Assessment of California's Data Protection Regime as Substantially Equivalent and Low Risk by the Dubai International Financial Centre Authority ("DIFC" or "DIFCA") Commissioner of Data Protection ("Commissioner")

DIFC

Table of Contents

Introduction

Articles 26 and 27 of the Data Protection Law, DIFC Law No. 5 of 2020 and Section 5 of the DIFC Data Protection Regulations 2020 (the "DIFC DP Law 2020") address transfers of Personal Data to Third Countries or International Organisations. Article 26(2) specifically states:

> *For the purposes of Article 26(1), the Commissioner may determine from time to time that a Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection.*

Recognition of the equivalence of another jurisdiction's data protection regime, also known as adequacy, is based on an assessment of key data protection concepts and obligations found in local data protection laws to ensure equivalence with the exporting jurisdiction or international organisation's data protection law. As such, the DIFC Office of the Commissioner of Data Protection assessed California's laws and regulations according to the fundamental data protection principles and criteria, including but not limited to:

1. Basic data protection concepts and definitions

2. Grounds for lawful and fair processing for legitimate basis

    a. Legitimate bases for processing
    b. Controller and Processor obligations

3. Existence of Data Protection Principles
    a. purpose limitation
    b. data quality and proportionality
    c. data retention
    d. security and confidentiality
    e. transparency

4. Data Subjects' Rights
    a. right of access, rectification, erasure and objection

5. International / Onward Data Transfer Restrictions

6. Security of Processing and Breach Reporting

7. Accountability
    a. Special categories of data (aka sensitive personal data)
    b. Direct marketing
    c. Automated decision making and profiling

8. Additional content principles for specific types of processing

9. Existence of international commitments and conventions binding on California or its membership of any multilateral or regional organisations.

Observation 1: Basic data protection concepts and definitions

California has enacted a standalone data protection law, the California Consumer Privacy Act of 2018 ("**CCPA**"), which gives consumers protection over personal data collected by businesses. The CCPA was amended by the California Privacy Rights Act of 2020 ("**CPRA**") which took effect on 1 January 2023 (together "**Amended CCPA**")[1].

The Amended CCPA sets out, among other things, consumer rights as well as obligations on businesses including providing privacy notices to consumers.

The California Consumer Privacy Act Regulations ("**CCPA Regulations**") provide procedures and guidance on the implementation of the Amended CCPA – providing clarity on the rights, concepts and requirements of the law.

Please note that the California approach addresses consumer information primarily, which is tantamount to personal data of data subjects as consumers. Throughout this Decision, please read the assessment of the Amended CCPA and CCPA Regulations in this context.

The DIFC Ethical Data Management Risk Index ("**EDMRI**") assessment of California importers is currently low risk.[2]

Summary of key obligations / changes reflected in California's data protection regime

- **Concepts and definitions:**
- **Breach notification requirements:**
- **Enforcement powers:**
- **Notifications to the Commissioner / Supervisory Authority:**
- **Powers and objectives of the Commissioner:**

1. Data protection laws of California

The Amended CCPA protects personal information and grants rights to California residents who reside in California or are based outside the state temporarily. [3]

Under the Amended CCPA, personal information is defined as "*information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*"[4]. This includes name, alias, postal address, unique personal identifier, online identifier, email address, social security number, driver's license number, passport number, biometric information, geolocation data, professional or employment related information and sensitive personal information. It does not include publicly

[1] Codes Display Text (ca.gov)
[2] https://www.difc.ae/business/operating/data-protection/guidance/#s17
[3] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General
[4] §1798.140(v)(1) of the Amended CCPA.

available information (as defined in §1798.140(v)(2) of the Amended CCPA) or consumer information that is deidentified or aggregate consumer information.

The Amended CCPA, applies to for-profit entities that conduct business in California, collect consumer personal information and which meet one or more of the following criteria[5]:

- *As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year;*
- *Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or households; or*
- *Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.*

The Amended CCPA, therefore, generally does not apply to non-profit organisations or government agencies. [6]

§1798.145(a)(7) of the Amended CCPA, explains the territorial effect of the law. In brief, the Amended CCPA does not restrict a business' ability to collect and process personal information if every aspect of that *"commercial conduct takes place wholly outside of California". The Amended CCPA* further explains that commercial conduct takes place wholly outside of California occurs if:

- the business collected that information while the consumer was outside of California,
- no part of the sale of the consumer's personal information occurred in California, and
- no personal information collected while the consumer was in California is sold.

Notwithstanding, §1798.145(a)(7) also states that there is no prohibition on a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

2. Non-privacy laws which include data protection elements

Additionally, California has other sectoral laws and regulations with privacy features. A list of the major privacy protection laws at state and federal level can be found on the California Offices of the Attorney General's ("**OAG**") website. These include:

California Law

- California Constitution, Article 1, section 1 gives each citizen an "inalienable right" to privacy.
- Information-Sharing Disclosure, "Shine the Light" - California Civil Code sections 1798.83-1798.84.
- Computer Misuse and Abuse: Criminal Sanctions - California Penal Code section 502.

[5] §1798.140(d)(1) of the Amended CCPA.
[6] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

- Automobile "Black Boxes" - California Vehicle Code section 9951
- California Electronic Communications Privacy Act (CalECPA) - Penal Code section 1546 et seq.
- Information Practices Act of 1977 - California Civil Code section 1798 and following.

Federal Law

- Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code section 6501 and following.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Driver's Privacy Protection Act of 1994 - 18 U.S. Code 2721 and following.
- Federal Privacy Act of 1974 - 5 U.S. Code section 552a.
- Telephone Consumer Protection Act (TCPA) - 47 U.S. Code section 227.
- Fair Credit Reporting Act (FCRA) – 15 U.S. Code section 1681-1681u.
- Gramm-Leach-Bliley Act (GLBA) – 15 U.S. Code section 6801 and following.

3. Regulatory/Supervisory Authorities

The CPRA created the California Privacy Protection Agency ("**CPPA**") and granted it administrative power under §1798.155 of the Amended CCPA. The CPPA also has rulemaking authority and published the CCPA Regulations to reflect the CPRA amendments. These can be found on the CPPA website, here. The Amended CCPA in §1798.199.40 sets out the functions of the CPPA including to administer, implement, and enforce through administrative actions of the Amended CCPA and provide guidance to consumers regarding their rights.

Although powers were transferred from the OAG to the CCPA, the Attorney General still retains enforcement powers.[7] More information on these powers is set out in Observation 7 of this Assessment.

[7] California Consumer Privacy Laws – CCPA & CPRA | Bloomberg Law

Observation 2: Grounds for lawful and fair processing for legitimate purposes

Lawful Grounds

The Amended CCPA sets out the lawful grounds for processing in the definition of "business purpose" in §1798.100(c). The law specifies that "*the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected."*

Section 7002 of the CCPA Regulations explains that businesses subject to the CCPA must limit the collection, use, and retention of your personal information to only those purposes that: (1) a consumer would reasonably expect, or (2) are compatible with the consumer's expectations and disclosed to the consumer, or (3) purposes that the consumer consented to, as long as consent was not obtained through dark patterns. For all of these purposes, the business' collection, use, and retention of the consumer's information must be reasonably necessary and proportionate to serve those purposes.

If a business does not disclose the categories of personal information it is collecting, the purpose(s) for which they will be used, whether they will be should or shared, and the length of time the business intends to retain them, the business cannot collect that personal information.[8]

Whether a disclosed purpose is a "business purpose," as defined in § 1798.140(e)(1)-(8), factors into whether it is a use compatible with the consumer's expectations. These business purposes are:

"(1) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

(5) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

[8] Section 7002(f) and 7012 of the CCPA Regulations.

(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

(7) Undertaking internal research for technological development and demonstration.

(8) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business."

Legal Obligations

The Amended CCPA sets out exceptions in §1798.145(a) including where businesses are required to fulfil their legal obligations such as to:

- comply with federal, state or local laws or court orders.
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

- cooperate with law enforcement agencies concerning conduct which may violate federal, state, or local law.

- in certain circumstances, cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury.

Further exceptions include the *"(5) ability to exercise or defend claims, (6) collect, use, retain, sell, share, or disclose consumers' personal information that is deidentified or aggregate consumer information or (7) collect, sell, or share a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not prohibit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California."*

Consent

Section 7002 of the CCPA Regulations allows the processing of personal information outside of their reasonable expectations and compatible disclosed purposes if the consumer gives consent. The Amended CCPA defines "consent" in § 1798.140(h) as "any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer…signifies agreement to the processing of personal information relating to the

consumer for a narrowly defined particular purpose." It further states that "agreement obtain through use of dark patterns does not constitute consent."

Section 7004 of the CCPA Regulations explains that methods for obtaining consent must be easy to understand, provide symmetry in choice, avoid language or interactive elements that confuse the consumer, avoid choice architecture that impairs or interferes with the consumer's ability to make a choice, and be easy to execute.

Sensitive Personal Data

Under §1798.140(ae) of the Amended CCPA, sensitive personal information includes, but is not limited to, personal information which reveals a consumer's social security, driver's license, state identification card, or passport number, financial information, precise geolocation, racial or ethnic origin, religious beliefs, contents of a consumer's mail, email and text messages, genetic data, biometric information, health information or sexual orientation. Publicly available information, however, is not included in the scope of sensitive personal information.

The Amended CCPA has the obligation to inform consumers of certain information (assessed further in Observation 4 of this Assessment). In respect to sensitive personal information, controllers must, at or before the point of collection, inform consumers:

- if it collects sensitive personal information, the categories of sensitive personal information to be collected, the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.[9]

- the length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.[10]

§1798.135 of the Amended CCPA, sets out the methods of limiting the use and disclosure of sensitive personal information. Sub-section (a) requires businesses that use or disclose consumer sensitive personal information for purposes other than those authorized by subdivision (a) of Section 1798.121 (set out in Observation 4 of this Assessment) to provide, for example, a clear and conspicuous link on the business's internet homepages, titled "Limit the Use of My Sensitive Personal Information", which enables a consumer to limit the use or disclosure of the consumer's sensitive personal information to certain authorized uses.

[9] §1789.100(a)(2) of the Amended CCPA.
[10] §1789.100(a)(3) of the Amended CCPA.

Please refer to Observation 4 in this Assessment for “Consumers’ Right to Limit Use and Disclosure of Sensitive Personal Information”.

Sale or Sharing Personal Data

§1798.135 of the Amended CCPA, also sets out the methods for limiting the sale or sharing of personal information. Businesses that sell or share personal information must provide a clear and conspicuous link on the business’s internet homepages, titled “Do Not Sell of Share My Personal Information,” or “Your Privacy Choices” or “Your California Privacy Choices.” Businesses must also consider opt-out preference signals conforming to the technical specifications set forth in CCPA Regulations and sent by the consumer, as a valid request to opt-out of sale or sharing of their personal information.

Businesses that process opt-out preference signals in a frictionless manner, as set forth in CCPA regulations, have the option of not posting a “Do Not Sell of Share My Personal Information” link, The CCPA Regulations explain these methods in further detail[11].

Children’s Data

Under §1798.120(c) of the Amended CCPA, businesses must not sell or share personal information of consumers if there’s actual knowledge that the consumer is less than 16 years old. Consumers aged between 13 years and less than 16 years, must consent before the business can sell or share their personal information. For consumers aged less than 13 years, their parent or guardian, must consent before the business can sell or share the consumer’s personal information.

The CCPA Regulations, in Article 6 titled “Special Rules Regarding Consumers Under 16 Years Of Age”, further explain the rules regarding consumers under 16 years of age including the process for opting-in to the sale or sharing of personal information, methods of determining parental or guardian consent (for consumers less than 13 years of age) and the obligation on businesses to inform consumers (or their parents/guardians of minors) of their right to opt-out of the sale or sharing.

A business should consider a consumer’s age. Otherwise, if the business wilfully disregards age criteria, businesses are deemed to have had actual knowledge of it.

Business must wait until the consumer attains 16 years of age before asking them to consent to the sale or sharing of their personal information, but if they have previously instructed the

[11] §§ 7025-7026 of the CCPA Regulations.

business not to sell or share their personal information, they must wait 12 months before requesting consent.[12]

Observation 3: Existence of Data Protection Principles

The adequacy assessment evaluated the framework of the California law and regulations with respect to the following data protection principles, inter alia:

a. purpose limitation;

b. data quality and proportionality;

c. data retention;

d. security and confidentiality; and

e. transparency.

§1798.100 of the Amended CCPA sets out the general duties of businesses that collect personal information. Within the obligation to inform consumers at the point of collection of the purposes for which the categories of personal data are collected, it sets out, among other things:

- that no additional categories of personal information should be collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with an adequate notice;

- the retention of each category of personal information or the criteria used to determine the period (provided it is not retained for longer than is reasonably necessary for the disclosed purpose); and

- A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.[13]

§1798.130(a)(3)(B) of the Amended CCPA similarly sets out the methods of disclosing the information that is collected to a consumer.

§ 7004 of the CCPA Regulations set out principles in relation to the methods for submitting CCPA requests and obtaining consumer consent. These include:

[12] §1798.135(c)(5) of the Amended CCPA.
[13] §1798.100(c) of the Amended CCPA; § 7002 of the CCPA Regulations.

- Using methods with language which is easy for consumers to read and understand.
- Symmetry in choice. The more privacy-protective option for consumers should not be longer, more difficult or time-consuming because that would interfere with the consumer's ability to make a choice.
- Avoiding language or interactive elements that are confusing to consumers such as double negatives.
- Avoiding design methods that impairs or interferes with the consumer's ability to make a choice as consent must be freely given, specific, informed, and unambiguous.
- Using methods which are easy to execute and does not add unnecessary burden or friction to the process by which the consumer submits a CCPA request.

The OAG explains in FAQs, Section G, entitled "Right to Non-Discrimination" that businesses cannot deny its goods or services, change its pricing, or provide a different level or quality of goods or services just because a consumer exercised their rights under the Amended CCPA. If, however, that personal information or sale is necessary for the business to provide goods or services, the business may not be able to complete that transaction.

Businesses can also offer promotions and deals in exchange of consumers personal information - if the promotion is reasonably related to the value of the personal information. If a consumer exercises their right, for example, to the deletion of personal data, they may not be able to continue participating in the deal.[14]

Businesses may compensate consumers for collecting, selling, and deleting personal information. Compensation must be reasonable and made in good faith, and can't be usurious, coercive, or unfair. Additionally, section 1798.125(a)(2) states that non-discrimination rights do not mean that a business cannot raise or lower its prices or change service levels if the delta is reasonable and proportionate to the value of the consumer information.

While the Amended CCPA addresses rights in the context of the individual as a consumer, the DIFC DP Law 2020 adopted these particular elements in the context of data subjects' right to non-discrimination.

[14] https://www.oag.ca.gov/privacy/ccpa#sectiong

Observation 4: Data Subjects' Rights (DSR)

The Amended CCPA sets out various DSR including:

1. §1789.105 – Right to Delete Personal Information;
2. §1789.106 – Right to Correct Inaccurate Personal Information (newly added by the CPRA);
3. §1789.110 –Right to Know What Personal Information is Being Collected. Right to Access Personal Information
4. §1789.115 - Right to Know What Personal Information is Sold or Shared and to Whom;
5. §1789.120 - Right to Opt Out of Sale or Sharing of Personal Information;
6. §1789.121 - Right to Limit Use and Disclosure of Sensitive Personal Information (newly added by the CPRA); and
7. §1789.125 - Right of No Retaliation Following Opt Out or Exercise of Other Rights.

In order to further comply with Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125, businesses must follow the Notice, Disclosure, Correction, and Deletion Requirements under §1798.130.

These requirements include (in reasonably accessible form to consumer), particularly for sections 1798.105, 1798.106, 1798.110, 1798.115:

- making available two or more methods for submitting requests including, at a minimum, a toll-free telephone number. The CCPA Regulations under Article 3, § 7020(a) explain that a business which only has online operations and has a direct relationship with a consumer from whom it collects personal information may only provide an email address for submitting requests. A business with an internet website should make available the submission of requests on the website through a webform. Article 3, § 7020(e) of the CCPA Regulations further explain that if a consumer submits a request in a manner that is not one of the designated methods of submission, the business must either treat the request as if it had been submitted in a designated manner or explain to the consumer how to submit the request.

- disclosing the required information to a consumer free of charge, and responding to all verifiable consumer requests within 45 days after promptly determining whether the request is a verifiable consumer request. This period may be extended once by an additional 45 days when reasonably necessary, where the consumer is provided notice of the extension within the first 45-day period. Article 3, § 7021(a) of the CCPA Regulations explains that no later than 10 business days after receiving a request to delete, request to correct, or request to know or a request to delete, a business shall confirm receipt of the request and provide information about how the business will process the request.

- disclosing the required information in writing and in a readily useable format.

- disclosing the required information which covers the 12-month period before the business' receipt of the verifiable consumer request, unless the consumer requests information beyond the 12-month period which the business should provide unless doing so proves

impossible or would involve a disproportionate effort. The request for information beyond the 12-month period, shall only apply to personal information collected on or after January 1, 2022.

- where a verifiable consumer request pursuant to §1798.110 or §1798.115 is received, a business shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor is not required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to §1798.110 or §1798.115, in their capacity as service provider or contractor but shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request such as providing consumer's personal information obtained as a result of providing services to the business, and by correcting inaccurate information or by enabling the business to do the same.[15]

- disclosing required information in its online privacy policy or on its internet website and updating this at least once every 12 months. This information includes a description of a consumer's rights and two or more designated methods for submitting requests as well as information described further below in §1798.110 and §1798.115.

- ensuring all individuals responsible for handling consumer inquiries about the business' privacy practices or compliance, are informed of all consumer rights and requirements under Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.125, and 1798.130, and how to direct consumers to exercise their rights under those sections;

- using any personal information collected for consumer verification solely for the purposes of verification and not disclosing this further, retaining it for longer than necessary for purposes of verification, or using it for unrelated purposes.

§1789.105 – Right to Delete Personal Information

Consumers have the right to request a business delete any of the personal information it is processing. Businesses that collect personal information about consumers shall disclose information about consumers rights to request the deletion of such personal information.

Upon receipt of a verifiable request, businesses shall delete the consumer's personal information from its records, notify any service providers or contractors to do the same, and notify all third parties where the personal information was sold or shared to delete the consumer's personal information - unless this proves impossible or disproportionate.

Under §1789.105(c)(3), service providers must cooperate with this right. Article 3, § 7022© of the CCPA Regulations newly set out how service providers should do this.

There are certain exceptions where it is reasonably necessary to maintain the consumer's personal information such as to complete the transaction for which the personal information was

[15] §1789.105(c)(3) of the Amended CCPA.

collected, help ensure security and integrity of the consumer's personal information is reasonably necessary and proportionate for those purposes, debug to identify and repair errors that impair existing intended functionality, exercise free speech and to comply with a legal obligation.

§1789.106 –Right to Correct Inaccurate Personal Information

This right was added by the CPRA and grants consumers the right to request inaccurate personal information held by a business about the consumer to be corrected. Similar to the right to delete, businesses that collect personal information about consumers shall disclose the consumer's rights to request correction of inaccurate personal information.

Upon receipt of a verifiable request, businesses shall use commercially reasonable efforts to correct the inaccurate personal information.

Article 3, §7023 of the CCPA Regulations sets out the process and considerations for this right including the various reasons and processes for denying a request (such as if a business cannot verify the identity of the requestor; after considering the totality of the circumstances relating to the contested personal information determining that it is more likely than not accurate or if the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months of receiving the request without any additional documentation to prove the inaccuracy).

The CCPA Regulations also explain that businesses should instruct all service providers and contractors that maintain the personal information at issue to make the necessary corrections in their respective systems. Service providers and contractors are obliged to comply with the business's instructions to correct the personal information or enable the business to make the corrections. Any personal information that is subject to correct which is on archived or backup systems may delay in compliance with the request to correct until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

A business may delete the contested personal information instead of correcting it, if the deletion does not negatively impact the consumer, or the consumer consents to the deletion.

§1789.110 – Right to Know What Personal Information is Being Collected. Right to Access Personal Information

Consumers have the right to request from a business that collects personal information about the consumer to disclose to the consumer: [16]

- the categories of personal information it has collected about that consumer.
- the categories of sources from which the personal information is collected.
- the purposes for collecting, selling, or sharing personal information.

[16] §1789.110(a) of the Amended CCPA.

- the categories of third parties to whom the business discloses personal information.
- the specific pieces of personal information it has collected about that consumer.

In addition to the aforementioned requirements of §1798.130, further obligations are placed on businesses.

Article 3, § 7024(i) of the CCPA Regulations also explains that service providers or contractors must assist a business responding to a verifiable request.

§1789.115 - Right to Know What Personal Information is Sold or Shared and to Whom

Consumers have the right to request disclosure of their personal information which that business sells or shares a business purpose, including[17]:

- the categories of personal information that the business collected about the consumer.
- the categories of personal information that the business sold or shared about the consumer and the categories of third parties to whom the personal information was sold or shared.
- the categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

In addition to the aforementioned requirements of §1798.130, further obligations are placed on businesses.

A business that sells or shares consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose to consumers i. the categories of consumers' personal information it has sold or shared, or the fact that the business has not sold or shared consumers' personal information and ii. the categories of consumers' personal information it has disclosed for a business purpose, or the fact that the business has not disclosed consumers' personal information.

Third parties must not sell or share consumer personal information that has been sold to, or shared with, the third party by a business, unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to §1798.120.[18]

§1789.120 - Right to Opt Out of Sale or Sharing of Personal Information

Consumers have the right, at any time, to direct a business not to sell or share their personal information to third parties.

[17] §1798.115.(a) of the Amended CCPA.
[18] §1798.115.(d) of the Amended CCPA.

Businesses must provide notice to consumers that this information may be sold or shared and that consumers have the "right to opt-out" of the sale or sharing of their personal information.

Please see our Children Data section of this Assessment which explains how businesses should handle the selling or sharing of personal information of consumers less than 16 years of age.

§1789.121 - Right to Limit Use and Disclosure of Sensitive Personal Information (newly added by the CPRA)

Consumers shall have the right, at any time, to direct a business that collects their sensitive personal information to limit its use of that information to that which is necessary, for certain business purposes and under certain exceptions. The CCPA Regulations list these out in Article 3, §7027(m) which are:

- to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services.
- to prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information.
- to resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions.
- to ensure the physical safety of natural persons.
- for short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.
- to perform services on behalf of the business.
- to verify or maintain the quality or safety of a product, service, or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured by, manufactured for, or controlled by the business.
- to collect or process sensitive personal information where the collection or processing is not for the purpose of inferring characteristics about a consumer.

Like the DIFC DP Law, the CCPA Regulations provide that where businesses process personal information for other purposes to provide two or more designated contact methods for submitting DSRs or other rights requests. Consideration should be taken to how the business interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for other purposes, available technology, and ease of use by the consumer when

determining which methods consumers may use to submit requests to limit. Some examples suggested by the CCPA Regulations include:

- for online collection of consumer information, a "Limit the Use of My Sensitive Personal Information" link or the Alternative Opt-out Link for consumers to submit requests onto. The CCPA Regulations go further into detail in §7014 on how this should be executed.
- for in-person and online interaction, an in-person as well as online form.
- toll free phone number, designated email address or form submitted in person or through mail.

A business that has received a direction from a consumer not to use or disclose the consumer's sensitive personal information, other than for the certain business purposes and exception set out above, must not use or disclose the consumer's sensitive personal information for any other purpose after its receipt of this direction unless consent from the consumer is subsequently provided for any additional purposes.

A service provider, contractor or third party that assist a business with processing for other purposes should be notified of the consumer request, required to comply with the request and forward the request to any other person whom the third party has disclosed or shared the sensitive personal information during that period.[19]

§1789.125 - Right of No Retaliation Following Opt Out or Exercise of Other Rights

Similar to Article 39 of the DIFC DP Law, the Amended CCPA requires businesses not to discriminate against a consumer because they exercised any DSR. There is a general prohibition (with limited exceptions) on businesses, following a consumer's exercise of a DSR, to:

- deny goods or services to the consumer.
- charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- provide a different level or quality of goods or services to the consumer.
- suggest that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

While Article 39 of the DIFC DP Law is quite broad regarding non-discrimination, the Amended CCPA specifically prohibits businesses from retaliate against an employee, applicant for employment, or independent contractor for exercising a DSR.

The section also sets out the requirements of offering financial incentives (referred to as price or service difference in the CCPA Regulations). The CCPA Regulations in Article 7, § 7080 titled "Discriminatory Practices", explain that price or service differences can be non-discriminatory

[19] Article 3, §7027(g) of CCPA Regulations.

where it is reasonably related to the value of the consumer's data. Article 7 of the CCPA Regulations provides guidance on how consumer information can be calculated. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the price or service difference. The CCPA Regulations also provide case study examples of what is discriminatory (and what is not permitted) and vice versa.

Notice

As mentioned previously, §1789.100 of the Amended CCPA places an obligation on controllers to inform consumers of certain information (at or before the point of collection). This includes:

- the categories of personal information and sensitive personal information to be collected;
- the purposes for which the categories of personal information and categories of sensitive personal information are collected or used; and
- whether that information is sold or shared.

A business must provide the consumer with notice before collecting additional categories of personal information, and categories of sensitive personal information, or using personal information, and sensitive personal information, for additional purposes.

The OAG explains[20] that where businesses sell consumers' personal information, then the notice at collection must include a Do Not Sell or Share link. The notice must also contain a link to the business's privacy policy, where consumers can get a fuller description of the business's privacy practices and of their privacy rights.

The Amended CCPA, requires that collecting, using, retaining and sharing personal information be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed and not further processed in a manner that is incompatible with those purposes. Businesses must not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.

Third parties acting as controllers may provide the required information prominently and conspicuously on the homepage of its internet website. If the collection of personal information is on the business' premises, then the business shall, at or before the point of collection, inform consumers as to the information above, in a clear and conspicuous manner at the location.

The Amended CCPA, sets out the requirement for businesses to enter into a written contract with third parties, service providers or contractors to which personal information

[20] Topic H on the OAG FAQs: California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

is sold, share or disclosed to for business purposes. The written agreement must, among other things from §1789.100(d) of the Amended CCPA:

- specify that personal information is sold or disclosed for limited and specified purposes
- obligate third parties, service providers, or contractors to comply with applicable obligations under the Amended CCPA, and provide the same level of privacy protection as is required by the Amended CCPA.
- grant the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligation under the Amended CCPA.
- require the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under the Amended CCPA.

Observation 5: International Data Transfers

The Amended CCPA does not have a provision dedicated to the transfer of personal information outside the state of California, or the USA more generally, as seen in other data protection legislation, for example Article 26 and 27 of the DIFC DP Law.

"Transferring", however is listed in the Amended CCPA under the definitions of "sell," "selling," "sale," or "sold,"[21] and "Share," "shared," or "sharing"[22].

Given the nature of the Amended CCPA, i.e., as a state law, there is little to no further guidance on international data transfers. However, the definitions in the Amended CCPA explain the instances where the sale of personal data may not occur, including where the consumer directs the business to disclose their personal information or where the business transfers to a third-party personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction. If a third-party materially alters how it uses or shares the personal information, prior notice should be provided to the consumer.

Also, as stated in Observation 4, the Amended CCPA and CPPA Regulations do require that any third party that receives personal information from the business be contractually bound to comply with the Amended CCPA and to provide the same level of privacy protection as is required under the Amended CCPA.[23]

DIFC exporters that send personal data to a California-based importer under the adequacy decision issued by the Commissioner would need to ensure that onward transfers of personal data are safeguarded, as per usual practice and obligations by law. This can be further assured through:

- onward transfer to another recognized jurisdiction, either by the UK, EU or DIFC;
- use of the EDMRI due diligence tools, or other verified organizational and technical measures to ensure secure storage and processing of personal data;
- compliance with other similar data protection laws that the importers are subject to in any case;
- to apply contractual measures both generally and in the form of standard clauses or a DPA so the next recipient is subject to the same requirements and obligations (flow down).

[21] §1798.140(ad)(2)(c) of the Amended CCPA.
[22] §1798.140(ah)(2)(c) of the Amended CCPA.
[23] §1798.100(d)(2) of the Amended CCPA; §§7052 and 7053 of the CCPA Regulations.

Subcontracting and Data Flows

The Amended CCPA provides that contractual obligations must flow down to contractual obligations to subcontractors, which are defined in the Amended CCPA as "service providers" and "contractors."[24] Both service providers and contractors receive and/or obtain access to a consumer's personal information pursuant to written contract with the business that prohibits them from:

> *(A) Selling or sharing the personal information.*
>
> *(B) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract with the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.*
>
> *(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider or contractor and the business).*
>
> *(D) Combining the personal information that the service provider or contractor receives pursuant to a written contract with the business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider or contractor may combine personal information for certain business purposes set forth in regulations adopted by the California Privacy Protection Agency.*[25]

Service providers and contractors cannot contract with a business to provide cross-context behavioral advertising.[26] They also cannot combine the personal information of consumers who have opted-out of the sale/sharing of their personal information that they have received from, or on behalf of, the business with personal information that they have received from, or on behalf of, another person or collected from its own interaction with consumers.[27]If a service provider or contractor subcontracts with another person to provide the services identified in their written contract with the business, the service provider or contractor must notify the business of the engagement of a subcontractor and must have a contract with the subcontractor that complies with the Amended CCPA and the CCPA regulations.[28]

In addition to any transfer requirements regarding DIFC-originating Personal Data being shared to other international jurisdictions after coming to rest in California, DIFC Exporters will need to consider this requirement as well.

For completeness, the requirements in CPRA §1798.40(ag) are comparable to those of Article 24, specifically Article 24(2) and Article 24(3), of the DIFC DP Law 2020.

[24] §1798.140(j), (ag) of the Amended CCPA; §§7050 and 7051 of the CCPA Regulations.
[25] §1798.140(j), (ag) of the Amended CCPA; §§7050 and 7051 of the CCPA Regulations.
[26] §1798.140(e), (j), (ag) of the Amended CCPA; §7050(b) of the CCPA Regulations.
[27] §1798.140(e), (j), (ag) of the Amended CCPA; §7050(b) of the CCPA Regulations.
[28] §1798.140(j)(2), (ag)(2) of the Amended CCPA; §7051(b) of the CCPA Regulations.

Onward Transfers

EU onward transfers

Where DIFC exporters transfer personal data to an EU Member State recognized by the DIFC Commissioner, which is then onward transferred, please note that in 2022, and more generally in the US, US President Joe Biden signed an executive order to facilitate the transfer of personal data from the EU to the US, known as the EU – US Privacy Framework, that will apply to the onward transfer. In other words, as this framework has been approved as adequate by the EU, then onward transfers may proceed to California accordingly as a state of the United States. If no longer accepted, or if the framework is approved and then invalidated, the Exporter in the EU engaging in the onward transfer will need to comply with applicable transfer mechanisms available at that time.

UK onward transfers

The UK is completing a UK – US Data Bridge review at the time this Decision was issued. As such, onward transfers to the US from the UK will be covered by this mechanism.

Rest of World

For all other jurisdictions, personal data transferred by DIFC exporters will be subject to (onward) transfer mechanisms required by the onward transferring jurisdiction.

Observation 6: Security of Processing and Breach Reporting

The OAG under Topic A of the FAQs[29], explains that consumers cannot bring a claim against businesses for most CCPA violations. Under the Amended CCPA, a claim can only be brought if there is a data breach, and even then, only under limited circumstances.

§1798.150 of the Amended CCPA sets out the provisions for personal information security breaches. Under this section, any consumer whose nonencrypted and nonredacted personal information, or whose log in details (in combination) that would permit access to the account is subject to unauthorized access as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information, is entitled to any of the following:

- to recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
- injunctive or declaratory relief.
- any other relief the court deems proper.

The court will consider the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the wilfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

To bring an action, a consumer must provide written notice identifying the specific provisions of Amended CPPA which has been breached. If the business remedies this breach within the 30 days and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, there is no action for a consumer against the business.

See Observation 7 of this assessment for enforcement action by the OAG and CPPA.

[29] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

Observation 7: Accountability, Redress and Enforcement

Accountability

The principle of Accountability requires the Processor and Controller to implement appropriate, effective, and verifiable measures to prove the correct compliance with data protection regulations. Said measures must be permanently revised and evaluated in order to measure their level of efficiency with regards to the compliance and protection of personal data. For example, a Privacy Management Program (PMP) is an operative mechanism that can be implemented to guarantee the correct processing of personal data.

This principle requires less rhetoric and more actions with regards to the compliance of the Controller and Processor's duties. It requires them to assess, document and implement concrete actions that guarantee the rightful processing of personal data.

These are clearly set out in Part 2D of the DIFC DP Law such as requiring companies to implement accountability mechanisms including to establish a program to demonstrate compliance, to conduct privacy impact assessments and to maintain a written record of its processing activities. The Amended CCPA and CCPA Regulations contain record-keeping obligations which are largely focused on maintaining records of consumer requests and deletion requests.

The Amended CCPA and CPRA, businesses will have to conduct "Regular Risk Assessments". While the details about this mechanism remain to be provided by the CPPA by guidance or other clarifications, Section 1798.185(a)(15)(B) of the CPRA provides for the following:

- Significantly risky processing activities
- Submit risk assessments to the CPPA on a regular basis
- Must highlight the use and processing of Sensitive Personal Information
- Include an analysis of the benefits of the processing and identify them vs the risks to the consumers or public
- Discontinue processing that create more risks to consumer compared to the benefits

Please note that in conducting regular risk assessments, information containing trade secrets does not need to be submitted.

The requirements regarding Regular Risk Assessments are comparable and compatible with the requirements for a DPO Controller Assessment ("**Annual Assessment**") to be conducted at least annually. Similar criteria are to be evaluated, and in the interest of consistency and

building a culture of privacy and compliance, a risk matrix is provided upon submission of the Annual Assessment. The risk matrix is for guidance purposes only, and may be amended.[30]

Privacy policies, both internal and notices online, are required in order to remain accountable to consumer data subjects. As part of the requirement around privacy and compliance policies, businesses must maintain reasonable security measures, provide information to consumers at or before the collection point, including retention length and measures, based on necessity and proportionality, rights to limit tracking and other rights, as set out above, and compliance obligations that generally align with the DIFC DP Law 2020.

Judicial Redress

Please see the analysis of security breaches in Observation 6 of this Assessment for information on redress measures in this regard.

For other violations of the Amended CCPA, only the OAG or the CPPA can take legal action against non-compliant entities. The OAG further explains in topic A of its FAQs[31] that by using consumer complaints and other information, it may identify misconduct and initiate investigations. Starting on July 1, 2023, consumers will also be able to file complaints with the CPPA for violations of the Amended CCPA occurring on or after that date.

These measures are all available to data subjects in accordance with the DIFC DP Law 2020 as set out in Part 9.

Enforcement

§1798.155. and §1798.199.90 of the Amended CCPA, sets out the penalties of non-compliance. Businesses, service providers, contractors, or other persons in violation of Amended CCPA, are subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation or for violations involving the personal information of children where the business, service provider, contractor, or other person has actual knowledge that they are under 16 years of age (deposited in the Consumer Privacy Fund ("**Fund**")). The Section also explains the powers and roles of the OAG and CPPA.

The Fund is defined in the Amended CCPA, as a fund to offset (such as) any costs incurred by the state courts in connection with actions brought to enforce the law and costs incurred by the Attorney General. Any earnings from the Fund are to be deposited in the General Fund, and to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.

[30] https://www.difc.ae/business/operating/data-protection/guidance/#s15
[31] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

OAG Enforcement

Since the first day of CCPA enforcement, July 1, 2020, the California OAG has taken extensive measures to investigate companies' compliance with the CCPA. Most recently, the OAG has focused on the areas of employee and job applicant data as well as mobile applications compliance with consumer opt-out requests.[32] The OAG also posts case studies and examples of business responses to notices of noncompliance. Normally a company has thirty (30) days to cure any notified noncompliance matter. The impact has been positive, with businesses taking appropriate actions to cure and thereby strengthening consumer privacy protections.[33]

[32] Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act

[33] CCPA Enforcement Case Examples

Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement)

§1798.145 sets out the exemptions to the Amended CCPA, including those assuring a business's ability:

- comply with federal, state, or local laws or comply with a court order or subpoena to provide information.
- comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. Law enforcement agencies may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information for a period of 90 days (or an additional 90-day period if extended).
- cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury. This occurs in limited circumstances including, but not limited to, where the request is approved by a high-ranking agency officer for emergency access to a consumer's personal information or the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.
- exercise or defend legal claims.

Similar obligations are addressed in the DIFC DP Law 2020 in a variety of places, including the obligations around data protection principles, lawful bases for processing personal data, and data subjects' rights. The acknowledgement set out in Appendix 1 regarding Article 28 further clarifies the obligations of DIFC-based Controllers, and by extension to the extent required by law, to properly obtain assurances and conduct impact assessments as needed or possible when sharing personal data with government authorities and law enforcement.

Observation 9: Existence of international commitments and conventions binding on California or its membership of any multilateral or regional organisations

As a state in the United States, California is unable to directly enter into international commitments and conventions. The CPPA became a Member of the Global Privacy Assembly in October 2022.

In June 2023, the CPPA became a member of the Global Privacy Enforcement Network.

The DIFC Commissioner's Office is also a member of both organisations.

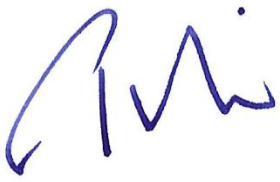
Conclusion

It is for the reasons set out in Observations 1 to 9 that the DIFC Office of the Commissioner of Data Protection issues this Decision recognizing the essential equivalence of the Amended CCPA with the principles and obligations of the DIFC DP Law 2020.

The current EDMRI risk assessment regarding California's laws and regulations, as well as the cultural and environmental approach to privacy and redress, align with the DIFC DP Law 2020 such that transfers to California will receive the same or substantially equivalent protection by importers subject to the CCPA.

It is recommended that this Decision is reviewed and where appropriate reconfirmed on an annual basis. The Commissioner has the right to repeal, amend or suspend this Decision regarding California's privacy regime at any time.

Dated: 7 August 2023



Jacques Visser

DIFC

DIFC Commissioner of Data Protection

Appendix 1: Undertaking to substantially comply with Article 28 of the DIFC DP Law 2020

Article 28 of the DIFC DP Law 2020 states the following:

Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("**Requesting Authority**") for the disclosure and transfer of any Personal Data, it should:

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;

(b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

California Privacy Protection Agency acknowledges that DIFC entities are required to comply with Article 28 of the DIFC DP Law 2020, to the extent permitted by applicable laws regarding law enforcement and government authority data sharing requests.