THE US-ISRAEL LEGAL REVIEW 2020

GLOBAL LEGAL MEDIA
STRATEGIC LAW FIRM MARKETING

A GLOBAL LEGAL MEDIA & NISHLIS LEGAL MARKETING PUBLICATION

NISHLIS LEGAL MARKETING SETTING THE BENCHMARK

IN ASSOCIATION WITH:
ACC Association of Corporate Counsel ISRAEL

CCPA Compliance: A To-Do List for Israeli Companies

California's Landmark Consumer Data Privacy Law is Approaching Its One-year Anniversary: Take Steps to Comply Now.

The California Consumer Privacy Act (CCPA) took effect on January 1, 2020 and became enforceable on July 1, 2020. The state issued final regulations in July. Israeli companies that do business in California and fall under jurisdiction of the CCPA must comply with a multitude of requirements involving privacy notices, opt-out mechanisms and consumer requests for data.

In a November 2020 referendum, the state's voters approved the California Privacy Rights Act (CPRA), which makes a variety of changes to CCPA, bringing it closer to the European Union's General Data Protection Regulation (GDPR) in several respects. As CPRA will go into effect in January 2023, CCPA remains the state's prevailing data privacy law.

WHAT ISRAELI COMPANIES ARE SUBJECT TO CCPA?

You can be subject to the law if you are a for-profit company that collects and processes California residents' personal information, "do business" in the state and meet one of the following three criteria:

- You have at least **$25 million in annual gross revenues**. This means $25 million from wherever acquired, not just revenues from California.
- You buy, sell, share and/or receive (alone or in combination with others) **the personal information of at least 50,000 California consumers, households or devices**, per year. [Note: To reach this threshold, 137 unique visits to your website a day suffices.]
- At least **50% of your annual revenue** comes from selling California consumers' personal information.

You can also fall under CCPA if you control or are controlled by an entity that meets the above criteria and share branding, meaning CCPA applies to entities that do business in California and those that are part of the corporate group (parents or subsidiaries) of an entity that does business in California.

You may indirectly be in scope if your B2B clients say so. In order to comply with obligations under CCPA, businesses that are subject to the law need to ensure that their third-party service providers use information in a way that allows the business to be compliant. Therefore, you could be required to comply with CCPA provisions indirectly, through an agreement with a customer. CCPA applies to any business that meets the above criteria, even if it does not deal directly with consumers.

WHAT DOES IT MEAN TO COLLECT AND PROCESS CALIFORNIANS' DATA?

- You receive, buy, rent or access information (including personal information collected passively, i.e. through cookies); and
- Determine the purpose and means of processing of information that both:
  - Identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household AND
  - Pertains to an individual who is (1) in

California for other than a temporary purpose, or (2) domiciled in California, but outside the state for a temporary purpose

"DOING BUSINESS IN CALIFORNIA" DOES NOT REQUIRE A PHYSICAL PRESENCE IN THE STATE

This phrase is not defined in the CCPA. It has, under California tax laws, been deemed to apply, in certain cases, to companies doing business online without any physical presence in California.

So, in the absence of guidance from the California Attorney General, it is likely that this will include you if:

- You have employees in California.
- You are an entity incorporated in California or an entity required to register in California as a "foreign entity" under existing California corporate and tax law. Per a recent amendment, as of April 1, 2019, companies not registered in California, with no physical presence in California, are required to register with the California Department of Tax and Fee Administration (CDTFA), collect the California use tax and pay the tax to the CDTFA based on the amount of sales into California, if their sales exceed a certain dollar threshold or they have more than 200 separate transactions.
- You have ties to the state including, in some cases, repeated sales into the state and ownership of real property in the state.

Consult with counsel to determine whether you fall in scope. If you do, below are some first steps to take:

1. CREATE NEW PRIVACY NOTICES

You need to adopt and maintain four privacy notices: notice of collection, notice of opt-out, notice of financial incentive and a privacy policy. What does this mean?

Create a ***Notice at Collection.***

- This needs to be made **readily available where consumers will see or encounter it** at or before the point of collection of any personal information.
- **Include** the information collected, purpose, whether or not there is a "sale" and a link to your privacy policy.
- Be **comprehensive and precise**. Draft in a way that is **very user-friendly**. This means that your notice must:
  - Use plain, straightforward language – such that the notice is understandable to an average consumer.
  - Avoid technical or legal jargon.
  - Be written in a way that consumers understand.
  - Use a format that draws the consumer's attention to the notice and makes the notice easy to read, including on smaller screens, if applicable.
  - Be available in the languages in which the business, in its ordinary course, provides contracts, disclaimers, sale announcements and other information to consumers.
  - Be accessible to consumers with disabilities. (At a minimum, for notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Consortium. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.)

Create a ***Notice of Opt Out***.

If you **sell personal information** (the way that this is defined in CCPA):

ODIA KAGAN
PARTNER

- **Provide the notice.** You need to provide a notice of the right to opt out.
- Draft the notice to be "**very user-friendly**" (as explained above).

You **do not have to provide a notice to opt out if**:

- You will not sell personal information during the time period a notice to opt out is not posted; and
- State unequivocally in your privacy policy that you do not and will not sell personal information. This has been a point of recent enforcement by the California Attorney General.
- Create a notation in your records of all information collected during this time as being **information of consumers who had exercised the right to opt out**. This way, if you change your practice going forward – you will have an opt-out list.

Create a ***Notice of Financial Incentive***.

Before **drafting the notice:**

- Review the documentation of your financial incentive.
- **Analyze,** using a reasonable and good faith method, whether it meets with the requirement that the price or difference is **directly related to** the value provided to the business by the consumer's data (or "the value of the consumer's data") and **document your analysis**.
- **Use the criteria for the analysis** provided in the regs.

The notice:

- **Provide the notice** of financial incentive.
- Draft in a **very user-friendly** manner (see above).
- **Include the information required** in the law/regs. This should include an explanation of why the financial incentive or price or service difference **is permitted** under the CCPA.
- Create a process for operationalizing the right to opt in and to withdraw that is easy for consumers to execute.

2. REVISE YOUR ONLINE PRIVACY NOTICE

- Not just website data collection! Make sure that it includes your **online and offline practices** regarding the collection, use, disclosure and sale of personal information.
- Draft the notice in a **very user-friendly** manner. (see above)
- **Include** the following information:
  - A description of **the right to know** and how to exercise it.
  - **What information you collect,** the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom you share the personal information.
  - Whether you have disclosed/sold personal information.
  - A description of the **right to request deletion** and how to exercise it.
  - A description of your **method for verifying the consumer's identity** (or if there is **no reasonable method, a statement to that effect and an explanation** of why you do not have any reasonable method by which you can verify the identity of the requestor).
  - A description of the **right to opt out of a sale** and how to exercise it.
  - A description of the **right to non-discrimination.**
  - **An explanation of how a consumer can designate an authorized agent** to make a request under the CCPA on the consumer's behalf.
  - A contact for more information.
  - The **date the privacy policy was last updated.**
- If you **collect or process the personal information of 10 million consumers** or more a year:
  - Number of each type of request that you have received in the past 12 months
  - Whether you complied with the request in whole or in part or whether you denied it
  - The median or mean number of days it took you to substantively respond to each type of request.

3. REVISE YOUR PROCESS FOR VERIFYING THE IDENTITY OF CONSUMERS MAKING KNOW/DELETION REQUESTS

- Establish or revise and maintain your written, reasonable method for verifying the identity of the person making a request to know or to delete.
- Establish and implement **reasonable security measures** to detect fraudulent identity verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

- You generally cannot require the consumer to pay a fee for the verification.
- Use the **principles** set forth in the regs to devise the **process**. Whenever feasible, use the information that you already have about the consumer and refrain from asking for sensitive information.
  - Consider the **type, sensitivity and value** of the personal information.
  - Consider the **risk of harm to the consumer** posed by any unauthorized access or deletion.
- Establish a process for **evaluating on a yearly basis** whether a reasonable verification method can be established and document its evaluation.

4. REVISE YOUR PROCESS FOR RESPONDING TO KNOW (ACCESS) REQUESTS

Before responding:

- Create or revise the two or more **methods you will make available** for submitting requests. **At minimum** (with some exceptions):
  - A toll-free telephone number and interactive web form accessible through the website or mobile application.
  - Additional method reflecting the manner in which you primarily interact with the consumer (e.g. paper form for point-of-sale retailers).

If you interact with consumer in person – consider a printed form/tablet or portal for submitting the requests.

- Create a process for identifying and responding to **requests not made through the designated process** (e.g. specific directions as to how make the request using the designated method).
- Create a process that **ensures that you do not at any time disclose** a consumer's 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 or security questions and answers.
- Create a process that **allows denying requests for specific pieces of information** if:
  - The disclosure creates a substantial, articulable and unreasonable risk to the security of that personal information, the consumer's account, or the security of your systems or networks.
  - There is a conflict with federal or state law.
  - There is an exception to the CCPA.
- Implement **reasonable security measures** for transmitting personal information to the consumer as part of a response.
- Devise/implement a process for dealing with requests pertaining to **household information.** (A household is defined as a person or group of people who reside at the same address, share a common device or the same service provided by a business and are identified by the business as sharing the same group account or unique identifier.)

For the response, create/implement a process that includes:

- **An initial response** within 10 business days confirming receipt and describing how you will verify identity and process the request. The response may be given in the same manner in which the request was received.

You need to adopt and maintain four privacy notices: Notice of collection, notice of opt-out, notice of financial incentive and privacy policy

- **The ability to request additional time** to respond, and the reason.
- **A notice of problem with verification** that includes an explanation of your inability to verify and (i) for a request for specific pieces of information – a possible response with categories of information; and (ii) for a request for categories of information – a possible link to an explanation of your common data processing practices.
- **Full response**: (Must be provided within 45 calendar days)

If you are granting the request (a YES response)

  - Avoid referring the consumer to your general practices outlined in the privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required

to be in a response to a request to know such categories.
  - Provide the information for each identified category of personal information collected about the consumer.

If you are denying the request (a NO response)
  - Explain why.
  - If only some disclosure is prevented, provide the rest.
  - For household request – If you cannot verify the identity you may provide aggregate household information, subject to verification requirements.

5. REVISE YOUR PROCESS FOR RESPONDING TO DELETION REQUESTS

Before responding:

- Assess whether it makes the most business sense for you to comply with deletion requests by a **complete deletion or, alternatively, through de-identification or aggregation**.
  - If de-identification – (i) make sure that it meets with the definition of de-identification and (ii) for sensitive information – consider getting a third party to confirm the de-identification.
- Conduct/revise your analysis of which **exceptions to the right to delete** may apply to you and make sure to assess whether those cover all of the information or only parts of it (if only parts – you would need to disclose the rest).
- Create or revise the two or more **methods you make available** for submitting requests.
- **A two-step process may be used but is not required** for online requests to delete, where the consumer must (i) clearly submit the request and (ii) separately confirm that they want their personal information deleted.
- Create a process for identifying and responding to **requests not made through the designated process** (e.g. specific directions as to how make the request using the designated method).
- Create a process for dealing with requests pertaining to **household information.**
- For **backup** – ensure that information is deleted, following the receipt of the deletion request, the next time that the archive or backup system is restored to an active system or accessed or used for a sale, disclosure or commercial purpose.

For the response: Create/implement a process that includes:

- **Initial response** (see above)
- **Request for additional time** (see above)
- If you like – **a notice presenting an option to delete only a selected portion** of the data, provided that (i) you also offer a global option to delete all personal information; (ii) you present the offer to delete all information more prominently than the other choices; (iii) you use the **two-step process (outlined above) for this**.
- Notice of problem with verification
  - Tell the consumer that you cannot verify their identity.
  - Provide an explanation of why you do not have any reasonable method by which you can verify.
  - Treat the request as an **opt-out of sale** and inform the consumer of this fact.
- **Full response** which includes:
  - Specify the **manner in which you deleted.**
  - Indicate that you will **maintain a record of the request** as required by the regs.
  - For a **denial of the request**: Provide the basis of denial, delete information not subject to an exception and use the information retained per an exception only as permitted by the exception.

6. REVISE YOUR PROCESS FOR RESPONDING TO OPT-OUT REQUESTS

Before responding:

- Create or revise the two or more **methods you make available** for submitting requests. **At minimum:**
- An interactive web form accessible through a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on your website or mobile application.
- Additional method reflecting the manner in which you primarily interact with the consumer (e.g. paper form for point-of-sale retailers)
- Incorporate into your process the ability to **submit a request through an authorized agent.**
- If you like – add into the process a **choice for the consumer to opt out of sales of certain categories** of personal information provided that (i) You also offer a global option to opt out of the sale of all personal information; (ii) You present the global option more prominently than the other choices.

- Revise your process so that it:
  - Allows you to respond as soon as feasibly possible but not later than **within 15 business days** from the date you received the request.
  - If you sell a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, notify those third parties that the consumer has exercised their right to opt-out and direct those third parties not to sell that consumer's information.
  - Allows you to **deny a request** if you have a good-faith, reasonable and documented belief that a request to opt out is fraudulent.

7. REVISE YOUR AGREEMENTS WITH THIRD-PARTY VENDORS

- Prohibit your service providers from using consumers' personal information received in connection with the services provided to one business client for another except for the following reasons:
  - To **retain and employ another service provider** as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and the regulations
  - For **internal use by the service** provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source
  - To **detect data security incidents** or protect against **fraudulent or illegal activity**
  - To comply with **federal, state or local laws**
  - To comply with **a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal, state or local authorities**
  - To **cooperate with law enforcement agencies** concerning conduct or activity that the business, service provider or third party reasonably and in good faith believes may violate federal, state or local law
  - To **exercise or defend legal claims**
- Require your service providers to **devise a process for recognizing and fielding consumer requests** and conveying them to the right business client.
- Address in your agreement with the service provider **who answers consumer requests,** you or the service provider.
- If **you will be responding to the requests**, require the service provider, in your agreement, to devise a process for responding to consumer requests, to inform them that the request cannot be acted upon because it was sent to a service provider.

8. REVISE OR DEVELOP RECORDS RETENTION AND TRAINING PROGRAMS

Records Retention:

- Maintain **records of consumer requests** made pursuant to the CCPA and how you responded to said requests for at least 24 months.
- **Retain all signed declarations** collected in connection with requests to know specific pieces of information. (Signed means physically signed or provided electronically under the Uniform Electronic Transactions Act.)
- **Avoid using records for any other purpose** than for record-keeping.

Training:

- **Revise or create a training policy** to ensure that all individuals responsible for handling consumer requests or your compliance with the CCPA are informed of all the requirements in the regulations and the CCPA.
- **Document and comply** with the training policy.

Note: The regulations also include special requirements in the event you collect the personal information of children and if you are a service provider, which are not covered in this article. ■

Odia Kagan is a partner at Fox Rothschild LLP and Chair of the firm's GDPR Compliance & International Privacy Practice.

She can be reached at okagan@foxrothschild.com