRE, SEPTIMO, KELLES, CARROLL, MAMDANI, HUNTER, BARRETT, BRONSON, PHEFFER AMATO, O'DONNELL, COOK, GUNTHER, BURKE, AUBRY, JONES, STIRPE, SAYEGH, RAGA, GALLAHAN, TAPIA, THIELE, GALLAGHER, ALVAREZ, SIMONE, EICHENSTEIN, PRETLOW, MORINELLO, SHRESTHA, EACHUS, MEEKS, JACOBSON, BRABENEC -- Multi-Sponsored by -- M. of A. GONZALEZ-ROJAS, WOERNER -- read once and referred to the Committee on Science and Technology -- recommitted to the Committee on Science and Technology in accordance with Assembly Rule 3, sec. 2 -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the general business law, in relation to establishing the New York child data protection act

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. The general business law is amended by adding a new article  
2 39-FF to read as follows:

3 ARTICLE 39-FF

4 NEW YORK CHILD DATA PROTECTION ACT

5 Section 899-ee. Definitions.

6 899-ff. Privacy protection by default.

7 899-gg. Processors.

EXPLANATION--Matter in italics (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD13150-12-4

1 899-hh. Ongoing coverage.

2 899-ii. Respecting user-provided age flags.

3 899-jj. Protections for third-party operators.

4 899-kk. Rulemaking authority.

5 899-ll. Scope.

6 899-mm. Remedies.

7 § 899-ee. Definitions. For purposes of this article, the following  
8 terms shall have the following meanings:

9 1. "Covered user" shall mean a user of a website, online service,  
10 online application, mobile application, or connected device, or portion  
11 thereof, in the state of New York who is:

12 (a) actually known by the operator of such website, online service,  
13 online application, mobile application, or connected device to be a  
14 minor; or

15 (b) using a website, online service, online application, mobile appli-  
16 cation, or connected device primarily directed to minors.

17 2. "Minor" shall mean a natural person under the age of eighteen.

18 3. "Operator" shall mean any person who operates or provides a website  
19 on the internet, online service, online application, mobile application,  
20 or connected device, and who, alone or jointly with others, controls the  
21 purposes and means of processing personal data. A person that acts as  
22 both an operator and processor shall comply with the applicable obli-  
23 gations of an operator and the obligations of a processor, depending on  
24 its role with respect to each specific processing of personal data.

25 4. "Personal data" shall mean any data that identifies or could  
26 reasonably be linked, directly or indirectly, with a specific natural  
27 person or device.

28 5. "Process" or "processing" shall mean an operation or set of oper-  
29 ations performed on personal data, including but not limited to the  
30 collection, use, access, sharing, sale, monetization, analysis,  
31 retention, creation, generation, derivation, recording, organization,  
32 structuring, storage, disclosure, transmission, disposal, licensing,  
33 destruction, deletion, modification, or deidentification of personal  
34 data.

35 6. "Primarily directed to minors" shall mean a website, online  
36 service, online application, mobile application, or connected device, or  
37 a portion thereof, that is targeted to minors. A website, online  
38 service, online application, mobile application, or connected device, or  
39 portion thereof, shall not be deemed directed primarily to minors solely  
40 because such website, online service, online application, mobile appli-  
41 cation, or connected device, or portion thereof refers or links to any  
42 other website, online service, online application, mobile application,  
43 or connected device directed to minors by using information location  
44 tools, including a directory, index, reference, pointer, or hypertext  
45 link. A website, online service, online application, mobile application,  
46 or connected device, or portion thereof, shall be deemed directed to  
47 minors when it has actual knowledge that it is collecting personal data  
48 of users directly from users of another website, online service, online  
49 application, mobile application, or connected device primarily directed  
50 to minors.

51 7. "Sell" shall mean to share personal data for monetary or other  
52 valuable consideration. "Selling" shall not include the sharing of  
53 personal data for monetary or other valuable consideration to another  
54 person as an asset that is part of a merger, acquisition, bankruptcy, or  
55 other transaction in which that person assumes control of all or part of  
56 the operator's assets or the sharing of personal data with a processor.

1 8. "Processor" shall mean any person who processes data on behalf of  
2 the operator. A person that acts as both an operator and processor shall  
3 comply with the applicable obligations of an operator and the obli-  
4 gations of a processor, depending on its role with respect to each  
5 specific processing of personal data.

6 9. "Third-party operator" shall mean an operator who is not the oper-  
7 ator:

8 (a) with whom the user intentionally and directly interacts; or

9 (b) that collects personal data from the direct and current inter-  
10 actions with the user.

11 § 899-ff. Privacy protection by default. 1. Except as provided for in  
12 subdivision six of this section and section eight hundred ninety-nine-jj  
13 of this article, an operator shall not process, or allow a processor to  
14 process, the personal data of a covered user collected through the use  
15 of a website, online service, online application, mobile application, or  
16 connected device, or allow a third-party operator to collect the  
17 personal data of a covered user collected through the operator's  
18 website, online service, online application, mobile application, or  
19 connected device unless and to the extent:

20 (a) the covered user is twelve years of age or younger and processing  
21 is permitted under 15 U.S.C. § 6502 and its implementing regulations; or

22 (b) the covered user is thirteen years of age or older and processing  
23 is strictly necessary for an activity set forth in subdivision two of  
24 this section, or informed consent has been obtained as set forth in  
25 subdivision three of this section.

26 2. For the purposes of paragraph (b) of subdivision one of this  
27 section, the processing of personal data of a covered user is permissi-  
28 ble where it is strictly necessary for the following permissible  
29 purposes:

30 (a) providing or maintaining a specific product or service requested  
31 by the covered user;

32 (b) conducting the operator's internal business operations. For  
33 purposes of this paragraph, such internal business operations shall not  
34 include any activities related to marketing, advertising, research and  
35 development, providing products or services to third parties, or prompt-  
36 ing covered users to use the website, online service, online applica-  
37 tion, mobile application, or connected device when it is not in use;

38 (c) identifying and repairing technical errors that impair existing or  
39 intended functionality;

40 (d) protecting against malicious, fraudulent, or illegal activity;

41 (e) investigating, establishing, exercising, preparing for, or defend-  
42 ing legal claims;

43 (f) complying with federal, state, or local laws, rules, or regu-  
44 lations;

45 (g) complying with a civil, criminal, or regulatory inquiry, investi-  
46 gation, subpoena, or summons by federal, state, local, or other govern-  
47 mental authorities;

48 (h) detecting, responding to, or preventing security incidents or  
49 threats; or

50 (i) protecting the vital interests of a natural person.

51 3. (a) For the purposes of paragraph (b) of subdivision one of this  
52 section, to process personal data of a covered user where such process-  
53 ing is not strictly necessary under subdivision two of this section,  
54 informed consent must be obtained from the covered user either through a  
55 device communication or signal pursuant to the provisions of subdivision

1 two of section eight hundred ninety-nine-ii of this article or through a  
2 request. Requests for such informed consent shall:

3 (i) be made separately from any other transaction or part of a trans-  
4 action;

5 (ii) be made in the absence of any mechanism that has the purpose or  
6 substantial effect of obscuring, subverting, or impairing a covered  
7 user's decision-making regarding authorization for the processing;

8 (iii) clearly and conspicuously state that the processing for which  
9 the consent is requested is not strictly necessary, and that the covered  
10 user may decline without preventing continued use of the website, online  
11 service, online application, mobile application, or connected device;  
12 and

13 (iv) clearly present an option to refuse to provide consent as the  
14 most prominent option.

15 (b) Such informed consent, once given, shall be freely revocable at  
16 any time, and shall be at least as easy to revoke as it was to provide.

17 (c) If a covered user declines to provide or revokes informed consent  
18 for processing, another request may not be made for such processing for  
19 the following calendar year, however an operator may make available a  
20 mechanism that a covered user can use unprompted and at the user's  
21 discretion to provide informed consent.

22 (d) If a covered user's device communicates or signals that the  
23 covered user declines to provide informed consent for processing pursu-  
24 ant to the provisions of subdivision two of section eight hundred nine-  
25 ty-nine-ii of this article, an operator shall not request informed  
26 consent for such processing, however an operator may make available a  
27 mechanism that a covered user can use unprompted and at the user's  
28 discretion to provide informed consent.

29 4. Except where processing is strictly necessary to provide a product,  
30 service, or feature, an operator may not withhold, degrade, lower the  
31 quality, or increase the price of any product, service, or feature to a  
32 covered user due to the operator not obtaining verifiable parental  
33 consent under 15 U.S.C. § 6502 and its implementing regulations or  
34 informed consent under subdivision three of this section.

35 5. Except as provided for in section eight hundred ninety-nine-jj of  
36 this article, an operator shall not purchase or sell, or allow a proces-  
37 sor or third-party operator to purchase or sell, the personal data of a  
38 covered user.

39 6. Within thirty days of determining or being informed that a user is  
40 a covered user, an operator shall:

41 (a) dispose of, destroy, or delete and direct all of its processors to  
42 dispose of, destroy, or delete all personal data of such covered user  
43 that it maintains, unless processing such personal data is permitted  
44 under 15 U.S.C. § 6502 and its implementing regulations, is strictly  
45 necessary for an activity listed in subdivision two of this section, or  
46 informed consent is obtained as set forth in subdivision three of this  
47 section; and

48 (b) notify any third-party operators to whom it knows it disclosed  
49 personal data of that covered user, and any third-party operators it  
50 knows it allowed to process the personal data that may include the  
51 personal data of that user, that the user is a covered user.

52 7. Except as provided for in section eight hundred ninety-nine-jj of  
53 this article, prior to disclosing personal data to a third-party opera-  
54 tor, or permitting a third-party operator to collect personal data from  
55 the operator's website, online service, online application, mobile

1 application, connected device, or portion thereof, the operator shall  
2 disclose to the third-party operator:

3 (a) when their website, online service, online application, mobile  
4 application, connected device, or portion thereof, is primarily directed  
5 to minors; or

6 (b) when the personal data concerns a covered user.

7 § 899-gg. Processors. 1. Except as provided for in section eight  
8 hundred ninety-nine-jj of this article, no operator or processor shall  
9 disclose the personal data of a covered user to a third party, or allow  
10 the processing of the personal data of a covered user by a third party,  
11 without a written, binding agreement governing such disclosure or proc-  
12 essing. Such agreement shall clearly set forth instructions for the  
13 nature and purpose of the processor's processing of the personal data,  
14 instructions for using or further disclosing the personal data, and the  
15 rights and obligations of both parties.

16 2. Processors shall process the personal data of covered users only  
17 when permitted by the terms of the agreement pursuant to subdivision one  
18 of this section, unless otherwise required by federal, state, or local  
19 laws, rules, or regulations.

20 3. A processor shall, at the direction of the operator, dispose of,  
21 destroy, or delete personal data, and notify any other processor to  
22 which it disclosed the personal data of the operator's direction, unless  
23 retention of the personal data is required by federal, state, or local  
24 laws, rules, or regulations. The processor shall provide evidence of  
25 such deletion to the operator within thirty days of the deletion  
26 request.

27 4. A processor shall delete or return to the operator all personal  
28 data of covered users at the end of its provision of services, unless  
29 retention of the personal data is required by federal, state, or local  
30 laws, rules, or regulations. The processor shall provide evidence of  
31 such deletion to the operator within thirty days of the deletion  
32 request.

33 5. An agreement pursuant to subdivision one of this section shall  
34 require that the processor:

35 (a) process the personal data of covered users only pursuant to the  
36 instructions of the operator, unless otherwise required by federal,  
37 state, or local laws, rules, or regulations;

38 (b) assist the operator in meeting the operator's obligations under  
39 this article. The processor shall, taking into account the nature of  
40 processing and the information available to them, assist the operator by  
41 taking appropriate technical and organizational measures, to the extent  
42 practicable, for the fulfillment of the operator's obligation to delete  
43 personal data pursuant to section eight hundred ninety-nine-ff of this  
44 article;

45 (c) upon reasonable request of the operator, make available to the  
46 operator all information in its possession necessary to demonstrate the  
47 processor's compliance with the obligations in this section;

48 (d) allow, and cooperate with, reasonable assessments by the operator  
49 or the operator's designated assessor for purposes of evaluating compli-  
50 ance with the obligations of this article. Alternatively, the processor  
51 may arrange for a qualified and independent assessor to conduct an  
52 assessment of the processor's policies and technical and organizational  
53 measures in support of the obligations under this article using an  
54 appropriate and accepted control standard or framework and assessment  
55 procedure for such assessments. The processor shall provide a report of  
56 such assessment to the operator upon request; and

1 (e) notify the operator a reasonable time in advance before disclosing  
2 or transferring the personal data of covered users to any further  
3 processors, which may be in the form of a regularly updated list of  
4 further processors that may access personal data of covered users.

5 § 899-hh. Ongoing coverage. 1. Upon learning that a user is no longer  
6 a covered user, an operator:

7 (a) shall not process the personal data of the covered user that would  
8 otherwise be subject to the provisions of this article until it receives  
9 informed consent pursuant to subdivision three of section eight hundred  
10 ninety-nine-ff of this article, and

11 (b) shall provide notice to such user that they may no longer be enti-  
12 tled to all of the protections and rights provided under this article.

13 2. Upon learning that a user is no longer a covered user, an operator  
14 shall provide notice to such user that such user is no longer covered by  
15 the protections and rights provided under this article.

16 § 899-ii. Respecting user-provided age flags. 1. For the purposes of  
17 this article, an operator shall treat a user as a covered user if the  
18 user's device communicates or signals that the user is or shall be  
19 treated as a minor, including through a browser plug-in or privacy  
20 setting, device setting, or other mechanism that complies with regu-  
21 lations promulgated by the attorney general.

22 2. For the purposes of subdivision three of section eight hundred  
23 ninety-nine-ff of this article, an operator shall adhere to any clear  
24 and unambiguous communications or signals from a covered user's device,  
25 including through a browser plug-in or privacy setting, device setting,  
26 or other mechanism, concerning processing that the covered user consents  
27 to or declines to consent to. An operator shall not adhere to unclear or  
28 ambiguous communications or signals from a covered user's device, and  
29 shall instead request informed consent pursuant to the provisions of  
30 paragraph a of subdivision three of section eight hundred ninety-nine-ff  
31 of this article.

32 § 899-jj. Protections for third-party operators. Sections eight  
33 hundred ninety-nine-ff and eight hundred ninety-nine-gg of this article  
34 shall not apply where a third-party operator is processing the personal  
35 data of a covered user of another website, online service, online appli-  
36 cation, mobile application, or connected device, or portion thereof,  
37 provided that the third-party operator received reasonable written  
38 representations that the covered user provided informed consent for such  
39 processing, or:

40 1. the operator does not have actual knowledge that the covered user  
41 is a minor; and

42 2. the operator does not have actual knowledge that the other website,  
43 online service, online application, mobile application, or connected  
44 device, or portion thereof, is primarily directed to minors.

45 § 899-kk. Rulemaking authority. The attorney general may promulgate  
46 such rules and regulations as are necessary to effectuate and enforce  
47 the provisions of this article.

48 § 899-ll. Scope. 1. This article shall apply to conduct that occurs in  
49 whole or in part in the state of New York. For purposes of this article,  
50 commercial conduct takes place wholly outside of the state of New York  
51 if the business collected such information while the covered user was  
52 outside of the state of New York, no part of the use of the covered  
53 user's personal data occurred in the state of New York, and no personal  
54 data collected while the covered user was in the state of New York is  
55 used.

1 2. Nothing in this article shall be construed to prohibit an operator  
2 from storing a covered user's personal data that was collected pursuant  
3 to section eight hundred ninety-nine-ff of this article when such  
4 covered user is in the state.

5 3. Nothing in this article shall be construed to impose liability for  
6 commercial activities or actions by operators subject to 15 U.S.C. 6501  
7 that is inconsistent with the treatment of such activities or actions  
8 under 15 U.S.C. 6502.

9 § 899-*mm*. Remedies. Whenever it appears to the attorney general,  
10 either upon complaint or otherwise, that any person, within or outside  
11 the state, has engaged in or is about to engage in any of the acts or  
12 practices stated to be unlawful in this article, the attorney general  
13 may bring an action or special proceeding in the name and on behalf of  
14 the people of the state of New York to enjoin any violation of this  
15 article, to obtain restitution of any moneys or property obtained  
16 directly or indirectly by any such violation, to obtain disgorgement of  
17 any profits or gains obtained directly or indirectly by any such  
18 violation, including but not limited to the destruction of unlawfully  
19 obtained data, to obtain damages caused directly or indirectly by any  
20 such violation, to obtain civil penalties of up to five thousand dollars  
21 per violation, and to obtain any such other and further relief as the  
22 court may deem proper, including preliminary relief.

23 § 2. Severability. If any clause, sentence, paragraph, subdivision,  
24 section or part of this act shall be adjudged by any court of competent  
25 jurisdiction to be invalid, such judgment shall not affect, impair, or  
26 invalidate the remainder thereof, but shall be confined in its operation  
27 to the clause, sentence, paragraph, subdivision, section or part thereof  
28 directly involved in the controversy in which such judgment shall have  
29 been rendered. It is hereby declared to be the intent of the legislature  
30 that this act would have been enacted even if such invalid provisions  
31 had not been included herein.

32 § 3. This act shall take effect one year after it shall have become a  
33 law. Effective immediately, the addition, amendment and/or repeal of any  
34 rule or regulation necessary for the implementation of this act on its  
35 effective date are authorized to be made and completed on or before such  
36 effective date.