What CCPA Means For:

1. **A Business that Collects a Consumer’s PI**
   - Provide notice at or before point of collection with categories of PI and purposes of use. 1798.100(b) *May not collect additional categories or use data for other purposes.*
   - Upon request, respect right to request deletion (subject to exceptions). 1798.105
   - Upon request, inform consumer about (i) categories of PI collected, (ii) sources, (iii) business or commercial purpose, (iv) categories of 3rd parties with who PI is shared, (v) specific pieces of PI collected. 1798.110 (a)(c). *If PI is not disclosed for a business purpose or sold, tell the consumer.*

   A service provider is not a “Third Party” if the PI is disclosed pursuant to a written contract that (i) prohibits the SP from retaining, using, or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract, retaining, using, or disclosing the PI outside of the direct business relationship between the SP and the business, AND (ii) includes a certification that the person understands the restrictions and will comply with them. 1798.140(w)

   - Upon request, inform consumer about (i) categories of PI collected, and (ii) the categories of PI disclosed for a business purpose. 1798.115 (a)(c)

   - Provide notice that PI is sold and tell consumers about right to opt-out. 1798.120(b)

   - Upon request, inform consumer about (i) categories of PI collected, (ii) categories of PI sold and categories of third parties to whom the PI was sold (by categories, so third party types are mapped to categories of PI). 1798.115 (a)(c)

   - Only sell data of children under 16 with opt-in consent. 1798.120(c)
   - If a person opts out, do not ask for permission to sell for 12 months 1798.135(a)(5)
   - Disclosures to Service Providers are not sales of PI, if done pursuant to a written contract, provided that the contract prohibits the SP from retaining, using, or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by this title. 1798.140(v)

2. **If PI is Disclosed for a Business Purpose**
   - Provide notice that PI is sold and tell consumers about right to opt-out. 1798.120(b)

3. **If PI is Sold**
   - Provide notice that PI is sold and tell consumers about right to opt-out. 1798.120(b)

Definitions:

1. Collect”… means buying, renting, gathering, obtaining, receiving, or accessing any PI by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer’s behavior. 1789.140(e)

2. Per 1798.130(c), the categories of PI required to be disclosed shall follow the definitions of PI in 1798.140.

3. Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. [Laundry list of possible types of PI] 1798.140(o) Note: the definition of PI includes “unique personal identifier” which is defined in 1798.140(x) as “a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to …. customer number unique pseudonym, or user alias,… or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.” [CCPA also excludes deidentified or aggregate consumer information from the definition of PI. But see those definitions on the next page.]

4. “Business purpose” means the use of PI for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use shall be reasonably necessary and proportionate to achieve the operational purpose for which the PI was collected… Business purposes are: (1)…, (2)security incidents, preventing fraud…(3) … (4)-term, transient use, provided the PIs not disclosed to another third party and is not used to build a profile about a consumer… (5)services on behalf of the business…(6)Internal research for technological development… (7)to verify, maintain and upgrade quality or safety of a service or device 1798.140(d)

5. “Sell” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration. [Does not include disclosures (A) intentionally directed by the consumer, (B) for opt-out management, (C) to service providers, (D) as part of M&A.] 1789.140(t)
A Business that Collects a Consumer’s PI

- Accept contractual terms 1798.140(v), 1798.140(w)
- Certify compliance 1798.140(w) and only process the PI per the contract (for the specified business purpose)
- Delete records as directed 1798.105(c)

CCPA does not require companies to retain PI collected for a single one-time transaction if that PI is not retained in the ordinary course of business or to reidentify PI that is not maintained in a manner that would be PI. 19798.100(e)(f)

CPA does not restrict a business ability to: (5) collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information. 1798.145(a):

“Aggregate consumer information” means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. “Aggregate consumer information” does not mean one or more individual consumer records that have been deidentified. 1798.140(a)

“Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information: (1) implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain. (2) implemented business processes that specifically prohibit reidentification of the information. (3) implemented business processes to prevent inadvertent release of deidentified information. (4) no attempt to reidentify the information. 1798.140(h) Given the definition of PI, we must assume that deidentified data does not contain any unique identifiers; it must be anonymized not pseudonymized.

GLBA Exception. This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150. 1798.145(e).

Other 1798.145 exceptions: FCRA, CMIA/HIPAA/Clinical Trial, DPPA, compliance with laws, et al.

A Service Provider receiving PI for a business purpose

A Third Party Receiving Sold PI

A Third Party Receiving PI that was Disclosed FABP

CCPA is not clear that notice and choice obligations do not apply directly to service providers, but common sense would dictate that these are “controller” obligations that belong to the business-that-collects.

A third party shall not sell PI that has been sold to it without the consumer having been given notice and choice. (Resale of PI is restricted.) 1798.115(d)

Not clearly specified in CCPA. Given that the definition of “collect” encompasses “receipt” of PI, you should just be a Business that Collects a Consumer’s PI. If so, then you have to consider compliance with the notice requirements. The sensible interpretation would be this: if you receive data for a BP and use it solely and proportionately for that BP (and related BPs), the notice given by the original business covers it. But, if you want to use the data independently, then (as a business that collects) you have to give notice, etc. Consider leveraging processes to comply with GDPR Art 14 (indirectly collected data).