Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

California AG Issues Significant Changes to Draft CCPA Regulations as of March 2020

Norton Rose Fulbright LLP – March 2020 – Private and confidential

Takeaways for CCPA Regulations as of March 2020

On February 7, 2020, and again on March 11, 2020, the Office of the Attorney General (OAG) issued revisions to the proposed California Consumer Privacy Act (CCPA) regulations, and there are some surprises in both the additions and in the deletions – click here for the text of modified regulations.

Notable changes include provisions relating to:

- accessibility standards;
- specific requirements for mobile applications and offline collection of data;
- data broker registration and notice requirements;
- how to calculate and communicate the value of data;
- new affirmative consent and reasonable security requirements;
- notifications to third parties, annual reporting requirement to begin on July 1; and
- various deadlines that are triggered upon receipt of a consumer request (i.e., 10 business days, 15 business days, and 45 calendar days).

For businesses that are looking to understand when the final text of the regulations may become available, click here for an OAG publication which outlines the rulemaking process. The CCPA requires the AG's regulations to become effective on or before July 1, 2020. In order to meet that deadline, we expect the final text of the regulations to be sent by OAG to the Office of Administrative Law (OAL) for approval no later than April. OAL will then have thirty (30) working days to determine whether the record satisfies all the procedural requirements of the California Administrative Procedures Act (APA), and if approved, the final regulation text will be filed with the Secretary of State. OAL's review will not include any comments on the substantive content of the regulations. For the CCPA regulations to become effective on July 1, OAL must file the final regulation text with the Secretary of State by May 29 (the deadline is technically May 31 but that day is Sunday this year).

As noted above, the AG has asked for comments on his most recent regulatory proposal by March 27. Although we can expect the AG to make revisions in light of the comments he receives, the short turnaround before he needs to get the regulations to the OAL may limit his ability to alter the regulations dramatically. Moreover, given the short period of time between the latest date on which the draft regulations may be made public and the regulation's effective date, businesses may not have much time to absorb the final version of the regulations before compliance efforts will need to begin. Thus, it may be prudent for businesses to get started on revising compliance procedures based on the current draft regulations in order to give themselves the best chance to be ready in time.

Below is a summary of key proposed revisions that businesses can use to evaluate if any changes should be made to existing compliance programs in advance of the regulations becoming finalized and to identify areas that appear to be enforcement priorities:

- Definitions
- Notice at Collection of Personal Information
- Notice of Right to Opt-Out of Sale of Personal Information
- Notice of Financial Incentive
- Privacy Policies
- Requests to Know and Requests to Delete
- Responding to Requests to Know and Requests to Delete
- Service Providers
- Requests to Opt-Out
- Requests to Opt-In
- Training: Record-Keeping
- Verification
- Authorized Agent
- Special Rules Regarding Minors
- Non-Discrimination

Here is a quick summary of the changes between the February and March versions of the draft regulations:

- The February version of the draft regulations stated that IP address alone, which did not or could not reasonably link to a particular consumer, was not "personal information." The March version deleted this provision.
- With respect to employment-related information, the regulations have loosened a bit so that employers now would not be required to provide a link to the privacy policy.
- The logo/button for "opt-outs" that was proposed in February was deleted in March.
- As for the privacy policy, businesses would need to identify categories of sources for collection and must identify the business or commercial purpose for collection, but not specifically for each category of personal information collected. Nevertheless both the categories and purposes must be described to provide consumers with "meaningful understanding."
- Certain types of information cannot be disclosed in response to a "Request to Know," including Social Security Numbers and biometrics. But under the March version of the draft regulations, the business would need to respond with a general description of what is collected but not the actual data, such as "we collect unique biometric data including a fingerprint scan."
- User-enabled privacy controls would no longer require the user to make an affirmative choice to opt-out.

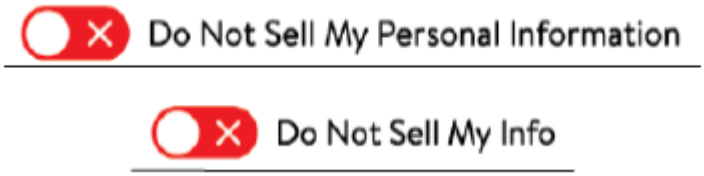
A more comprehensive summary is provided below.

	Proposed Changes to the CCPA Regulations	Takeaways
Definitions	Additional examples are added to clarify what the OAG expects to see as "**categories of sources**" from whom personal information is collected: "from consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers." This is the same list of examples provided for "categories of third parties" to whom the business shares personal information. The definition of "**categories of third parties**" is changed from "types of entities that do not collect personal information directly from consumers" to "types and groupings of third parties with whom the business shares personal information." The definition of "**household**" is clarified to mean "people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier." "**Price or service difference**" is clarified to mean "(1) any difference in the price or rate charged for any goods or services to any consumer *related to the collection , retention, or sale of personal information*… or (2) any differences in the level or quality of any goods or services offered to any consumer *related to the collection, retention, or sale of personal information*." (emphasis added) This is the same qualifier that was already in the proposed regulations for "**financial incentive.**" The definition of "**request to know**" has been clarified to mean "a consumer request that a business disclose personal information that it has *collected* about the consumer," and includes a request for "specific pieces of personal information that a business has *collected* about the consumer." (emphasis added) Without this clarification, the regulations required businesses "to disclose personal information that it has about the consumer." We note the definition of "**request to delete**" has not changed with the revised draft regulations and continues to only require businesses to "delete personal information about the consumer that the business has collected *from* the consumer." (emphasis added)	☐ Review whether the current privacy notices include disclosures relating to categories of sources and categories of third parties, including the ones OAG set out as examples. Expect scrutiny on whether the business receives personal information from data brokers or shares personal information with data brokers. ☐ Review whether and how the business collects and processes "household" data.

	The OAG provides a new definition for "**signed**." The new term means physically signed or electronically signed per California's codification of the Uniform Electronic Transaction Act (UETA). Note that the definition did not use the more common federal reference to ESIGN, but instead uses the much simpler—and far more widely adopted—requirements of UETA. This would allow businesses to use either physical or electronic signatures for purposes of verifying non-accountholders' requests (Section 325), authorized agent requests (Section 326), and parental consent (Section 330). "**Value of the consumer's data**" is also added as a new definition to mean "the value provided to the business by the consumer's data as calculated under section 999.337." This is the same language that was already included in section 999.337 previously but it is now moved to the definitions section of the regulations.	☐ Review if non-discrimination requirements under the CCPA apply to the business, based on the clarification that the "financial incentive" and "price or service difference" must be related to the collection, retention, or sale of personal information. ☐ Review the broad definition of "collect" under CCPA to assess what personal information the business has collected about consumers.
Notice at Collection of Personal Information	In several sections throughout the draft regulations, the Attorney General has now provided a standard for what it means to provide a notice that is "**reasonably accessible**" for consumers with disabilities. For online notices, a business must follow "generally recognized industry standards, such as the Web Content Accessibility Guideline, version 2.1 of June 5, 2018, for the World Wide Web Consortium, incorporated herein by reference." For businesses that collect personal information through a **mobile application**, the OAG provides guidance that "a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu" will satisfy the requirement to provide notice at collection. The OAG also includes a new **"just-in-time" notice** requirement for businesses that collect personal information from a consumer's mobile device for a purposes that "the consumer would not reasonably expect." The notice must contain a summary of the	☐ Businesses should review online notices to determine if the accessibility requirement is met, using one of the generally recognized industry standards, such as the WCAG. ☐ Businesses should review if mobile applications include a link to the privacy notice on the download page and in the

	categories of personal information being collected and a link to the full notice at collection. A flashlight application that collects geolocation information is provided as an example requires a "just-in-time" notice, such as a pop-up window when the consumer opens the application. For businesses that collect personal information **over the telephone** or **in person**, the notice may be provided orally. The draft regulations also provide that a business that collects personal information **offline** may "include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online." The proposed regulations clarify that "a business shall not use a consumer's personal information for a purpose ***materially different*** than those disclosed in the notice at collection." (emphasis added) Before using personal information for a purpose that is materially different than what was previously disclosed in the notice at collection, businesses must obtain **explicit consent** from the consumer to use it for this new purpose. The proposed regulations remove the requirement to disclose the business or commercial **purpose** "for each category of personal information" and instead include a broader requirement to disclose the business or commercial purposes for which the categories of personal information will be used generally. Businesses that do not collect information directly from consumers but are in the business of selling personal information should be relieved to see that the OAG has now removed the cumbersome and onerous requirement to contact the source of the personal information to obtain signed attestations about the notice that was provided at collection and to have those attestations available to the consumer upon request for two years. Instead, a business that does not collect personal information directly from consumers does not need to provide a notice at collection as long as it is registered as a **data broker** with the OAG and includes in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. A data broker is defined as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct	application's settings menu. - Businesses should identify any uses of personal information by mobile applications that may trigger a "just-in-time" notice. - Businesses should identify any business processes where personal information may be collected offline, including over the telephone or in person. Businesses may consider where paper forms of notice or physical signage may be appropriate for offline collection of personal information. - Businesses should evaluate current disclosures in privacy notices to review whether any uses contemplated by the business would be materially different, and seek to minimize

	relationship." As of January 31, 2020, when the new data broker registration law went into effect, 102 companies had registered. To provide snapshots, 142 companies had registered as of February 18 and 233 companies had registered as of March 13. Click here to view the Data Broker Registry or register as a data broker.	instances where explicit consent from consumers will be needed. □ Businesses can streamline the notice to include the business or commercial purposes for the categories of personal information collected generally, instead of separately disclosing the purpose for each category of personal information. □ If the business is "collecting" and "selling" personal information under CCPA, determine if the business needs to register as a data broker under California Civil Code § 1798.99.82.
Notice of Right to Opt-Out of Sale of Personal Information	The OAG clarifies that the notice of right to opt-out is required to inform consumers of their right "to direct a business that sells their personal information" and removes language from the previous version of the regulations that would have required a notice to opt-out if the business "may in the **future sell**" personal information. A notice of the right to opt-out is not required as long as the business currently does not sell personal information. The OAG also removed the requirement to state in the privacy policy that the business *will not sell* personal information (emphasis added).	□ Businesses should consider adding an opt-out button to the website homepage or the download or landing page of a mobile application next to the "Do Not Sell My Personal

	Also under the revised regulations, a business need not include in the opt-out notice information relating to when a consumer wishes to use an authorized agent to opt-out, or a link to the privacy policy. The February draft of the regulations provided the following design of an **opt-out button** but this draft guidance was deleted in the March version:  This button – which was always optional – would have needed to direct users to a webpage containing the notice of the right to opt-out, including an interactive form by which the consumer can submit their request to opt-out (see further guidance below on "The Requests to Opt-Out"). Businesses should monitor this section to see if the OAG includes a different button design in the final regulations. A business that collects personal information through a **mobile application** shall include the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the download or landing page of a mobile application or within the application, such as through the application's settings menu. Requirements for businesses that collect personal information **offline** or businesses that do not operate a website did not change under the revised regulations. Businesses must provide notice in a method that facilitates consumer awareness of their right to opt-out, which may include printing the notice on paper forms or posting signage at physical locations, and a separate offline method for consumers to submit their request to opt-out if the business does not operate a website. If the business did not provide a notice of right to opt-out, the business may not sell the personal information it	Information" or "Do Not Sell My Info" link. Note this does not remove the requirement to provide the notice of right to opt-out which includes an interactive form by which the consumer can submit their request to opt-out online. ☐ Businesses should separately consider if and how a notice of right to opt-out should be provided offline and on mobile applications. ☐ To avoid having to obtain affirmative consent from consumers, businesses should consider providing the notice of right to opt-out. ☐ If the business is not currently selling personal information, it may not need to affirmatively state that it will never sell personal information in the future.

	collected unless it obtains **affirmative consent** from the consumer.	
Notice of Financial Incentive	As noted above, "financial incentive," "price or service difference" and "value of the consumer's data" are defined terms. The proposed regulations clarify that a business that does not offer a financial incentive or price or service difference related to the collection, retention, or sale of personal information is not required to provide a notice of financial incentive. If a business is offering a financial incentive or price or service difference, however, the notice must be provided and be **readily available** where consumers will encounter it before **opting in**. The notice must include not only a description of the material terms of the financial incentive or price or service difference and the categories of personal information that are implicated, but also the **value of the consumer's data** and how the financial incentive or price or service difference is reasonably related to the value of the consumer's data.	☐ Businesses should determine if a notice of financial incentive needs to be provided and how the value of the consumer's data can be estimated and communicated to the consumer.
Privacy Policies	Under revised draft regulations, businesses no longer need to identify for each category of personal information the sources from which the information was collected, the business or commercial purposes for which the information was collected, the sources of personal information, and the categories of third parties with whom the business shares personal information. The description of the categories of sources and business or commercial purposes must be described to give consumers a "meaningful understanding." A business must still identify the **categories of personal information collected** in the preceding 12 months, categories of personal information, if any, that the business **disclosed for a business purpose or sold** to third parties in the preceding 12 months, and state whether the business sells personal information and if it has affirmative knowledge that it sells personal information of **minors** under 16 years of age. Under the revised proposal, businesses that **sell** personal information must also provide for each category of personal information identified the categories of third parties to whom the information was disclosed or sold. A **mobile application** may include a link to the privacy policy in the application's settings menu.	☐ Businesses should determine if disclosures in privacy policies need to be revised.

Requests to Know and Requests to Delete	The regulations clarify that if a business is **exclusively online**, providing an email address would be sufficient where consumers can submit requests to know. The revised regulations also remove the requirement for businesses that operate a website to provide an **interactive webform**. For businesses that interact with consumers **in person**, the draft regulations have slightly eased the requirements. The OAG deleted the example that would require a retail business to offer three (3) methods for submitting consumer requests, including a form that can be submitted in person at the retail location. The revised regulations require a business to "consider" providing an in-person method such as a printed form that can be sent by mail, or a tablet, computer portal or a telephone that consumers can use to submit their requests. The revised regulations remove the requirement for **businesses that do not interact directly with consumers** to provide at least one method by which consumers can submit requests online, such as through the business's website or a link posted on the business's website.	☐ Businesses should determine if and how consumers can be made aware of the designated methods for submitting requests to know and requests to delete.
Responding to Requests to Know and Requests to Delete	The revised regulations clarify that businesses will have **10 business days** to confirm a request to know or delete and states that the confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation need not be given separately in writing. Businesses will have **45 calendar days** to respond to requests to know or delete and an additional 45 calendar days to respond if needed, for a total of **90 calendar days** from the day the request is received. The OAG removed in this version guidance which would have allowed businesses to refuse to provide specific pieces of personal information "if a disclosure creates a substantial, articulable, and unreasonable **risk to the security** of that personal information, the consumer's account with the business, or the security of the business's systems or networks." This clause would have potentially allowed businesses to deny certain information requests.	☐ Businesses should consider revising consumer request response procedures to reflect the different response deadlines. ☐ Businesses should understand to what extent they must search and interrogate their systems to respond to requests for

	Businesses can still rely on other exceptions to the right to know and the OAG adds "unique **biometric data** generated from measurements or **technical analysis of human characteristics**" to the list of data elements business should not disclose in response to a request to know, in addition to Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, account password, and security questions and answers. Instead of disclosing these data elements, the business should instead respond to a "Request to Know" with a general description, such as "we collect unique biometric data including fingerprint scans." The draft regulations also added a section which allows businesses to not have to search for personal information in response to an access request if all four (4) elements are present: 1. The personal information is not in a searchable or reasonably accessible format; 2. The business maintains the information only for legal or compliance purposes; 3. The business does not sell or use the information for commercial purposes; and 4. The business describes to the consumer the categories of records it did not search because they met these criteria. The OAG further clarifies that businesses are required to inform the requestor if the request to know specific pieces of personal information or a request to delete was **denied in whole or in part** and explain the basis for the denial, unless doing so would be prohibited by law. The revised regulations clarify the information that should be provided in response to a **verified request to know**, including for each category of personal information the categories of third parties to whom the business sold that particular category of personal information in the preceding 12 months and the categories of third parties to whom the business disclosed for a business purpose that particular category of personal information in the preceding 12 months. The OAG also removed the requirement for businesses to treat a **deletion request as an opt-out request** if the	access or deletion. □ Businesses should evaluate consumer response procedures to ensure that information that should not be disclosed in response to a right to know request is redacted or removed. □ Businesses should evaluate under which circumstances they will be prohibited from informing the requestor about the denial of their request. □ Businesses that sell personal information should consider if an opt-out should be offered to requestors who request deletion of their personal information. □ Businesses that collect household data should develop a separate verification process for handling requests to know or delete

	identity of the requestor cannot be verified. Instead, a business that sells personal information should ask the consumer if they would like to opt-out. The OAG also removed the requirement for businesses to specify the **manner in which it has deleted** the personal information in response to a consumer's request to delete, but a business must inform the consumer where or not it has complied with the consumer's request and that it will maintain a record of the request. If personal information is stored on **archived or backup systems**, businesses need not comply with the request to delete unless the data is restored to an active system or at a later date accessed or used for a sale, disclosure, or commercial purpose. This potentially could provide relief for companies that maintain backup copies of data that is not actively in use. A business need not comply with **requests to access or delete household information** unless <u>all</u> consumers jointly make the request, the business verifies all members, and the business verifies that all members are <u>currently</u> members of the household. If a member of a household is under 13, the business must obtain verifiable parental consent.	household information collected by the business.
Service Providers	The OAG changed almost every section of the service provider regulations. Perhaps the most significant change proposed is to permit a service provider to use the personal information internally "to build or improve the quality of its service, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or cleaning or augmenting data acquired from another source." The revised regulations also clarify that a business that provides services to non-business entities and otherwise meets the requirements and obligations of a "service provider" will be considered a service provider for CCPA. The AG's Initial Statement of Reasons explains that this subsection is not intended to address a service-provider-to-service-provider scenario, but rather is to address service providers that provide services to **government entities and nonprofit organization**s.	Service provider obligations under the draft regulations have significantly been modified and should be carefully reviewed and continue to be monitored until the regulations are finalized.

	The OAG clarifies that **if a business directs a second business to collect personal information** on behalf of the first business, the second business would be deemed a service provider of the first business. The OAG added that a **service provider shall not sell data** on behalf of a business if a consumer has opted-out. This addition can be interpreted to mean that if a business is instructing its service providers to sell data, it should comply with opt-out requests prior to sharing that consumer's data with service providers. In addition, the OAG removed the requirement for service providers to provide the consumer with contact information for the business in **response to a request to know or delete** and instead allows service providers to either act on behalf of the business in responding to consumer requests or simply inform the consumer that the request cannot be acted upon because the request has been sent to a service provider.	
Requests to Opt-Out	Another section with significant changes is the opt-out section. Notably, the revised regulations add a requirement that a business's method for submitting requests to opt-out shall be "**easy for consumers** to execute and shall require **minimal steps** to allow the consumer to opt-out. A business shall not utilize a method that is designed with the purpose or substantial effect of subverting or impairing a consumer's decision to opt-out." The OAG also adds that if a consumer's business-specific privacy setting or participating in a business's financial incentive program **conflicts with a business's global privacy controls**, the business must respect the global privacy control, but may notify the consumer and give the consumer the choice to confirm the business-specific privacy setting or participating in the financial incentive program. Under the revised regulations, a business must comply with a request to opt-out no later than **15 business days** from the date the business receives the request. The revised regulations remove the previous requirement that a business receiving an opt-out request must notify all third parties to whom it has sold the personal information within 90 days prior to the business's receipt of the consumer's request. Instead, the OAG would require that	☐ Businesses should evaluate whether the methods to submit an opt-out request is sufficiently "easy" and requires minimal steps. ☐ Businesses should evaluate how consumer's request to opt-out may or may not conflict with their global privacy control settings. ☐ Businesses should assess how long it will take to act upon an opt-out request and whether any

	if a consumer's personal information is sold to third parties between the time a business receives an opt-out request and before it can comply with the request, it must **notify** those third parties that the consumer has exercised their right to opt-out and direct them not to sell that consumer's information. We note that this effectively means a **resale** is prohibited but a sale may be permissible during that 15-day window.	notifications to third parties may be necessary.
Requests to Opt-In	If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in.	Businesses can have products or services that sell personal information as long as consumers are provided the ability to opt-out or opt-in.
Training: Record-Keeping	Businesses are required to maintain records of consumer requests and how the business responded to said requests for at least 24 months. The revised regulations introduce a new requirement for businesses to implement and maintain **reasonable security** procedures and practices in maintain these records. Another new requirement is that information maintained for recordkeeping purposes shall not be shared with any **third party**. The OAG also made modifications to the **annual reporting requirement** that applies to businesses that sell consumer's personal information. The OAG raised the minimum threshold number for this requirement from 4,000,000 to 10,000,000 consumers. By **July 1 of every calendar year**, which coincides with the date when the OAG will begin CCPA enforcement this year, a business that alone or in combination buys, receives or shares for commercial purposes, or sells personal information of 10,000,000 or more consumers in a calendar year will be required to compile the following metrics and display them in their privacy policy or post them on a website that is accessible from a link included in the privacy policy:	Businesses should evaluate which record-keeping requirements are applicable and prepare documentation that can be produced upon request. Businesses need to implement and maintain reasonable security procedures and practices to maintain consumer request records.

	a. The number of requests to know that the business received, complied with in whole or in part, and denied; b. The number of requests to delete that the business received, complied with in whole or in part, and denied; c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and d. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out. The OAG also added a new requirement that businesses shall upon request compile and provide to the Attorney General the information required above.	
Verification	The OAG clarifies that a business shall not require the consumer or the consumer's authorized agent to **pay a fee** for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a **notarized affidavit** to verify their identity unless the business compensates the consumer for the cost of notarization. The revised regulations also provide new examples for how to **verify non-accountholders** and how businesses can respond to consumer requests where the business has no reasonable method by which they can verify any consumer.	Businesses should evaluate their verification procedures, including to remove consumer requirements that the regulations prohibit the business from using.
Authorized Agent	The OAG adds a new requirement for authorized agents to implement and maintain reasonable security procedures and practices to protect the consumer's information when a consumer uses an authorized agent to submit a request to know or a request to delete.	Authorized agents need to implement and maintain reasonable security procedures and practices to protect the consumer's information.
Special Rules Regarding Minors	The previous regulations required a business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 to establish, maintain, and comply with a reasonable method for	Businesses that collect or sell personal information of

	determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. The revised regulations clarify the requirement to apply it to businesses that have knowledge that they ***sell*** **the personal information of minors**, not collect or maintain. The OAG adds a requirement for businesses to establish and document the method used for determining whether a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the **parent or guardian** of that child. A business that has actual knowledge that it sells the personal information of minors at least 13 and less than 16 years of age should establish, document, and comply with a reasonable process for allowing such **minors to opt-in** to the sale of their personal information.	minors should review the parental consent and verification methods. ☐ Businesses should evaluate if an opt-in process should be established for minors between the age of 13 and 16.
Non-Discrimination	Businesses that offer loyalty programs or other financial incentives will be interested in the changes to this Article. First, the Attorney General has added a provision that, if a business cannot **estimate the value of the consumer's data** or cannot show how the difference in price or service is reasonably related to the value of the consumer data, the business cannot offer the financial incentive or price or service differential. Second, the Attorney General deleted the previous example about a retailer offering discounts to consumers who signed up for a mailing list, where the consumer could opt-out or have data deleted and still receive the discounts. Instead, the Attorney General has proposed an example of a **loyalty program** for customers who receive a $5 coupon to their email address after spending $100 with the business. In the example, the consumer files a deletion request but wants to stay in the loyalty program. The Attorney General advises that the business may deny the deletion request for the email address and amounts spent because that information is necessary to provide the loyalty program and is reasonably anticipated by the consumers. The Attorney General added another example that follows the one above, except this time, the business honors the deletion request and stops offering coupons. The example concludes that the business's actions are	☐ Businesses that offer financial incentives or a price or service difference related to the value of the consumer's data should carefully review the changes in the revised regulations, including the four (4) examples provided by the OAG.

	discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the personal information.	

Contacts

Jeewon Kim Serrato

Head of Data Protection, Privacy and Cybersecurity
Norton Rose Fulbright US – San Francisco Office
555 California Street, Suite 3300 San Francisco, CA 94104
Tel +1 628 231 6809
jeewon.serrato@nortonrosefulbright.com

Jeff Margulies

Partner-in-Charge, Los Angeles and San Francisco
Norton Rose Fulbright US – Los Angeles Office
555 South Flower Street Forty-First Floor Los Angeles, CA 90071
Tel +1 213-892-9286
jeff.margulies@nortonrosefulbright.com

David Kessler

Head of Data and Information Risk, United States
Norton Rose Fulbright US – New York Office
1301 Avenue of the Americas New York, NY 10019-6022
Tel +1 212 318 3382
david.kessler@nortonrosefulbright.com

Sue Ross

Senior Counsel
Norton Rose Fulbright US – New York Office
1301 Avenue of the Americas New York, NY 10019-6022
Tel +1 212 318 3280
susan.ross@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global legal practice. We provide the world's pre-eminent corporations and financial institutions with a full business law service. We employ more than 3800 lawyers based in over 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

Law around the world

nortonrosefulbright.com