American Bar Association
47th Annual Forum on Franchising

I-2: PRIVACY, PLEASE: PRACTICAL TIPS FOR NAVIGATING THE COMPLEXITIES OF DOMESTIC AND INTERNATIONAL DATA PRIVACY LAWS

Beata Krakus
UB Greensfelder LLP
Chicago, Illinois

and
Anthony Marks
Bryan Cave Leighton Paisner LLP
Los Angeles, California

and
John Pratt
Hamilton Pratt
Warwick, United Kingdom

and
Jacqueline Romano
Purpose Brands LLC
Woodbury, Minnesota

and
David Zetoony
Greenberg Traurig LLP
Denver, Colorado

October 16-18, 2024
Phoenix, AZ

TABLE OF CONTENTS

I. INTRODUCTION....4

II. OVERVIEW OF PRIVACY LAWS....4

A. Privacy Laws That Apply to Franchise Systems in the U.S.....4

B. Privacy Laws that Apply to Franchise Systems in the EEA and the UK....5

1. Introduction....5

2. Overview of the GDPR and the UK GDPR....6

3. Concepts....9

4. Restricted Transfers....14

5. Franchising Issues....14

C. Privacy Laws that Apply to Franchises in Other Parts of the World....19

III. GENERAL CONCEPTS INCLUDED IN MODERN PRIVACY LAWS....20

A. Personal Data....20

1. Personal Data Defined....20

2. Information that Qualifies as Personal Data....21

3. Business Contact Data....22

4. Aggregated Data....23

5. Anonymized or Deidentified Data....24

6. Pseudonymized Data....25

7. Sensitive Personal Data....26

B. Individuals Covered Under Modern U.S. State Privacy Laws and Modern Privacy Laws....27

C. Processing....28

1. Processing Activities Defined....28

2. "Selling" Personal Data....30

3. "Targeted Advertising"....30

D. Controllers and Processors....31
1. Controller Defined....31
2. Processor Defined....33
IV. GENERAL PRIVACY COMPLIANCE CONSIDERATIONS....34
A. Compliance Obligations for Controllers....34
B. Core Compliance Documents Considered by Controllers....36
C. Compliance Obligations for Processors....38
D. Interaction Between Modern Privacy Laws and Data Security Laws....40
E. Incorporating Privacy Compliance into Franchise Agreements....41
1. Allocation of Risk and Liability....41
2. Franchise Agreement Terms....42
3. Recent Litigation in the Franchise Space....44
F. Incorporating Privacy Compliance Into Franchise Disclosure Documents....46
G. Incorporating Privacy Compliance Into Operations Manuals....49
V. CROSS-BORDER DATA TRANSFER REQUIREMENTS....49
A. Restrictive Transfers....49
B. Adequacy Decisions....50
C. Transfer Mechanisms....51
1. Standard Contractual Clauses....51
2. Binding Corporate Rules....52
3. Exceptions to the Requirement to Have an Adequacy Decision or an Approved Transfer Mechanism....55
VI. OTHER NON-GDPR LEGISLATION AFFECTING PRIVACY....57
VII. ENFORCEMENT, PENALTIES FOR NON-COMPLIANCE....58
A. Enforcement and Comparing Jurisdictional Differences....58
1. Modern U.S. State Privacy Laws....58

2. GDPR and UK GDPR....62
3. Comparing Private Right of Action Provisions....63
B. Examples of Enforcement Actions....64
1. California Enforcement Actions....64
2. Colorado and Connecticut Enforcement Actions....66
3. GDPR and UK GDPR Enforcement Actions....67
VIII. CONCLUSION....68
Biographies....69
Appendix A: References to Modern U.S. State Privacy Laws....71
Appendix B: Types of Personal Data Under CCPA....72
Appendix C: Checklist for U.S. Franchisors Entering EEA or UK Markets....74

PRIVACY, PLEASE: PRACTICAL TIPS FOR NAVIGATING THE COMPLEXITIES OF DOMESTIC AND INTERNATIONAL PRIVACY LAWS

I. INTRODUCTION

We live in a data-driven world. Using and sharing data is an essential part of business activity. Data privacy laws define what must be done to ensure an individual's data is used properly and fairly. In the United States ("U.S."), several states have enacted privacy laws affecting franchise systems. In addition, franchise systems that offer goods or services to individuals outside of the U.S., or which monitor the behavior of individuals outside of the U.S., may need to understand and comply with international privacy laws and regulations, such as the European Union's General Data Protection Regulation (defined below). This paper will help you understand the legal obligations to protect the personal data collected in franchise systems.

Once a franchisor has a foundational understanding of the legal obligations to protect personal data, it will be able to address the central question facing it regarding privacy: how should a franchisor allocate the responsibility and associated risks for identifying, implementing and utilizing each of the systems and procedures necessary to comply with Modern Privacy Laws (defined below)? Allocation of risk and responsibility necessarily also requires franchise systems, franchisors, franchisees and franchise agreements to be adaptable to the ever-evolving legal landscape. The franchise agreement and operations manual should be drafted in a manner that will allow for sufficient flexibility and discretion for continued development, updates, upgrades and modifications.

The following terminology is applied throughout this paper. When the term "CCPA" is used, it generally refers to the provisions of the California Civil Code Section 1798.100, *et seq*. that were adopted on June 28, 2018, and that was amended by the California Consumer Privacy Rights Act of 2020. When the term "GDPR" is used, it refers to the General Data Protection Regulation, which is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, O.J. 2016 L. 119/1.[1] When the term "UK GDPR" is used, it refers to the United Kingdom ("UK") implementing the GDPR in the Data Privacy Act 2018 ("2018 Act"). The 2018 Act and the Data Protection, Privacy and Electronic Communications (including its Amendments) (EU Exit) Regulations 2019 amend the provisions of the GDPR. As such, the amended GDPR which applies in the UK is referred to as the "UK GDPR." All references to "Articles" will refer to articles of both the GDPR and the UK GDPR unless otherwise stated. When the phrase "Modern Privacy Laws" is used it refers to the GDPR, UK GDPR, and Modern U.S. State Privacy Laws (defined below). Any additional references and citations are in standard form.

II. OVERVIEW OF PRIVACY LAWS

A. Privacy Laws That Apply to Franchise Systems in the U.S.

While the U.S. has over 600 federal, state, and municipal data privacy and security statutes, regulations or ordinances, there is no consolidated omnibus legislation that applies to

[1] *See* General Data Protection Regulation (GDPR), https://gdpr-info.eu (last visited July 2, 2024) (this is the official PDF of the GDPR as a neatly arranged website).

most private entities or that covers the range of data privacy issues. Historically, the data privacy legislation in the U.S. has focused on certain industries (such as financial institutions, educational institutions, health care providers or data brokers), particular types of data (for example, video viewing history or driver's license information), or specific sharing practices (like wiretapping).

California was the first U.S. state to enact privacy legislation. On October 12, 2017, a privacy advocate filed a ballot initiative in the state of California proposing legislation that would regulate most private entities that conducted business in the state and that would apply to a broad range of privacy obligations. The ballot initiative was withdrawn on June 28, 2018, as part of a negotiated agreement between the privacy advocate and the California legislature that led to the passage of the California Consumer Privacy Act or the CCPA. While the CCPA was enacted on June 28, 2018, it did not become "operative," until January 1, 2020.[2] Before the CCPA went into effect, a second ballot initiative was filed, and approved by California voters, to amend the CCPA. That ballot initiative known as "Proposition 24" or the California Privacy Rights Act ("CPRA") significantly altered the CCPA and went into force on January 1, 2023.[3] The CCPA, as amended by the CPRA, became the first statute in the U.S. to impose broad privacy requirements on most private entities, and ushered in a wave of what are often referred to as "modern" U.S. privacy statutes.

As of the time of the writing of this paper, twenty states have enacted modern privacy legislation. While those statutes differ in several important respects, they are collectively referred to herein as the "Modern U.S. State Privacy Laws." For a list of these laws as of this writing, please refer to Appendix A: References to Modern U.S. State Privacy Laws ("Appendix A"). It is worth noting that while the CCPA started the trend of Modern U.S. State Privacy Laws and the states that followed incorporated some of the concepts that were included in the CCPA, no other state has used the CCPA itself as a guide or model when drafting their own legislation. Instead, the laws enacted by the two states that immediately followed California--Colorado[4] and Virginia[5]--became the de facto standard by which subsequent states based the structure and text of their own laws. As a result, privacy attorneys will often refer to the Modern U.S. State Privacy Laws as based on the Colorado and Virginia "models." It is also worth noting that the Modern U.S. State Privacy Laws are set to phase in over time, with some laws not scheduled to go into force until 2026.

B. Privacy Laws that Apply to Franchise Systems in the EEA and the UK

1. Introduction

In the European Union ("EU"), the regulation and protection of personal data has been a major focus of attention for some time, although the adoption of the GDPR and UK GDPR have

[2] CAL. CIV. CODE §§ 1798.100–1798.199.95; CAL. CODE REGS. Tit. 11, §§ 7000–7102 (West 2024).

[3] CAL. CIV. CODE §§ 1798.100–1798.199.100, CAL. CODE REGS. Tit. 11, §§ 7000–7304 (West 2024).

[4] COLO. REV. STAT. ANN. §§ 6-1-1301–1313.

[5] VA. CODE ANN., Tit. 59.1, Ch. 53, § 59.1-575.

resulted in an increased focus on data protection issues. That focus has further increased with businesses being heavily fined by the relevant authorities for data privacy breaches.[6]

2. Overview of the GDPR and the UK GDPR

a. To Whom Does the GDPR and the UK GDPR Apply?

The GDPR and the UK GDPR apply to "controllers" and "processors". A controller determines the purpose and means of processing personal data.[7] A processor is responsible for processing personal data on behalf of a controller.[8] Processors are subject to specific legal obligations, for example, to maintain records of personal data and processing activities. Controllers are not relieved of their obligations where a processor is involved, and controllers must ensure that their contracts with processors comply with the GDPR and the UK GDPR. The GDPR and the UK GDPR apply to processing carried out by organizations operating within the EU and the EEA[9] countries (in the case of GDPR) and inside the UK (in the case of the UK GDPR). They also apply to organizations outside those geographic areas that offer goods or services to individuals inside those areas, or which monitor the behavior of an individual within those areas.[10]

b. What is Personal Data?

"Personal data" means any information relating to a person who can be directly or indirectly identified.[11] As a result, a wide range of data types can constitute personal data including name, identification number, location, and online identifiers.[12] Processing refers to any operation or set of operations which is performed on personal data.[13] This includes, for example, the collection, storage, transmission, use, structuring, disclosure, or deletion of personal data.[14]

The GDPR imposes additional requirements on some types of personal data that are considered particularly sensitive. These data types are referred to as "special categories of personal data" within the regulation. The special categories specifically include genetic data and

---

[6] The UK's regulatory body, the Information Commissioner's Office, announced its intention in July 2019 to fine British Airways and Marriott a combined £282 million for their data breaches. Marriott has many hotels operating using the franchise model. See GDPR Enforcement Tracker, https://www.enforcementtracker.com (last visited July 2, 2024) for a full list of fines and penalties.

[7] GDPR, Article 4(7).

[8] GDPR, Article 4(8).

[9] The European Economic Area ("EEA") countries are Norway, Iceland and Lichtenstein.

[10] GDPR, Article 3(2(b).

[11] GDPR, Article 4(1).

[12] GDPR, Article 4(1).

[13] GDPR, Article 4(2).

[14] *Id.*

biometric data when processed uniquely to identify an individual, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership as well as data concerning health, sex life and sexual orientation.[15] In order to process special categories of data, you must identify both a lawful basis for the processing under Article 6 and a separate condition under Article 9. It is worth noting that while personal data relating to criminal convictions and offences are not technically included within the definition of "special category" data, similar extra safeguards apply to their processing.[16]

c. Is there a Substantive Difference between the GDPR and the UK GDPR?

Following the UK's departure from the EU, the UK amended its version of the GDPR and incorporated this amended version of the GDPR into UK law. While the UK GDPR does not materially deviate from the substantive obligations contained in the GDPR, the following summarizes some of the differences:

Topics	Explanation of Differences
Authoritative Institutions	The UK GDPR replaces references to EU institutions, such as the European Commission and European Data Protection Board, with UK equivalents.
Cooperation with EU Institutions	The UK GDPR establishes mechanisms for cooperation and consistency with EU supervisory authorities. It outlines processes for mutual assistance, joint operations, and information sharing between the UK's Information Commissioner's Office ("ICO") and EU supervisory authorities.
Transfers of Personal Data between the EU and the UK	Following Brexit, a transfer of personal data from the EU to the UK is technically treated as a transfer to a "third country" outside the EU. That said the EU has recognized the UK as an "adequate" country (and the UK has recognized the same of the EU). As an adequate country, additional protections are not needed to be put in place by a controller or processor to transfer data between the EU and the UK.
EU and UK Representatives	The GDPR stipulates those businesses outside the EU (such as those that do not have

[15] GDPR, Article 9(a).

[16] The Data Protection (Fundamental Rights and Freedoms) (Amendment), Regulations 2023 No. 1417 (Dec. 18, 2023), https://www.legislation .gov.uk/uks/2023/1417/made.

Topics	Explanation of Differences
	an establishment within the EU) must appoint an EU representative if they process the personal data of EU residents. The EU representative must be established in an EU member state where the data subjects, whose data is being processed, are located. This is necessary to ensure that there is a point of contact for data protection authorities and individuals within the EU to facilitate communication and address data protection concerns. The UK GDPR introduced a different provision for businesses outside the UK that process the personal data of UK individuals. These businesses must appoint a representative in the UK, but, unlike the GDPR, the UK GDPR does not require the representative to be physically located in the UK.
Updates and Changes	In the case of the GDPR, any changes or updates to the regulation are made through the EU legislative process. This process involves several steps including a requirement that proposals of the European Commission are discussed among the EU member states. The UK GDPR gives the UK government the authority to make changes or updates.
Penalty Structure	The GDPR states that some violations of the regulation are more serious than others. Less serious infringements can result in a fine of up to €10 million, or 2% of a business' annual revenue from the preceding financial year, whichever is higher. More serious infringements could result in a fine of up to €20 million, or 4% of the business' annual revenue from the preceding financial year, whichever is higher. In the UK the €10 million and €20 million figures are replaced by £8,700,000 and £17,500,000 respectively.
Advisory and Governing Bodies	The GDPR establishes the European Data Protection Board ("EDPB") as a key element in promoting cooperation and consistency among supervisory authorities across EU member states. The UK GDPR also emphasizes cooperation with EU supervisory

Topics	Explanation of Differences
	authorities, and establishes mechanisms for cooperation, coordination, and information sharing between the ICO and EU supervisory authorities. The UK recently proposed amendments to UK data protection laws in the Data Protection and Digital Information Bill, but the Bill was not passed because it failed to pass all its stages before the UK Parliament was dissolved ahead of the General Election. The Bill contained a small number of major changes such as loosening the rules on cookies, allowing greater use of automated decision making and replacing data protection officers with "senior responsible individuals." The UK Government has also passed the Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023.[17] This amends the UK GDPR so that it no longer protects personal data as a "fundamental right," but rather only as a right within the meaning of the European Convention on Human Rights.[18]

3. Concepts

a. Data Protection Principles

The data protection principles – set forth in Article 5(1) of the GDPR – outline the main responsibilities for organizations. According to these data protection principles, personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes

[17] The Data Protection (Fundamental Rights and Freedoms) (Amendment), Regulations 2023 No. 1417 (Dec. 18, 2023), https://www.legislation.gov.uk/uksi/2023/1417/made.

[18] Council of Europe, *European Convention on Human Rights* (Oct. 2, 2013), www.echr.coe.int/documents/d/echr/convention ENG.

or statistical purposes shall not be considered to be incompatible with the initial purpose;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

The GDPR requires that controllers be not only responsible for the above principles, but "able to demonstrate compliance."[19]

b. Lawful Basis for Processing

There must be a valid lawful basis to process any personal data.[20] The lawful basis should be established before processing begins and should be documented.[21] Six lawful bases for processing are set out, but in a franchising context only four (in italics below) are likely to be relevant. They are:

- Consent: the individual has given clear consent for the processing of their personal data for a specific purpose.

- Contract: the processing is necessary for a contract entered into with an individual, or because an individual has asked for specific steps to be taken before entering into a contract.

[19] GDPR, Article 5(2).

[20] GDPR, Article 6.

[21] *See e.g.*, GDPR, Article 5(1)(a) (noting that personal data must be processed lawfully, fairly and in a transparent manner).

- Legal Obligation: the processing is necessary to comply with a European (or UK) law (not including contractual obligations).

- Vital Interests: the processing is necessary to protect an individual's life.

- Public Task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

- Legitimate Interests: the processing is necessary for a processor's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

c. When is Processing "Necessary"?

Many of the lawful bases for processing depend, with the exception of "consent,"[22] on the processing being "necessary."[23] This does not mean that processing always must be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful bases will not apply if the commercial purpose of the processing can reasonably be achieved by some other less intrusive means. Processing will not be necessary simply because a business has chosen to operate its business in a particular way. The question is whether the processing is necessary for the stated purpose, not whether it is a necessary part of a chosen method of pursuing that purpose.[24]

d. Documenting the Lawful Basis

The principle of accountability is important under the GDPR. It requires controllers to be able to demonstrate that they are complying and have appropriate policies and processes in place. This means that controllers need to be able to show that they have properly considered which lawful basis applies to each processing purpose and can justify their decision.[25] As a result, a record needs to be kept of which basis is being relied on for each processing purpose, and what is recorded is sufficient to demonstrate that a lawful basis applies. That record is often called a "record of processing" or a "data inventory."[26] For example, if a franchise system's loyalty program is open to individuals to whom GDPR applies, the franchisor may wish to use the loyalty program contract as the lawful basis for processing data of the program members. To use the contract as the lawful basis for the processing, the franchisor could conspicuously include in the contract with

[22] GDPR, Article 6.1(a).

[23] GDPR, Article 6.1(b), (c), (d), (e), (f).

[24] Information Commissioner's Office, Principles and grounds for processing, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/principles-and-grounds-for-processing/ (last visited Aug 27, 2024).

[25] GDPR, Article 5 and GDPR, Article 6.

[26] GDPR, Article 30.

the member what type of data may be processed, and state that it will rely on the contract as the lawful basis for the processing of the members' personal data.[27]

e. What Must Individuals be Told?

Information about the lawful basis that applies must be included in the privacy notices provided to individuals. Under the applicable transparency provisions, the information that needs to be given includes (a) the intended purposes for processing the personal data, and (b) which lawful basis for the processing applies.[28]

f. Consent

Consent may be used as a lawful basis for processing personal data. To rely on consent as a lawful basis, controllers must be able to demonstrate the following:[29]

- consent is the most appropriate lawful basis for processing personal data;
- the request for consent is prominent and separate from any terms and conditions;[30]
- the individual has positively opted in (i.e., pre-ticked boxes or any other type of default consent are not used);[31]
- clear, plain language that is easily understood is used;[32]
- the data and what is going to be done with it is specified;[33]
- individuals are offered options to consent separately to different purposes and types of processing;
- details of the business organization and any third-party controllers who will be relying on the consent are set out;
- the individual should be able to withdraw their consent after it has been given;[34]

---

[27] GDPR, Article 6.1(b).

[28] GDPR, Article 12.

[29] GDPR, Recital 42.

[30] *See, e.g.,* GDPR, Article 7(2), Recital 32.

[31] *See, e.g.,* GDPR, Consent, https://gdpr-info.eu-0issues/consent/ (last visited July 8, 2024).

[32] GDPR, Recital 42.

[33] GDPR, Recital 32.

[34] GDPR, Article 7(3).

- the individual must be able to refuse consent without detriment;[35]
- consent should not be a precondition of the provision of a service;[36] and
- if online services are offered directly to children, consent can only be sought if age-verification measures (and parental control measures for younger children) are in place.[37]

g. Contract

"Performance of a contract" is a lawful basis that applies to the processing of personal data where such processing is necessary to fulfil certain contractual obligations to the individual. The processing of the personal data must be considered necessary to perform the contract. If what is being asked for could be done without processing personal data, this lawful basis will not apply.[38]

h. Legal Obligation

This lawful basis can be used if personal data must be processed to comply with a common law or statutory obligation imposed by an EU Member State (or the UK in the context of the UK GDPR), but not contractual obligations. The specific legal provision should be identifiable, and the processing must be necessary, and the decision to use this lawful basis should be documented.[39]

i. Legitimate Interests

The basis of "legitimate interests" is the most flexible lawful basis for processing. It is likely to be most appropriate where personal data is used in ways that individuals would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. There are three elements to the legitimate interest basis. It is necessary to identify a legitimate interest; show that the processing is necessary to achieve it; and balance the legitimate interest against the individual's interests, rights and freedoms.

The relevant legitimate interests[40] can be a controller's own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal

[35] GDPR, Recital 43.

[36] *Id.*

[37] GDPR, Article 8.

[38] *See, e.g.,* Information Commissioner's Office, Contract, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/contract (last visited Aug. 21, 2024). *See also,* GDPR, Article 6(1)(b) and Recital 44.

[39] *See, e.g.,* Information Commissioner's Office, *Legal obligation* (July 2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legal-obligation/. *See also,* GDPR Article 6(1)(c) and Recitals 41 and 45.

[40] GDPR, Article 6.1(f).

benefits. The processing must be necessary. If the same result can reasonably be achieved in another less intrusive way, legitimate interests should not apply. A record of legitimate interest assessments should be maintained to help demonstrate compliance and details of applicable legitimate interests should be contained in privacy information that is provided.

4. Restricted Transfers

The GDPR and the UK GDPR primarily apply (with some exceptions) to controllers and processors located in the EEA and the UK respectively, and individuals risk losing the protection of these data protection laws if their personal data is transferred[41] outside of the EEA and/or UK. As a result, rules apply to transfers of personal data to recipients located outside the EEA and/or the UK to help ensure that individual's rights concerning their personal data continue to apply when the data leaves the EEA and/or UK.

The transfer rules apply where the recipient is a separate controller or processor and legally distinct from the sender. The recipient can be a separate sole trader, partnership, company, public authority or other organization, and includes separate companies in the same group. The transfer rules do not apply where the recipient is an employee of the sender, or the sender and recipient are part of the same legal entity, such as a company. A transfer of personal data to recipients located outside the UK is referred to as a "restricted transfer." Further information on restricted transfers is contained in Section V of this paper.

5. Franchising Issues

The GDPR and the UK GDPR apply to franchisors and franchisees in the same way that each applies to other businesses, but there are several issues which are of particular importance in a franchising context. Because of the international nature of franchising, the exporting of personal data is an important issue, but there are other issues which are summarized in this section.

a. Who is a Data Processor and who is a Data Controller?

Franchisees will collect information about their employees, customers and suppliers. In some franchise systems the information that franchisees collect will be left at least in part to franchisees. In many franchise systems, franchisors set out the information that franchisees must collect and usually pass to the franchisor. In other systems, franchisors may be less proscriptive concerning information collection. As a result, one of the main threshold issues in a franchise system is to determine whether, with respect to certain data, the franchisor is a controller[42] or a processor,[43] and whether the franchisee is a controller or a processor.

In order to determine whether a franchisor or a franchisee is a controller or a processor, it is useful to establish who decides:

[41] Defined in Chapter V of GDPR.

[42] GDPR, Article 4(7).

[43] GDPR, Article 4(8).

- to collect the personal data in the first place and the legal basis for doing so,
- which elements of personal data to collect,
- the purpose for which the data is to be used,
- which individual's data is to be collected,
- who is to receive the data,
- whether "subject access" and other rights apply, and
- how long the data will be retained.[44]

The above decisions can only be taken by the controller. This does not mean that if a franchisee or franchisor is a processor that entity cannot make any decisions. A processor can generally still decide:

- what IT systems or other methods to use to collect personal data,
- how to store the personal data,
- security to protect data, and
- the means to transfer the personal data from itself to the controller.

Simply put, if a franchisor or franchisee deals only with the "technical" aspects of an operation then it may be a processor, but if such entity interprets or exercises professional judgment in relation to the personal data it will be a controller.[45] Note that while it is useful for a franchise agreement to specify the roles of the franchisor and the franchisee, contractual designations are not necessarily determinative. Ultimately supervisory authorities will examine on a case-by-case basis, the factors discussed above to determine which parties may be acting in the capacity of a controller.

b. Franchisor Advice to their Franchisees

Inevitably, franchisees will look to their franchisor for advice and guidance concerning data protection compliance. A franchisor has a direct interest in ensuring that its franchisees are GDPR or UK GDPR compliant, because the franchisor may be responsible for any violations by its franchisees if the franchisor is a data controller and franchisees are joint controllers and/or data

[44] *See,* Information Commissioner's Office, *How do you determine whether you are a controller or processor?* (Oct. 2022), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/how-do-you-determine-whether-you-are-a-controller-or-processor/. *See, also*, GDPR, Article 24.

[45] *Id.*

processors.[46] Further, because of negative publicity, a privacy or security violation by a franchisee will have a negative impact on the entirety of the franchise system.

Nevertheless, there is a significant danger in a franchisor being too prescriptive in their instructions and requirements for their franchisees. This is because when providing any such guidance concerning data protection compliance, a franchisor is likely to owe franchisees a duty of care and, as a result, if any such advice and guidance proves to be inaccurate, the franchisor could be liable to franchisees in the tort of negligence. Compliance with data privacy requirements is not only complex but also subject to a wide range of possible interpretations of these requirements. Some franchisors have sought to address the risk of incurring liability to their franchisees for advice they provide by instructing or recommending a third-party expert to advise all of their franchisees. This is also not without risk because if the expert fails to provide accurate advice and guidance to franchisees, the franchisor may, again by virtue of a breach of its duty of care, be liable for such a recommendation.

Generally, UK franchisors have adopted an approach with their franchisees by giving only general advice setting out, in general terms, a data protection compliance action plan containing the steps that franchisees must take. This advice may, in the context of compliance with UK GDPR, take many forms and purely by way of an example could be along the lines of the following:[47]

> *"UK data privacy laws require data controllers to give individuals more information at the time their data is collected – this includes explaining the legal basis of your processing, your data retention periods and that individuals have a right to complain to the Information Commissioner's Office ("ICO").*
>
> ***Actions to take now:***
>
> - *Review your customer-facing terms and your privacy policies.*
> - *If you are relying on customer consent to legitimize your processing (for example, for email marketing), check that the method of obtaining consent will meet the data privacy rules. Consent requires a positive opt-in.*
> - *If you cannot rely on consent, establish if you can rely on one of the alternative conditions for processing.*

[46] *See,* Information Commissioner's Office, *What responsibilities and liabilities do controllers have when using a processor?*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/ (last visited Aug. 21, 2024). *See, also,* GDPR, Articles 83 and 84.

[47] These sample recommendations are modified version of sample recommendations provided in Helen Goff Foster, Dawn Newton, & John Pratt, *Collect If You Dare: Practical Strategies to Help Franchise Parties Cope with GDPR and Other International Privacy Laws and the Evolving US Privacy and Data Security Landscape*, ABA 42ND ANNUAL FORUM ON FRANCHISING W-17, at 17-21 *et seq.* (2019).

- *If you employ people, you won't be able to rely on employee consent to process their data, so you will need to determine on what other legal basis you will process your employee data.*

- *Employees will require privacy notices.*

Demonstrating your compliance

An overarching theme of UK data privacy laws is the principle of "accountability." There are new requirements (which are limited for businesses with fewer than 250 employees) on data controllers (and data processors) to demonstrate their compliance by fully documenting all their data-processing activities.

Actions to take now:

- *Consider what records you keep of your decision making and your processing activities.*

- *Can you, for example, demonstrate your compliance by pointing to staff training, internal audits of processing and reviews of internal policies?*

- *Review your contracts with processors to ensure that they meet the requirements of UK data privacy laws and that you are suitably protected if there is a breach.*

Mandatory breach notifications

Controllers will have no more than 72 hours to report any data protection breach that is not "de minimis" to the ICO. Where the breach is likely to result in a high risk to individuals, they must also notify individual data subjects without undue delay.

Actions to take now:

- *Review your internal systems to ensure that you can meet the new breach notification requirements.*

- *Review your processor contracts to ensure they contain obligations to report breaches to you.*

- *Invest in and use secure systems including the use of passwords and encryption, firewalls and current anti-virus software.*

- *Address the "human element" through training and procedures designed to minimize the risks of hacking, phishing and other cyber security breaches.*

Much higher penalties when things go wrong

Businesses may face much higher penalties for non-compliance.

Actions to take now:

- *Ensure that the risk of penalties for non-compliance with UK data privacy laws are fully understood at senior management and board level.*

- *Review your processor contracts to ensure that liability is adequately flowed down.*

Enhanced rights for individuals

UK data privacy laws include a suite of rights for individuals or "data subjects."

As well as subject access rights, which reflect the current law, individuals will have the right to receive their data in a commonly used and machine readable format.

They will also have the right to have their data erased (called the "right to be forgotten"), though the right to erasure is subject to certain exceptions. These include if an organization has legal requirements to retain data or if an employer needs to hold on to data and has lawful grounds for doing so.

Actions to take now:

- *Review your process for responding to subject access requests where a person is entitled to request details of the personal information you hold about them and how it is being processed.*

- *Ensure you can supply this without delay, free of charge and in any event within one month.*

- *Make any changes necessary to comply with the new rights for individuals.*

- *Consider whether you need to change your communications with individuals to ensure they are aware of the new rights, including your own staff.*

- *Remember that it is already a general principle of data protection law that personal data should be accurate, where necessary kept updated and not held for longer than necessary.*

Direct obligations on processors

Currently controllers are solely responsible to data subjects and the ICO for compliance, but UK data privacy laws impose direct obligations on processors, such as to take security measures to protect personal data and maintain records of all processing activities. Processors won't be able to subcontract processing without the controller's prior consent.

Actions to take now:

- *List all your arrangements with data processors, such as outsourced services and cloud suppliers, businesses that manage your email marketing as well as any IT service providers. Where necessary seek to renegotiate terms to comply with the new law.*

Privacy Notice

The provisions of privacy notices need to change.

Actions to take now:

- *Review the enclosed notice and amend as necessary.*
- *Forward to us the privacy notice you will use and make any amendments we require."*

The above is just one example of how franchisors may remind franchisees of their obligations under GDPR and UK GDPR.

c. Existing Franchisees

Existing franchisees will presumably have a franchise agreement setting out their franchisor's data protection requirements, which generally cannot be changed unilaterally by the franchisor. As a result, franchisors have sought to introduce changes to ensure data protection compliance through modifications to the operations manual. Whether such modifications are legally enforceable, especially if they conflict with express provisions of the franchise agreement, is unclear. To try to overcome that uncertainty, franchisors have sought when sending their franchisees advice on and their new requirements concerning data protection a confirmation in which franchisees are asked to confirm that they have: complied with the principal elements of the action plan laid out by the franchisor and agree that the revised data protection provisions (contained in the operations manual) will replace or supplement the data protection clause in their current franchise agreement.

C. Privacy Laws that Apply to Franchises in Other Parts of the World

An increasingly large number of countries worldwide have enacted their own privacy laws. While a full description of all international data privacy laws is beyond the scope of this paper, to the extent that a franchise system does business in countries outside the U.S. and Europe privacy counsel knowledgeable about the local privacy laws should be consulted. One source for information for a quick overview about applicable laws, is the database[48] maintained by UNCTAD, the United Nations trade and development body. The database enables the user to see what countries have laws, and pending legislation in several different areas, including data protection and privacy, e-transactions, cybercrime, and consumer protection. The statutes are usually available, though often only in the official language of the country in question.

[48] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited July 17, 2024).

III. GENERAL CONCEPTS INCLUDED IN MODERN PRIVACY LAWS

A. Personal Data

1. Personal Data Defined

Modern Privacy Laws often use the term "personal data" or "personal information." For consistency, we have used the term "personal data" throughout this paper. While the definitions of personal data differ between and among Modern Privacy Laws, they generally define the phrase as including any information that "identifies" a "particular" person.[49] The following compares how the term is defined under the CCPA and the GDPR:

CCPA[50]	GDPR[51]
"Personal information" means 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."	"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person."

While it is difficult to identify data types that would fall under the CCPA's definition of "personal information," but would not fall under the GDPR's definition of "personal data," the reverse is not necessarily true. Put differently, it is possible for data to be considered "personal data" under the GDPR because it can theoretically be linked to an individual, and not be considered "personal information" under the CCPA or other Modern U.S. State Privacy Laws because it cannot reasonably be linked to an individual.

For example, while European regulators have suggested that data that is "hashed" would still fall within the definition of "personal data" because there remains a theoretical possibility that the data could be re-identified,[52] courts applying Modern U.S. State Privacy Laws may determine that such information falls outside the scope of some Modern U.S. State Privacy Laws as it cannot be "reasonably" linked to a consumer. In the context of the GDPR, the Article 29 Working Party[53]

[49] CAL. CIV. CODE § 1798.140(v)(1) (West 2024).

[50] *Id.*

[51] GDPR, Article 4(1).

[52] Opinion 05/2014 on Anonymisation Techniques, Art. 29 Data Protection Working Party, 0829/14/EN WP 216 at 20 (adopted on April 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[53] European Data Protection Board, *Legacy: Art. 29 Working Party*, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-

considered "hashing" to be a technique for pseudonymization that "reduces the linkability of a dataset with the original identity of a data subject" and thus "is a useful security measure," but is "not a method of anonymization."[54]

It is important to note that prior to the enactment of Modern Privacy Laws, it was common in the data privacy industry to refer to the term "personally identified information" or "PII." While that term was used by various industry groups, it tended to have a narrower definition than the more modern term "personal data." As an example, the following provides a side-by-side comparison of the term "personal information" as used within the CCPA and PII as used by the National Advertising Initiative ("NAI") in its code of conduct.

CCPA[55]	**NAI 2020 Code of Conduct[56]**
"Personal information" means 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."	Personally Identifiable Information ("PII") is any data linked, or intended to be linked, to an identified individual, including name, address, telephone number, email address, financial account number, and non-publicly available government-issued identifier.

2. Information that Qualifies as Personal Data

The broad definition of personal data means that many data types may fall within the scope of the definition. While most privacy statutes do not provide examples of data types that are encompassed by the term, the CCPA provides a non-exhaustive list of over sixty data types that may fall under its definition. The general categories of personal data include, for example: personal identifiers (such as full name, email address, postal address), financial information (such as, bank account number, credit card number), health related information (such as health insurance information or an individual's mental or physical condition), commercial information (such as purchasing or consuming tendencies), internet or other electronic network activity information (such as search history, products or services considered), geolocation data (such as IP address or precise geolocation), and audio, electronic, visual or similar information. Please refer to Appendix B: Types of Personal Data Under CCPA ("Appendix B") for a complete list of these data types.

party_en#:~:text=The%20EDPB%20replaces%20the%20Article%2029%20Working%20Party,May%202018%20%28 (last visited August 31, 2024).

[54] Opinion 05/2014 on Anonymisation Techniques, Art. 29 Data Protection Working Party, 0829/14/EN WP 216 at 20 (adopted on April 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[55] CAL CIV. CODE. § 1798.140(V)(1) (West 2024).

[56] Network Advertising Initiative, 2020 NAI Code of Conduct at 19 (2020), https://thenai.org/wp-content/uploads/2021/07/nai_code20220.pdf.

Also, for purposes of the CCPA, a data element from the list above falls within the definition of "personal information" only if it identifies, relates to, describes, is associated with, or could be linked to a particular person or household, and the piece of information is not otherwise "publicly available."[57] Other Modern Privacy Laws (such as the GDPR) do not exempt from the scope of what constitutes personal data publicly available information, and what constitutes "publicly available" itself differs between and among the Modern U.S. State Privacy Laws.

Within the EU, the GDPR contains both data privacy and data security provisions and both utilize the same definition for the term "personal data." Within the U.S., data security statutes (particularly data breach notification statutes) typically use a narrower definition of terms like "personal data" to refer only to a person's name in combination with a small sub-set of data fields viewed by legislators as being particularly sensitive. For example, the state of Maryland defines the term as follows:

> an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: (i) A Social Security number; (ii) A driver's license number; (iii) A financial account number . . .; (iv) *An Individual Taxpayer Identification Number.*[58]

The Florida statute defines the term as follows:

> an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. … or a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.[59]

3. Business Contact Data

Both franchisors and franchisees collect and process data from a variety of business partners. For example, franchisors maintain the names, contact information, and financial information of their franchisees. They may also maintain names and contact information for their various vendors. Franchisees also maintain names and contact information for various franchisor

[57] CAL CIV. CODE. § 1798.140(V)(1), (2) (West 2024).

[58] MD. CODE ANN., COM. LAW § 14-3501(e)(1)(i) (2024).

[59] FLA. STAT. § 501.171(1)(g) (2024).

employees. They also may have their own vendors, where permitted under the franchise agreement, and for those vendors they would also maintain name and contact information.

As discussed above, "personal data" is defined broadly by many Modern Privacy Laws to include any information that "relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular" person.[60] Some privacy laws, like the GDPR and the CCPA, apply to personal data processed about consumers as well as business contacts.

For example, the GDPR extends to personal data of any "data subject" which is defined as a "natural person."[61] The CCPA extends to personal data of any "consumer" but defines that term broadly to include any "natural person who is a California resident."[62] As a result, if an individual is a California resident, their information is covered by the CCPA regardless of whether the individual is a consumer, an employee, or a business contact. Most other Modern U.S. State Privacy Laws also use the term "consumer," but adopt a more traditional definition of that term that means that their statute only applies to consumers. For example, the Virginia Consumer Data Protection Act ("VCDPA") excludes from the scope of the definition of "consumer" individuals who act in "a commercial . . . context."[63]

The net result is that information about business partners will be "in-scope" for some Modern Privacy Laws, and "out-of-scope" for other Modern Privacy Laws. For those jurisdictions in which it is "in-scope," the following provides a non-exhaustive list of the data types that may constitute personal data: contact's name, contact's email address (if it directly identifies an individual and is not a shared email account), contact's job title, contact's employer, contact's telephone number, contact's educational history, contact's qualifications or certifications.

Note that generic information about a business partner that does not identify a person would not be personal data. So, for example, "John.Smith@acme.com" would be personal data governed by the CCPA (if John Smith were a California resident) or the GDPR (if John Smith were in Europe), whereas "contact@acme.com" would not, even if the latter email address is used by John Smith to communicate with the public.

4. Aggregated Data

The CCPA specifically states that it does not restrict a business's ability to collect, use, retain, sell, share, or disclose "aggregated consumer information."[64] Aggregate consumer information is defined as

---

[60] CAL. CIV. CODE § 1798.140(v)(1) (West 2024).

[61] GDPR, Article 4(1). Note that while the GDPR and the UK GDPR applies to personal data about any data subject, the processing must still be within the territorial. Scope of the GDPR and the UK GDPR as explained in Article 3.

[62] CAL. CIV. CODE 1798.140(j) § (West 2024).

[63] *See, e.g.* VA. CODE ANN. § 59.1-575 (2024).

[64] CAL. CIV. CODE § 1798.145(a)(6) (West 2024).

> 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.[65]

Other Modern U.S. State Privacy Laws do not expressly exempt aggregated personal data from their scope, but some states (including Utah) expressly exempt aggregated data from their definition of personal information. For most Modern U.S. State Privacy Laws (such as the Colorado, Connecticut, and Virginia statutes) while there is no express exemption for aggregated data, most aggregated data is implicitly exempted insofar as once aggregated it arguably no longer satisfies the definition of personal data. For example, using the example of Virginia's statute, if information about multiple consumers has been combined to create an average or aggregate statistic, that information arguably no longer is "linked or reasonably linkable to an identified or identifiable natural person,"[66] and, therefore, would no longer be "personal data" under the VCDPA.

Aggregated data is generally data derived from personal data but when aggregated does not directly or indirectly reveal a person's identity data. For example, individual usage data can be aggregated to calculate the percentage of users accessing a specific website feature. Another example of aggregated data is customer satisfaction survey results showing only the results of all participating consumers. Under the GDPR and the UK GDPR aggregated data is not defined but if personal data is processed to create aggregated data that processing is regulated even if the aggregated data is no longer considered to be personal data.

5. Anonymized or Deidentified Data

The terms "deidentified" and "deidentification" are commonly used in Modern U.S. State Privacy Laws and are functionally exempt from most privacy and security related requirements. While some differences originally existed between how California and the rest of the Modern U.S. State Privacy Laws defined those terms, those differences have largely been resolved with California amending the CCPA to match the other state statutes. As a result, all Modern U.S. State Privacy Laws currently view data as deidentified if it meets all the following requirements:

- Data not reasonably associated to an individual. An organization must make a reasonable attempt to ensure that the data cannot be associated with specific individuals.[67]

[65] CAL. CIV. CODE § 1798.140(b) (West 2024).

[66] VA. CODE ANN. § 59.1-571 (2024).

[67] *See, e.g.* COLO. REV. STAT. § 6-1-1303(11((A) (2024).

- Public commitment. An organization must publicly commit (e.g., in its privacy notice) to maintain and use the information in deidentified form and not attempt to reidentify it.[68]

- Downstream recipient contracts. An organization must contractually obligate recipients of the information to abide by the same restrictions.[69]

Under both the GDPR and the UK GDPR anonymized data is data from which it is no longer possible to identify a person and therefore ceases to be personal data which is regulated.

6. Pseudonymized Data

The terms "pseudonymize" and "pseudonymization" are commonly referenced in the data privacy community, but their origins and meaning are not widely understood among many attorneys. Most American dictionaries did not historically recognize either term at all.[70] While they derive from the root word "pseudonym," which is defined as a "name that someone uses instead of his or her real name," their meanings are slightly more complex.[71]

To understand its meaning, it is important to understand how the term has evolved over time within different data privacy contexts. "Pseudonymization" was defined within the ISO 29100 privacy framework published in 2011 simply as a "process applied to personally identifiable information ("PII") which replaces identifying information with an alias."[72] Although the term was defined, it did not form an integral part of the privacy framework. Indeed, it was only referenced in the context of a technique that might contribute to privacy enhancing technology, and to explain that not all substitutions of personal identifiers create anonymized data.[73]

The GDPR included the term, albeit with a slightly broader definition than that which was used within the ISO framework. Within the GDPR it encompasses "personal data [that] can no longer be attributed to a specific data subject without the use of additional information . . . ."[74] Two years later, the CCPA became the first U.S. statute (federal or state) to use the term adopting a definition near identical to the one contained within the GDPR.[75] Indeed, except for minor

[68] *See, e.g.* COLO. REV. STAT. § 6-1-1303(11)(b) (2024).

[69] COLO. REV. STAT. § 6-1-1303(11) (2024).

[70] Neither term was in the Miriam Webster or Cambridge dictionaries as of March 8, 2021.

[71] Cambridge dictionary definition of "pseudonym" as of November 28, 2019.

[72] ISO/IEC 29100.2011 at § 2.24 (Dec. 2011). Note that this standard (Edition 1, 2011) has been withdrawn and replaced with ISO/IEC 29100:2024, which new version may be accessed here: ISO/IEC 29100:2024 – Information technology — Security techniques — Privacy framework (last visited Aug. 21, 2024). These ISO/IEC are only available in print and not accessible online.

[73] ISO/IEC 29100.2011 at §§ 2.15, 4.4.4.

[74] GDPR, Article 4(5).

[75] A Westlaw search of all federal and state statutes did not identify any other federal or state law that utilizes either term.

adjustments to conform the definition to CCPA-specific terminology (such as "consumer" instead of "data subject"), the definitions are virtually identical. Most of the other Modern U.S. State Privacy Laws have followed suit using definitions that deviate to a small degree but capture the same substantive provisions.

Franchisors and franchisees may be confused surrounding the impact that pseudonymization has (or does not have) on privacy obligations. That confusion largely stems from ambiguity concerning how the term fits into the larger scheme of Modern Privacy Laws. For example, aside from the definition, the CCPA only refers to "pseudonymized" on one occasion. Within the definition of "research" the CCPA implies that personal information collected by a business should be "pseudonymized and deidentified" or "deidentified and in the aggregate."[76] The conjunctive reference to research being both pseudonymized "and" deidentified raises the question whether the CCPA lends any independent meaning to the term "pseudonymized." Specifically, the CCPA assigns a higher threshold of anonymization to the term "deidentified." As a result, if data is already deidentified it is not clear what additional processing or set of operations is expected to pseudonymize the data. The net result is that while the CCPA introduced the term "pseudonymization" into the American legal lexicon, it did not give it any significant legal effect or status.

Unlike the CCPA, the pseudonymization of data does impact compliance obligations under many of the other Modern U.S. State Privacy Laws. Many of the other states do not require that organizations apply access or deletion rights to pseudonymized data but imply that other rights (such as the right to opt-out of the sale of data) might still apply. Ambiguity remains as to what impact pseudonymized data has on rights that are not exempted, such as the right to opt-out of the sale of personal data. For example, while Virginia (under the VCDPA) does not require an organization to re-identify pseudonymized data, it is unclear how an organization could opt a consumer out of having their pseudonymized data sold without reidentification.

Under both the GDPR and the UK GDPR, pseudonymized data is treated differently than anonymized data. Pseudonymization involves the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[77]

7. Sensitive Personal Data

Some privacy statutes explicitly reference "sensitive" or "special" categories of personal data. While such terms, when used, often include similar data types that are considered as raising greater privacy risks to data subjects if disclosed, the exact categories that fall under those rubrics

[76] CAL. CIV. CODE § 1798.140(ab)(2) (West 2024). It should be noted that the reference to pseudonymizing and deidentifying personal information is found within the definition of the word "research." As such it is unclear whether the CCPA was attempting to indicate that personal information will not be considered research unless it has been pseudonymized and deidentified, or whether the CCPA is mandating that companies that conduct research must pseudonymize and deidentify. Given that the reference is found within the definition section of the CCPA, the former interpretation seems the most likely intent of the legislature.

[77] *See, e.g.,* Information Commissioner's Office, *Chapter 3: Pseudonymisation*, (Feb. 2022), https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf.

differ between statutes. Furthermore, some privacy statutes do not expressly reference "sensitive" categories of personal information at all but impart additional protections on certain categories of personal data. As a result, many data privacy attorneys colloquially refer to data types under these statutes as "sensitive" or "special" as they receive special protections.

For example, while the CCPA originally did not use the term "sensitive personal information," it imparted upon data subjects enhanced protections for specific data types (such as social security number or driver's license number) in the event of a data breach. That caused many privacy attorneys and privacy advocates to informally refer to those data types as being "sensitive." Ultimately the CCPA was amended to expressly define a specific data field as being within the rubric of "sensitive personal information."[78] That functionally created a second category of data types that received special status (albeit one that overlapped in many cases with the earlier category).

Some privacy frameworks, such as the NIST Privacy Framework, do not refer to sensitive personal information. Other privacy frameworks, such as ISO 27701 and 29100, define the term generally (and circuitously) as any category of personal information "whose nature is sensitive" or that might have a significant impact on a data subject.

While comparing all the data fields that are considered sensitive between the Modern U.S. State Privacy Laws and the GDPR is beyond the scope of this paper, generally, certain data fields are consistently considered "sensitive" between and across jurisdictions. These include data such as biometric data, ethnic origin, genetic data, sexual orientation, and religious beliefs. Other data fields are recognized by some jurisdictions, but not others, under Modern Privacy Laws. For example, while "sex life" is considered a sensitive category in Europe, California, Colorado, Connecticut, Delaware, Maryland, Montana, New Jersey, and New Hampshire, it is not considered a sensitive category in Florida, Indiana, Iowa, Kentucky, Nebraska, Oregon, Tennessee, Utah, or Virginia.

B. Individuals Covered Under Modern U.S. State Privacy Laws and Modern Privacy Laws

Modern U.S. State Privacy Laws use different terms to describe the individuals that are protected under such laws. The terms that are used include "covered person,"[79] "individual,"[80] and "customer."[81] The term used in a particular statute is less important than its definition. For example, two statutes may use the term "individual," but one may define it as referring to all natural persons, whereas another may define it as referring to only natural persons that are residents within the state.

The CCPA uses the term "consumer" to refer to the individuals whose information is governed by the statute. While the common definition of "consumer" suggests that it refers to an

[78] CAL. CIV. CODE § 1798.140(v)(1)(L)(ae) (West).

[79] ALASKA STAT. ANN. § 45.48.090(2).

[80] *See* ARIZ. REV. STAT. ANN. § 18-552(B)(2).

[81] *See* ARK. CODE ANN. § 4-110-103(3) (West 2021); *see also*, CAL. CIV. CODE § 1798.80(c) (West 2021).

individual that has "consumed" a product or a service, the definition ascribed by the CCPA is far broader. The term is defined to include any "natural person who is a California resident."[82] As a result it includes not only California residents that consume products (such as, a customer of a store) but also California employees, business contacts, or prospective customers. The CPRA deferred most of the substantive provisions in the context of employees and business contacts of the CCPA to January 1, 2023.[83]

In contrast to the diverse terminology used within Modern U.S. State Privacy Laws, the GDPR and the UK GDPR and many EU member state implementing statutes consistently use the term "data subject", which is defined broadly as any "identified or identifiable natural person."[84] Unlike in the CCPA, the term "data subject" contains no residency qualifier.[85] The GDPR does not govern data about companies or legal entities. However, information in relation to one-person companies (such as a single member LLC, as many franchisees have) may constitute personal data where it allows the identification of a natural person. The GDPR also applies to all personal data relating to natural persons in the context of a professional activity, such as the employees of a franchise business, business email addresses such as 'firstname.lastname@franchisebusiness.eu' or employees' telephone numbers. As such, the personal data of a franchise business (franchisor and franchisee) may likely be protected under the GDPR and the UK GDPR.[86]

C. Processing

1. Processing Activities Defined

The CCPA defines "processing" as "any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means."[87] Although the California office of the Attorney General was asked to further define what types of activities constitute "operation[s]" or "set of operation[s]" and, hence, processing, the Attorney General refused stating that the terms were "reasonably clear based on their commonly understood meaning[s]."[88] The Attorney General was further asked to verify that the storage of personal information in the cloud would constitute processing. That request was also declined

[82] CAL. CIV. CODE § 1798.140(i) (West 2021).

[83] CAL. CIV. CODE § 1798.145(m), (n) (West 2021).

[84] GDPR, Article 4(1).

[85] While the term "data subject" does not contain a residency qualifier under the GDPR, the location of a data subject may be relevant, in some situations, when determining whether the GDPR applies to a business.

[86] *See, e.g.,* GDPR, Articles 1-3.

[87] CAL. CIV. CODE § 1798.140(y) (West 2021). The original version of the CCPA included the phrase "personal data" in place of "personal information." The CPRA replaced "information" with "data."

[88] State of California Department of Justice, *Final Statement of Reasons, Appendix A Response 30,* at 8, https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf (last visited Aug. 26, 2024).

with the Attorney General stating that the request constituted a "specific legal question […] that would require a fact-specific determination."[89]

The CCPA's definition of "processing" is substantially like the definition provided for in the GDPR, which is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means."[90] Unlike the CCPA, however, the GDPR provides the following non-exhaustive list of activities that fall within the definition of processing:

- The collection of personal data,*
- The recording of personal data,
- The organization of personal data,
- The structuring of personal data,
- The storage of personal data,*
- The adaptation of personal data,
- The alteration of personal data,*
- The retrieval of personal data,
- The consultation of personal data,
- The use of personal data,*
- The disclosure (or transmission) of personal data,* and
- The destruction of personal data.*[91]

The other Modern U.S. State Privacy Laws have adopted a definition like that of the GDPR, and followed the GDPR's lead by including examples of what constitutes processing. They chose, however, not to include all the examples identified within the GDPR and, instead, only identified those designated with an asterisk in the list above.[92] It is unclear whether U.S. courts will interpret the decision to include some of the GDPR examples, and exclude others, as indicating an intention to substantively diverge from the European definition.

No matter the exact definitions of what constitutes processing under Modern U.S. State Privacy Laws, franchisors and franchisees in most franchise systems are likely to regularly

[89] *Id.*

[90] GDPR, Article 4(2).

[91] *Id.*

[92] *See*, *e.g.,* VA. CODE ANN. § 59.1-575 (2024) and COLO. REV. STAT. § 6-1-1303(18).

process personal data. For example, selling services and products to consumers will often require consumers sharing personal data with the franchisor or franchisee – it would be impossible to make a restaurant reservation, order food online, make a hotel booking, or join a gym without the consumer sharing some personal data with the vendor.

2. "Selling" Personal Data

The Modern U.S. State Privacy Laws create special rules for activities that involve "selling." Among other things, most Modern U.S. State Privacy Laws require companies to allow individuals to opt-out of having their personal information sold. The term "sale" is defined slightly different between and among the state statutes, with some statutes defining the term as including exchanges of personal data in return for valuable consideration, others only exchanges of personal data in return for monetary consideration, and some defining it as both valuable and monetary consideration. It has been suggested that sharing consumer data between franchisors and their franchisees may constitute the sale of personal data.[93]

The GDPR does not discuss the sale of data, nor does it impart specific obligations on a franchisor or franchisees that sells data. That said, under the GDPR for a controller to transfer data to another controller, whether that transfer is considered a "sale," it must identify one of six lawful purposes such as the consent of the data subject, or the legitimate interest of the transferor.[94] Depending on which lawful purpose is identified, a data subject may have the right to opt-in[95] (for example, consent) or object[96] (such as, legitimate interest).

3. "Targeted Advertising"

Most Modern U.S. State Privacy Laws require companies to allow individuals to opt-out of having their personal data used for targeted advertising. The term "targeted advertising" is defined by most states as (1) displaying an ad that is (2) selected based on personal data obtained from (3) a consumer's activities over time (4) a consumer's activities across non-affiliated websites or online applications, and (5) for the purpose of predicting the consumer's preferences or interests.[97]

California is the noticeable exception. Unlike most of the other states, California uses the term "cross-context behavioral advertising"[98] instead of "targeted advertising." The definition of

---

[93] *See* Earsa R. Jackson & Tony Marks, *Do You Want to Know a Secret: The Impact of Consumer Privacy Laws on Franchise Companies*, ABA 43RD ANNUAL FORUM ON FRANCHISING W-15, at 13 (2020).

[94] GDPR, Article 6(1).

[95] *See,* Information Commissioner's Office, Consent, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent (last visited Aug. 21, 2024).

[96] *See,* Information Commissioner's Office, Legitimate interests, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/legitimate-interests/ (last visited Aug. 21, 2024). *See, also,* GDPR, Article 6(1)(f).

[97] *See*, *e.g.,* VA. CODE ANN. § 59.1-575 (2024).

[98] CAL. CIV. CODE § 1798.140(k),(s) (West 2024).

cross-context behavioral advertising is broader insofar as it omits the third and the fifth element identified above.[99] It is narrower insofar as the fourth element within the CCPA's definition refers to activities across different "businesses" and, hence, may not be limited to just online activities occurring on a website or within an application.[100] It remains to be seen whether the California Privacy Protection Agency ("CPPA") or California courts will attempt to align the CCPA's definition with that used in other states' statutes by finding that both elements are implied.

The GDPR does not discuss targeted advertising specifically, nor does it expressly impart obligations on a franchisor or franchisees that engage in the activity. That said, under the GDPR for a controller to use data for a marketing purpose, such as targeted advertising, it must identify one of six lawful purposes such as the consent of the data subject, or the legitimate interest of the transferor.[101] In addition, the ePrivacy Directive requires that direct marketing to data subjects and any retrieval of data stored on a data subject's computer be based on consent. Some European supervisory authorities have interpreted the ePrivacy Directive as functionally requiring that activities such as targeted advertising – particularly if they are going to utilize cookies stored on a data subject's computer – require the prior affirmative consent of the individual.

D. Controllers and Processors

1. Controller Defined

As noted above, under the GDPR a "controller" refers to an entity that "determines the purposes and means" of how personal data will be processed.[102] Most of the Modern U.S. State Privacy Laws adopted the GDPR's definition nearly verbatim.[103]

Unlike the other Modern U.S. State Privacy Laws, the CCPA uses the term "business" instead of "controller." While the definition of business is similar to that of controller, California incorporated volume-of-data and volume-of-revenue thresholds into the definition such that a company that determines the purpose and means of processing is not a "business" under the CCPA if it has gross revenue of less than $25 million per year, derives less than 50 percent of its annual revenue from selling or sharing personal data for the purpose of cross-context behavioral advertising, and buys, sells, or shares for cross-context behavioral advertising data about less than 100,000 Californians.[104] For the purpose of this paper we use the term "controller" in a generic sense to refer to either a "controller" (most statutes) or a "business" (such as, CCPA).

---

[99] *Cf.* CAL. CIV. CODE § 1798.140(k) (West 2024).

[100] *Id.*

[101] *See* GDPR, Article 6(1).

[102] GDPR, Article 4(7).

[103] *See, e.g.,* VA. CODE ANN. § 59.1-575 (2024); N.H. REV. STAT. ANN. § 507-H:1(IX) (2024).

[104] CAL. CIV. CODE § 1798.140(d)(1)(A)-(C) (West 2024).

In some situations, it is straightforward whether a company fits the definition of a controller. For example, all companies are "controllers" in relation to their human resources data as they determine what personal data they collect from their employees and how they will process that data.

In other situations, determining whether a company is a "controller" can be complex. While the analysis is fact driven and can depend upon a variety of factors, if a company makes any of the following decisions in relation to personal data a regulator may consider it to be a controller:

- what personal data will be collected,
- what the personal data will be used for,
- how long the personal data will be stored, and
- who will have access to the personal data (within or outside of the company).

a. Franchisor as Controller

Franchisors will always be considered controllers in relation to two types of personal data: personal data about their employees and personal data that they collect about their franchisees. Some franchisors also consider themselves controllers of consumer information; other franchisors do not. The following are typically the most influential factors that determine whether a franchisor will be considered a controller with regards to the information of consumers:

- Does the franchise agreement or other franchise documents position the franchisor as a controller?
- Does the franchisor have the right and ability to retain consumer data if a franchisee leaves the franchise system?
- Does the franchisor have the right and ability to decide what types of marketing will be sent to a consumer?
- Does the franchisor have the right and the ability to independently choose what vendors or service providers may have access to consumer information?

b. Franchisee as Controller

Franchisees will always be considered controllers in relation to three types of personal data: personal data about their own employees, personal data that they collect about business contacts at the franchisor (such as, franchisor employee business contact information), and personal data about prospective franchisees and their owners. Some franchisees may also be controllers of consumer information gathered by franchised and company-owned outlets; other franchisees will not be. The factors that determine whether a franchisee will be considered a controller with regards to information of consumers are like those that apply to franchisors. They include:

- Does the franchise agreement or other franchise documents position the franchisee as a controller?

- Does the franchisee have the right and ability to retain consumer data if the franchisee leaves the franchise system?

- Does the franchisee have the right and ability to decide what types of marketing will be sent to a consumer independent of the franchisor?

- Does the franchisee have the right and the ability to independently choose what vendors or service providers may have access to consumer information, without supervision by the franchisor?

Historically, franchise agreements have often boldly declared that the franchisor is the owner of the customer data gathered by franchisees. It should be noted that contract provisions such as those are not determinative of who the controller of the data is.

c. Joint Controllers and Separate Controllers

If the franchisor and the franchisee are both considered "controllers" as it relates to a particular type of data (such as, consumer data) some legal systems make a distinction between whether the parties are functioning as joint controllers or separate and independent controllers. The concept of a joint controller was introduced by the GDPR, which defined it as a situation in which two controllers "jointly determine the purpose and means of processing."[105] Designation as a joint controller may have a significant liability ramification under the GDPR, as the regulation allows a data subject to "exercise his or her rights under this Regulation in respect of and against each of the controllers."[106] While Modern U.S. State Privacy Laws recognize that controllers might "jointly" determine the purpose and means of processing, they do not formally recognize the concept of "joint controllers" nor do they state, or imply, that two controllers may be held jointly or severally liable for a statutory violation.

2. Processor Defined

Under the GDPR, a "processor" refers to a company (or a person such as an independent contractor) that "processes personal data on behalf of [a] controller."[107] Most of the Modern U.S. State Privacy Laws adopted the GDPR's definition nearly verbatim.[108]

Unlike the other Modern U.S. State Privacy Laws, the CCPA uses the term "service provider" instead of "processor." While the definition of service provider is like that of a processor, the CCPA requires that to be a service provider the parties must have a written contract in place that imparts that designation and contains specific contractual prohibitions.[109] If such a contract does not exist, or does not match the CCPA's requirements, an entity is arguably not a service provider. While the GDPR and the other Modern U.S. State Privacy Laws also require controllers

[105] GDPR, Article 26(1).

[106] GDPR, Article 26(3).

[107] GDPR, Article 4(8).

[108] *See, e.g.,* VA. CODE ANN. § 59.1-575 (2024); N.H. REV. STAT. ANN. § 507-H:1(XXII) (2024).

[109] CAL. CIV. CODE § 1798.140(ag)(1) (West 2024).

to impose contractual requirements upon processors, if a contract does not exist or a contract is deficient as to its terms that fact does not necessarily transform the processor to a controller; rather the parties' designations may remain the same, but one (or both) parties may be in breach of the privacy laws contracting requirements. For this paper, we use the term "processor" in a generic sense to refer to either a "processor" (most statutes) or a "service provider" (CCPA).

Modern Privacy Laws require that an agreement with a processor contains specific contractual requirements. The contractual requirements of the GDPR and most Modern U.S. State Privacy Laws are similar, although the CCPA contains approximately nine requirements that are not found within other modern privacy statutes.

Franchisors often provide services to their franchisees. If a franchise agreement classifies that a franchisor is the processor of its franchisees, that agreement will need to contain specific contractual provisions that limit the franchisors' ability to use, process, retain, or disclose personal data received from franchisees. Franchisees may provide services to franchisors or collect personal data on behalf of a franchisor. If a franchise agreement classifies a franchisee as the processor of a franchisor, that agreement will need to contain specific contractual provisions that limit the franchisees' ability to use, process, retain, or disclose personal data received from the franchisor or collected on behalf of the franchisor.

IV. GENERAL PRIVACY COMPLIANCE CONSIDERATIONS

A. Compliance Obligations for Controllers

While each of the Modern Privacy Laws impart different obligations on controllers, they generally share core categories of compliance obligations which can broadly be grouped as follows:

- The ability to process data,
- Individual rights owed by businesses to data subjects,
- Accountability and governance obligations,
- Data security obligations,
- Data localization and/or geographic transfer restrictions, and
- Vendor management.

The following chart links each of these categories to specific requirements found in one, or more, of the Modern Privacy Laws. As a reminder, while all Modern Privacy Laws impose some of the requirements (such as creation of a privacy notice), other requirements are not universally applied (for example cross-border data transfer restrictions).

Core Categories of Compliance Obligations	Specific Requirements
Ability to Process Data	Permissible Purpose / Limitations on Use

Core Categories of Compliance Obligations	Specific Requirements
	Data Minimization
	Disclosure Prohibitions
Accountability / Governance	Internal Documentation & Records
	Data Protection / Privacy Risk Assessments
	Training Program
	Designated Data Protection Officer (if necessary) or other responsible individual
Security	Appropriate Data Security to Safeguard Information
	Data Security Adults
	Breach Notification
Individual Rights	Notices to Data Subjects (i.e., Privacy Notice)
	Right to Access Data
	Right to Fix Errors
	Right to Be Forgotten
	Right to Opt-Out of Sale of Information
	Right to Opt-Out of Targeted Advertising
	Right to Object to Automatic Decision making and Profiling
	Right to Object to Other Uses
	Right to Receive Services on Equal Terms
Cross-border transfers	Adequacy measure required for any country determined not to have laws equivalent to those in the data subject's jurisdiction (EEA)

Core Categories of Compliance Obligations	Specific Requirements
Transfers to Third Parties	Contractual Requirements in Service Provider Agreements
	Joint Controllers Should Allocate Responsibilities

B. Core Compliance Documents Considered by Controllers

The written policies and procedures that controllers put into place to assist in their compliance with Modern Privacy Laws differ depending upon several factors including the size of the business, the quantity of personal data that it collects, its industry, what the controller does with the data it collects, with whom it shares it, and under which Modern Privacy Laws the controller is subject. That said, most controllers consider the following seventeen compliance-related documents when trying to create a privacy program built to address the core requirements of Modern Privacy Laws:

- Data Inventory/Data Map,
- Data Retention/Data Destruction Policy and Protocols,
- Privacy Notices,
- Data Subject Request Policies and Protocols,
- Marketing Practices Policies and Protocols,
- Data Protection Impact Assessments,
- DPO/Designation of privacy leaders,
- Privacy Training Program and Policy,
- Written Information Security Program and Policy,
- Incident Response Plan and Protocol,
- Policy on Controller-to-Controller Transfers (inclusive of sales),
- Affiliate Sharing Policy and Documentation,
- Vendor Management Policy, Protocol, and Templates,
- Cross-border Transfer Policy and Supporting Documentation,

- Policy on website-based Targeted Advertising,
- Policy on non-website Targeted Advertising, and
- Artificial Intelligence Policy.

Each of the above documents maps to more than one compliance obligation. For example, drafting and distributing a privacy notice relates to each of the following obligations in bold directly, or indirectly:

Core Categories of Compliance Obligations	Specific Requirements
Ability to Process Data	**Permissible Purpose / Limitations on Use**
	Data Minimization
	Disclosure Prohibitions
Accountability/ Governance	Internal Documentation & Records
	Data Protection / Privacy Risk Assessments
	Training Program
	Designated Data Protection Officer (if necessary) or other responsible individual
Security	Appropriate Data Security to Safeguard Information
	Data Security Audits
	Breach Notification
Individual Rights	**Notices to Data Subjects (i.e., Privacy Notice)**
	Right to Access Data
	Right to Fix Errors
	Right to Be Forgotten
	Right to Opt-Out of Sale of Information

Core Categories of Compliance Obligations	Specific Requirements
	Right to Opt-Out of Targeted Advertising
	Right to Object to Automatic Decision making and Profiling
	Right to Object to Other Uses
	Right to Receive Services on Equal Terms
Cross-border Transfers	Adequacy measure required for any country determined not to have laws equivalent to those in the data subject's jurisdiction (EEA)
Transfers to Third Parties	Contractual Requirements in Service Provider Agreements
	Joint Controllers Should Allocate Responsibilities

Some controllers will decide that they do not need each of these documents; other controllers will decide that they need these and several more. The number of documents that a controller may feel it needs could depend on considerations such as the size of the company; whether the company has the bandwidth to create and comply with these documents; whether the company is involved in activities like targeted advertising, other marketing initiatives, or the cross-border flow of data; whether the company has been in existence long enough to be required to comply with data retention requirements; whether the company offers its products or services in a country that requires a DPO, among other considerations.

C. Compliance Obligations for Processors

Modern Privacy Laws impose some obligations directly on processors, such as a duty to make sure that reasonable and appropriate security is used to protect personal data. That said, most obligations are imposed indirectly on processors. In other words, while the privacy statute or regulation may not expressly mandate that a processor take a certain action (such as delete personal data), it may require that an agreement with a processor impose a specific contractual prohibition or contractual obligation to support the controller (for example contractually requires the processor to delete personal data at the request of the controller or at the expiration of the processing agreement). As a result, it is quite common for agreements and/or data processing agreements (such as marketing or IT-related agreements) to address the deletion of personal data as a contractual requirement where the processor collects or otherwise processes personal data on behalf of the controller. Here is an example provision:

> Vendor and each Vendor affiliate shall promptly and in any event within seven (7) days of the date of cessation of any services involving the processing of company personal data

or at any time by written notice to Vendor (the "Cessation Date"), delete and procure the deletion of all copies of those Company personal data. Vendor shall provide Company with a letter of destruction signed by an executive of the company confirming compliance with this provision.[110]

Because processors are not directly responsible for most of the compliance obligations imposed by Modern Privacy Laws, they tend to have fewer core compliance documents in practice. Specifically, processors tend to consider the following ten compliance-related documents (a sub-set of the seventeen identified above regarding controllers) when creating a processor-oriented privacy program:

- Data Inventory/Data Map,[111]
- Data Retention/Data Destruction Policy and Protocols (in support of contractual obligations to delete),
- Data Subject Request Policies and Protocols (in support of controller requests),
- DPO/Designation of Privacy Leader,
- Written Information Security Program and Policy,
- Incident Response Plan and Protocol,
- Affiliate Sharing Policy and Documentation,
- Sub-processor Management Policy, Protocol, and Templates,
- Cross-border Transfer Policy and Supporting Documentation, and
- Artificial Intelligence Policy.

Processors are often considered "controllers" in connection with other types of personal data that they hold. For example, if a franchise agreement structures franchisees as processors, they may still be controllers in connection with their own employees' personal data as well as business contact information that they maintain about third parties (such as the franchisor's employees). If a processor is considered a controller, it may also consider the additional policies, procedures, and compliance-related documents discussed in the context of controllers.

[110] Note that this language is an example of what a provision may read like regarding a processor needing to comply with deleting data; however, there are several variations of such language. This language was extracted from a data processing agreement that is used by an author of this paper.

[111] Note that processors that keep personal data in self-contained, well-defined, and structured service offerings often choose not to do a formal data inventory or data map, and instead will generate documentation regarding what personal data they collect as requested or needed by their controller.

D. Interaction Between Modern Privacy Laws and Data Security Laws

Before the enactment of the Modern Privacy Laws, states enacted a series of laws focused on securing data from unauthorized access or acquisition (the "data security" laws).

Data security laws can broadly be grouped into three categories:

- Data Safeguard Laws. Data safeguard laws refer to statutes or regulations that require organizations to protect the confidentiality of certain types of personal data. Many state safeguard laws impart only a broad obligation for organizations to utilize "reasonable"[112] security measures to protect such data from unauthorized access, and leave to organizations (and ultimately courts) to determine what specific measures are reasonable. Some states, however, mandate that specific security measures (e.g., encryption or access controls) be implemented by organizations to protect specific types of personal data,[113] or have included guidance as to what practices would be deemed per se reasonable.[114] It is important to note that the safeguards laws in the United States did not extend to all personal data; they focused only on subsets of personal data that were identified within the statutes such as Social Security numbers.

- Data Destruction Laws. Data destruction laws refer to statutes or regulations that require organizations to properly dispose of certain types of personal data once such data is no longer needed by the organization. Some statutes give examples of proper disposal methods for both electronic and paper documents, such as shredding, burning, pulverizing, destroying, or erasing information.[115]

- Data Breach Laws. Data breach laws require organizations to notify impacted individuals, and in some cases government regulators, if the confidentiality of certain types of personal data is compromised. All states, and federal territories, in the United States have enacted a data breach law, although the statutes differ in various respects including what types of personal data trigger an obligation to report a breach.[116]

The Modern Privacy Laws in the United States primarily focus on the collection, use, and intentional sharing of personal data, and do not attempt to replace the data security laws

[112] *See, e.g.,* ARK. CODE § 4-110-104(b) (2024); 815 ILL. COMP. STAT. § 530/45(a) (2024).

[113] *See* MASS. REGS. CODE tit. 201, § 17.03(2) (2024) (setting forth minimum security measures that must be utilized by organizations to protect Social Security numbers, driver's license numbers, or financial account numbers).

[114] *See* 23 N.Y. GEN. BUS. LAW § 899-bb (2024).

[115] David Zetoony & Jena Valdetero, *The Human Resource Professional's Handbook for Data Security Breaches* at 43, BRYAN CAVE LLP, (2017), https://www.bclplaw.com/a/web/96794/Data-Breach-Handbook-HR-Professionals-2017.pdf.

[116] A list of the United States data breach notification laws is available from the International Association of Privacy Professionals (IAPP) and can be downloaded at https://iapp.org/resources/article/state-data-breach-notification-chart/ (last visited July 18, 2024).

discussed above.[117] That said, Modern Privacy Laws have impacted data security in the following ways:

- Expansion of Safeguard Laws. While data safeguard laws traditionally applied to a subset of enumerated personal data types – e.g., Social Security number, Driver's License Number, or financial account number – the Modern Privacy Laws typically extend the obligation to apply "reasonable" security to all personal data.

- Private Right of Action. The CCPA is the only United States Modern Privacy Law that created a private right of action for individuals to recover statutory damages (between $100 and $750 per consumer per incident) if a company failed to enact reasonable security procedures, and that failure resulted in the unauthorized access, exfiltration, theft, or disclosure of personal data.[118] As with traditional safeguards and breach notification laws, it should be noted that this aspect of the CCPA only applies to a narrow subset of personal data.[119]

E. Incorporating Privacy Compliance into Franchise Agreements

The franchise agreement is the foundation for the legal relationship between the franchisor and the franchisee. In addition to express terms in the franchise agreement defining roles and obligations, the modern franchise agreement allows franchise systems to adapt over time. Adaptation is typically implemented by the terms of the agreement that allow the "system," the products and services offered and the systems and processes used to operate the business to change over time as required by the franchisor. As discussed below, adaptation also occurs through the franchise operations manual and the mechanisms in the franchise agreement that allow for franchisors to implement change from time to time.

1. Allocation of Risk and Liability

The first questions a franchisor must ask when considering how to incorporate privacy compliance in the franchise agreement are as follows:

(1) Is the franchisor or franchisee better positioned to identify, evaluate and engage the systems and vendors used by the franchise system with respect to privacy?

(2) Is the franchisor or franchisee better positioned to monitor and respond to changes in applicable law and technology for the system?

---

[117] In contrast, the Modern Privacy Laws in Europe did introduce security concepts that had not previously existed in most Member States. For example, the GDPR breach notification obligations (Articles 33 and 34) which had not previously existed in most Member States.

[118] *Cf.* VA. CODE ANN. § 59.1-578(A)(3) (2024) (requiring under the Virginia Consumer Data Protection Act that controllers establish "reasonable administrative, technical, and physical data security practices" to protect all "personal data") with N.M. STAT. ANN. 57-12C-4 (2024) (requiring that reasonable security be applied only to name in conjunction with Social Security number, driver's license number, biometric data, government-issued identification numbers, or financial account information).

[119] CAL. CIV. CODE § 1798.150(a)(1) (West 2024).

(3) Is the franchisor or franchisee better positioned to identify the systems necessary to control information subject to Modern Privacy Laws?

(4) Is the franchisor or franchisee better positioned to prepare the baseline policies and procedures necessary to achieve system objectives and compliance with Modern Privacy Laws?

(5) Who should bear the liability for decisions made in response to the questions above?

The answers to these questions will instruct the franchisor as to how to draft its franchise agreement and use existing franchise agreement terms to implement changes necessary to address Modern Privacy Laws. These answers may be somewhat contrary to franchisors' instinctual notions that it must mitigate against behaviors that could result in a finding of vicarious liability for actions of franchisees. Thus, franchisors strive to limit the direct control over many aspects of franchisees' day-to-day operations of the business only to the areas and to the degree necessary to protect the brand.

Yet, as between the franchisor and franchisee, the franchisor may be in the best position to evaluate the hardware, software, systems and policies that are necessary for the system to implement from time to time with respect to privacy of the franchisor. The alternative – having each franchisee make these determinations on their own – will likely lead to lack of coordination and uniformity in the franchise system, which will in turn likely lead to greater risks to both the franchisor and the franchisees. Given the potential reputational and monetary risks to the franchisor for privacy violations, franchisors are in the best positions to control and regulate system-wide privacy matters. Accordingly, franchisors will likely find it necessary to accept the vicarious liability risk and control matters related to privacy. The hallmark consideration for franchisor vicarious liability is whether the franchisor exercised control over the specific aspect of the franchisee's business that caused the alleged injury.[120]

2. Franchise Agreement Terms

The franchise agreement is the tool through which the brand and franchise system is implemented in a uniform fashion throughout the entire network of franchisees. Being that the term of franchise agreements is usually five years on the low end, and as long as twenty years, flexibility and adaptability must be built in. Through the mandatory terms of the franchise agreement and the flexibility it offers through language that allows changes, adaptability and evolution of the "system," the standards of the franchisor and the operations manuals, a franchisor can allocate the obligations and associated risks. It is important that the franchise agreement be drafted with data privacy and other technology concerns in mind.

Modern franchise agreements have been drafted with adaptability in mind. Terms such as "system," "standards," "manuals," "policies," and "trademarks" frequently allow the franchisor to supplement or modify the defined terms so that the franchise offering may evolve over time.

[120] *See* Patterson v. Domino's Pizza, LLC, 60 Cal. 4th 474, 498 (2014) (holding franchisor was not vicariously liable for alleged sexual harassment of franchisee's employee by supervisor because franchisor was not involved in personnel decisions regarding franchisee's employees and franchisee—not franchisor—controlled its own sexual harassment policy).

Franchise agreements also frequently include an express provision that allows for modifications and upgrades to various aspects of the system to occur from time to time. Such terms may also include covenants that require the franchisee to agree that systems changes may require additional expenditures by the franchisee. Additional provisions in the franchise agreement also implicate privacy concerns: (1) collection and use of customer data; (2) the right to require types of insurance and coverage amounts; (3) indemnification; (4) the right to designate approved vendors; (5) management of loyalty and gift card programs; (6) limitations on the franchisees use or retention of personal data (particularly if the franchisee is to be a processor); (7) prohibitions on the franchisee keeping personal data if they leave the system (particularly if the franchisee is to be a processor).

Though it is not necessary that such provisions specify that franchisee may have to implement system changes relating to technology, or data privacy specifically, it may be worthwhile to clarify this. Such changes may be costly and may occur with greater frequency than other changes throughout the term of a franchise agreement. The following is an example of what a franchise agreement provision regarding compliance with technology-related system requirements and updates may look like (with additional language intended to avoid joint employer liability related to the franchisor's access to employee information):[121]

> *Franchisee shall, at Franchisee's expense, purchase or lease and install at the Franchised Business all FF&E, software systems, including point of sale systems, and other systems and technology programs specified by Franchisor from time to time. Without regard to the actual capabilities of any enterprise or customer management system or other computer hardware or software that Franchisee installs and that Franchisor has access to directly or indirectly, Franchisor does not have the right to use such technology or tools to direct or assert control over Franchisee's employees' working conditions, except to the extent the control relates to Franchisor's legitimate interest in protecting the quality of the System or the products or services offered by the Franchised Business.*

There is not one way to draft this type of provision. Another example is the following:

> *Franchisee expressly acknowledges that adherence to each and every provision of the System is reasonable, necessary, and essential to maintain the uniform image and favorable reputation of each Location and the System and the success of Franchisor's franchise program, and not to control the day-to-day operation of the Franchised Business. Accordingly, Franchisee expressly agrees to comply with each and every mandatory requirement of the System during the term hereof, as the same may be modified or supplemented by Franchisor in its sole discretion. Such modifications and supplementations may relate to, without limitation, changes in the business, authorized products and services, FF&E requirements, quality standards, operating procedures, compliance with any requirements for computer systems or technology programs, and to pay any fees or charges associated with any such System modifications or supplementations and any other changes reflected in the Manual. Franchisee acknowledges that the marketplace in which it operates may change frequently and quickly during the Term, and that some aspects of the Franchised Business, such as computer systems and technology may need frequent upgrades and changes.*

[121] The two sample clauses are based on provisions in franchise agreements that the authors have come across in their practice.

3. Recent Litigation in the Franchise Space

a. Civil Lawsuits

Because of the complexity of Modern Data Privacy Laws, it is safe to assume that technical data privacy violations of some level occur in franchise systems on a daily basis. For example, requests to opt out of targeted advertising may not be timely processed, or a consumer's information may be retained in some databases, even though it was removed from others. However, in most instances, those types of violations do not make waves in media. Usually, it is not until an actual data breach happens that the public at large becomes aware of issues relating to the maintenance by companies of their personal data.

Data breaches place franchisors at risk of class action lawsuits brought by consumers. Risk increases dramatically when franchisors do not conduct sufficient due diligence to ensure their franchisees' cybersecurity practices sufficiently protect consumer data and when the franchisees' networks connect to the franchisors corporate database. The consequences of such a data breach can be significant.

For example, in November 2023, a Maryland federal court granted a motion for class certification for a suit brought by consumers against hotel franchisor Marriott International after a data breach allowed hackers to gain access to the consumers' personal information from its Starwood guest reservation database.[122] Marriott acquired Starwood in 2016 but failed to conduct appropriate due diligence of Starwood's cybersecurity risks before or after the acquisition, leading to a missive data breach that impacted approximately 383 million guest records.[123] This ruling demonstrates how a franchisor may be held liable for their franchisees' cybersecurity practices even if those practices were put in place before the acquisition occurred.

On June 6, 2023, a judge granted final approval of a class action settlement of $2,350,000, reached with Dickey's Barbecue Pit, to settle claims arising out of a data breach that impacted 172 Dickey's franchise locations in 2019 and 2020.[124] The claims arose from a cyber-attack on Dickey's computer servers and payment card environment, through the installation of an unauthorized code on the point-of-sale- software of certain franchisee restaurants, that granted attackers access to the financial information of hundreds of thousands of Dickey's customers. The settlement agreement also required Dickey's to change many of its business practices surrounding cybersecurity including: the use of multi-factor authentication to access franchisee servers; the use of firewalls to restrict all inbound and outbound traffic not expressly permitted; mandate through its franchising agreements that franchisees migrate to an EMV point of sale system; provide an annual security awareness training for employees; maintain and update a

[122] *In re* Marriott Int'l Customer Data Sec. Breach Litig., 8:19-cv-00094, 2023 WL 8247865 (D. Md. Nov. 29, 2023).

[123] Class Action Complaint, *In re* Marriott Int'l, Inc., Customer Data Sec. Breach Litig., No. 8:19 cv-00094 (D. Md. Oct. 26, 2020).

[124] Kostka v. Dickey's Barbecue Restaurants, Inc., Case No. 3:20-cv-03424-K, 2023 WL 3914266 (N.D. Tex. Jun. 06, 2023).

reasonable written information security program; and conduct risk-based monitoring and threat management of security events on its network.

Data breaches make franchisors not only vulnerable to lawsuits by consumers, but also employees and shareholders.

On March 12, 2024, a former Arby's employee filed a class action lawsuit against Arby's franchise owner DRM Inc. for a data breach that compromised the personal information of former and current Arby's employees.[125] The complaint accuses DRM of failing to properly train employees on cybersecurity measures, failing to maintain reasonable security safeguards, and failing to monitor its employees, vendors, agents, contractors, and suppliers who it allowed to handle employee personal information.

On July 18, 2023, former employees of Domino's Pizza filed a proposed class action complaint against franchisor MAC Pizza Management Inc. alleging that the company failed to protect the personal information of at least 39,000 employee class members during a cyberattack.[126] The plaintiffs alleged that MAC Pizza failed to implement adequate cybersecurity measures to protect employees' confidential data stored on its systems.

In 2016, Wendy's shareholders brought a shareholder derivative suit against certain current and former members of Wendy's board of directors and executive officers seeking remedy for alleged violations of fiduciary duty that caused a data breach impacting over 1,000 franchise locations.[127] The lawsuit alleges that the Aloha point of sale systems, which Wendy's demanded franchisees use, was fraught with security issues that the defendants knew were likely to cause a data breach, and that a data breach would damage the Wendy's brand. Further, the complaint alleges that the defendants breached their duties of loyalty, care, and good faith by: (i) failing to implement and enforce a system of effective internal controls and procedures with respect to data security for the company and its franchisees; (ii) failing to exercise their oversight duties by not monitoring the company and its franchisees' compliance with federal and state laws, payment card industry regulations and its agreements with payment card processors and networks; (iii) failing to cause the company to make full and fair disclosure concerning (a) the effectiveness of the company and its franchisees' policies and procedures with respect to data security, and (b) the scope and impact of the data breach, resulting in the commencement of the financial Institutions class action and consumer class action. This suit reached a settlement that required Wendy's to adopt certain remedial and prophylactic technology and cybersecurity measure, including the establishment of a separate board-level committee to oversee the company's technology and cybersecurity, as well as the creation of a number of data security protocols involving the company's franchisees.

[125] Class Action Complaint, Ruff v. DRM Inc. d/b/a Arby's, No. 1:24-cv-01902-SEG (N.D. Ga. May 01, 2024).

[126] Class Action Complaint, Schramm et al. v. Mac Pizza Management, Inc., No. 4:23-cv-02614 (S.D. Tex. Jul. 18, 2023).

[127] Verified Shareholder Derivative Complaint, *In re* The Wendy's Company Shareholder Derivative Action, No. 1:16-cv-1153 (S.D. Ohio Dec. 08, 2016).

While robust cybersecurity and privacy provisions in franchising agreements are important to protect franchisors from liability in case of a data breach, they should also address how vendors may access and use consumer data collected from franchisees.

On March 20, 2024, a class action lawsuit was filed in California District Court against Carl's Jr. Restaurants, LLC, where the plaintiffs alleged that Carl's Jr. violated California's privacy laws by instructing its franchisees to install and use an automated drive-thru assistant platform, Presto Voice, which plaintiffs used to order food at Carl's Jr. restaurants.[128] This platform was provided and managed by Presto Automation, Inc. who partnered with CKE Restaurant Holdings, Inc., Carl Jr's parent company, in 2023 to deploy Presto Voice in Carl's Jr. restaurants nationwide. The plaintiffs further alleged that they were under the impression that they were interacting only with the Carl's Jr. location where they were placing their order, and they were not notified that their voice recordings would be intercepted by a third-party vendor, who in turn sends the recordings to off-site agents to help train their AI system.

In the above cases, consumers brought suit against franchisors, even if the actions of franchisees themselves directly caused the data breaches, or other violations of consumers' privacy. These cases illustrate the need for franchisors to consider all of the links in the chain of its collection, processing, use, control and protection of personal data and the resulting damage to the brand if there is a break in any link. Accordingly, as a matter of brand maintenance, franchisors may want to strongly consider the highest level of involvement with respect to how data is managed, stored and controlled.

b. Government Action

Data breaches also expose franchisors to the risk of government action. In 2015, the FTC reached a settlement with Wyndham to settle claims that alleged Wyndham's lax security practices allowed hackers to infiltrate the network of a Wyndham franchisee and access Wyndham's corporate network to further access the sensitive consumer data from dozens of other Wyndham franchisees.[129] The stipulated order for injunction required Wyndham to: establish a comprehensive information security program to protect cardholder data; consider risks arising from network connection between Wyndham branded hotels and its corporate data center; and get an annual independent assessment from PCI DSS to insure Wyndham safeguards the connection with its franchisee hotels, and engages in comprehensive risk assessments.

F. Incorporating Privacy Compliance Into Franchise Disclosure Documents

The Franchise Disclosure Document ("FDD") is in large part regulated by the Federal Trade Commission's trade regulation, which is adopted under the FTC Act. The current version of the FTC trade regulation, titled "Disclosure Requirements and Prohibitions Concerning Franchising and Business Opportunities" (the "FTC Franchise Rule") was adopted in 2007.[130] The purpose of the franchise disclosure document is to describe in plain English the information

[128] Class Action Complaint, Cohen v. Carl's Jr. Restaurants, LLC., No. 2:24-cv-2299 (C.D. Cal. Mar. 20, 2024).

[129] Stipulated Order for Injunction, FTC v. Wyndham Worldwide Corp. et. al., No. 2:13-cv-01887-ES-JAD (D.N.J. Dec. 09, 2015).

[130] 16 C.F.R. § 436.1 *et seq*. (2007).

required by the FTC Franchise Rule to be disclosed to prospective franchisees. Below is a table of possible areas of disclosure, each of which may be used to frame and describe the franchisor's then-current standards, intentions and expectations in connection with privacy:

Disclosure Item	Required Disclosures	Privacy Related Implications
Item 1(6)(v)	Any laws or regulations specific to the industry in which the franchise business operates.	Any privacy related disclosures that are specific to the franchise business rather than those that generally apply.
Item 6 (Other fees payment to the franchisor or its affiliates)	Technology fees and other fees similar fees payable.	Disclosures regarding fees that are paid to franchisor or its affiliates for technology fees and the like.
Item 7	Initial Investment for items of hardware and software.	Disclosure of amounts necessary to acquire or license the hardware and software necessary to comply with Modern Privacy Laws.
Item 8	Any particular obligations of the franchisee to purchase or lease computer hardware and software either from the franchisor, its designee, or suppliers approved by the franchisor, or under the franchisor's specifications.	These disclosures may not have specific privacy related disclosures, but consideration should be giving to whether there are additional disclosures relating to privacy matters.
Item 11	A description of computer systems generally in non-technical language. A description of the types of data to be generated or stored in these systems, and state the following: (i) The cost of purchasing or leasing the systems. (ii) Any obligation of the franchisor, any affiliate, or third party to provide ongoing maintenance, repairs, upgrades, or updates. (iii) Any obligations of the franchisee to upgrade or update any system during the term of the franchise, and, if so, any contractual limitations on the frequency and cost of the obligation. (iv) The annual cost of any optional or required maintenance, updating, upgrading, or support contracts.	Consideration should be given to whether new or amended disclosures are needed to address matters related to privacy.

Disclosure Item	Required Disclosures	Privacy Related Implications
	(v) Whether the franchisor will have independent access to the information that will be generated or stored in any electronic cash register or computer system. If so, describe the information that the franchisor may access and whether there are any contractual limitations on the franchisor's right to access the information.	
Item 17	Explanation of any specific curable or non-curable defaults relating to privacy matters. Explanation of the disclosures to include a description of the franchisee's obligations on termination/non-renewal relating to privacy and the information protected and maintained.	If the franchise agreement contains provisions specific terms relating privacy matters, these will be disclosed.
Item 22	Attach a copy of all proposed agreements regarding the franchise offering, including those relating to privacy/data sharing and data protection that the franchisor provides or for which the franchisor makes arrangements.	If the franchisor requires or arranges for additional agreements addressing privacy and related obligations to be signed in connection with entering into the franchise, those agreements may need to be attached to the FDD.

The FTC has been in the process of reviewing and revising the FTC Franchise Rule for several years. General market changes appear to necessitate a review, but the changes to technology since 2007 likewise warrant revisions to the FTC Franchise Rule.

For example, the FTC Franchise Rule technology-specific disclosure are focused on "electronic cash registers."[131] In 2019, the FTC asked for public comment on the FTC Franchise Rule.[132] Among a series of general questions about the impact of the regulation, the FTC also requested input regarding the how the FTC Franchise Rule should be revised to take into consideration changes in technology.[133] Forty-one comments were submitted in response to the request, coming from law firms, franchisors, and from industry groups. The North American Securities Administrators Association ("NASAA") commented and spent a significant amount of its response on how technology changes in general, and also on how additional data privacy-

[131] *Id*. at §436.5(k)(5).

[132] Request for Public Comment, Disclosure Requirements and Prohibitions Concerning Franchising; Regulatory Review, 84 Fed. Reg. 49 (Mar. 13, 2019).

[133] *Id.*

related disclosures would benefit franchisees.[134] For example, NASAA suggested that franchisors would have to disclose if the franchisor would have independent access to customer data, have the right to sell customer data, and whether revenue from such sales would be shared with franchisees.[135]

G. Incorporating Privacy Compliance Into Operations Manuals

The operations manual is the central place to implement system operational standards and system change. Because virtually all franchise agreements will reference and require compliance with the operations manual, the operations manual is a key tool for franchisors to implement standards relating to Modern Privacy Laws. Courts have generally upheld a franchisor's right to implement system changes, even if at additional expense to the franchisee.

V. CROSS-BORDER DATA TRANSFER REQUIREMENTS

A. Restrictive Transfers

Individuals risk losing GDPR protection if their personal data is transferred outside the EEA (in the case of the GDPR) or the UK (in the case of UK). As a result, the transfer of personal data outside the EEA or the UK (which is referred to as a "restricted transfer") is restricted unless the rights of the individuals in respect of their personal data are protected in another way, or one of a limited number of exceptions applies. A restricted transfer is made if:

- processing of the personal data is being transferred outside the EEA or the UK as applicable,
- personal data is accessible to a recipient to whom the GDPR or the UK GDPR does not apply (usually because the recipient is in a country outside the EEA or the UK), and
- the recipient is a separate entity, which includes transfers to another company within the same corporate group. If personal data is sent to an employee of the entity sending the personal data, this is not a restricted transfer.

Before making a restricted transfer, it is necessary to consider whether the aim of the transfer can be achieved without sending personal data outside the EEA or the UK. If data is made anonymous so that it is impossible to identify individuals (even when combined with other information which is available to a recipient), it is not personal data and therefore may be transferred outside the EEA or the UK. The first issue to address is whether the proposed restricted transfer is covered by an "adequacy decision." If an adequacy decision does not exist, then a transfer mechanism must be identified.

[134] Letter from the North American Securities Administrators Association, Inc. submitted to the Federal Trade Commission re: Franchise Rule Regulatory Review, 16 C.F.R. § 436, Matter No. R511003, at 6 (May 13, 2019).

[135] *Id.*

B. Adequacy Decisions

The GDPR and the UK GDPR provide that European and UK governing bodies may determine that a particular country provides "adequate" protection for people's rights and freedoms about their personal data. If such a determination is made, the transfer of information to the country is no longer considered a restricted transfer (as defined directly above). The UK has adequacy regulations relating to the following countries and territories:

- the EEA countries (which include the EU member states, Norway, Iceland, and Lichtenstein),
- the EU or EEA institutions, bodies, offices or agencies,
- Gibraltar,
- the Republic of Korea, and
- countries, territories and sectors covered by the European Commission's adequacy decisions which went into force on December 31, 2020.

The EU Commission has adequacy decisions relating to the following countries and territories:

- Andorra,
- Argentina,
- Faroe Islands,
- Guernsey,
- Isle of Man,
- Israel,
- Jersey,
- New Zealand,
- Switzerland,
- Uruguay, and
- the UK.

In addition, there are partial findings of adequacy concerning:

- Canada though only in respect of data that is subject to Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),

- Japan though only in respect of personal data transferred to private sector organizations subject to Japan's Act on the Protection of Personal Information. This does not include transfers of the types listed in the EU's adequacy decision for Japan, and

- The U.S. though only in respect of personal data which is transferred under the UK Extension to the EU-U.S. Data Privacy Framework.[136]

The UK Government has announced that it is working in partnership with several priority countries which may be the subject of adequacy regulations in the future, including Australia, Brazil, Colombia, the Dubai International Financial Centre, India, Indonesia, Kenya and Singapore.

C. Transfer Mechanisms

In the event that an organization intends to send data to another organization in a country that lacks an adequacy decision, the data exporter (which is the organization transmitting personal data outside of Europe or the UK) and the data importer (which is the organization receiving personal data in a country outside of Europe or the UK) must put a "safeguard"[137] in place that imposes many of the substantive provisions found within the GDPR. Acceptable safeguards are those that have been validated by the European Commission (for Europe) and the ICO (for the UK). Such safeguards are often referred to colloquially as "transfer mechanisms."[138] Those safeguards are set out below.

1. Standard Contractual Clauses

A restricted transfer can be made if the data exporter and the data importer have entered into a contract incorporating one of the four standard data protection clauses adopted by the European Commission (referred to as "Standard Contractual Clauses" or "SCCs"). In the UK the ICO[139] has indicated acceptance of two sets of such standard data protection clauses (referred to as the "International Data Transfer Agreement" or "IDTA"). The SCCs contain contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter.

The SCCs must be used in their entirety. Except for certain provisions within the SCCs and IDTA that are customizable, the clauses cannot be amended or modified without losing their status as an effective transfer mechanism. While the clauses cannot be amended or modified, additional clauses can be included on business related issues, if they do not contradict the SCCs

[136] Data Privacy Framework (DPF) Overview, DATA PRIVACY FRAMEWORK PROGRAM, https://www.dataprivacyframework.gov/Program-Overview (last visited July 2, 2024).

[137] GDPR, Article 42.

[138] GDPR, Articles 44-49.

[139] GDPR, Articles 46(2)(d) and 93(2).

or IDTA. SCCs and the IDTA are the most common transfer mechanism utilized to facilitate a restricted transfer.

2. Binding Corporate Rules

A restricted transfer can be made if both the data exporter and the data importer have signed up to a group document called binding corporate rules[140] ("BCRs").[141] BCRs are an internal code of conduct that operate within a multinational group, which applies to restricted transfers of personal data from the group's EEA or UK entities to non-EEA or UK group entities. This may be a corporate group, or a group of undertakings or enterprises engaged in a joint economic activity, such as franchisees and their franchisor. BCRs must be submitted for approval to the relevant supervisory authority or to the ICO if one of the companies is based in the UK or if outside the UK where the relevant EEA head office is located.[142] Due to their complexity, the need for advance approval by supervisory agencies, and limitations in transmitting data to entities that are not within a common group, BCRs are not a common transfer mechanism. For perspective, although millions of cross-border data transfers have occurred since the GDPR went into effect, according to the European Data Protection Board ("EDPB") only 61 companies have submitted, and received approval for, their BCRs since 2018.[143]

a. Approved Code of Conduct Together with Binding and Enforceable Commitments by the Recipient

Theoretically, a restricted transfer may be completed where the data importer has agreed to a code of conduct, which has been previously approved by a supervisory authority. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, and which can be directly enforced. While the GDPR endorses the use of approved codes of conduct to demonstrate compliance with its requirements in theory, no codes of conduct have been approved by the EDPB or the ICO in practice.[144] As a result, the use of an approved codes of conducts is not a viable method for effectuating a restricted transfer at this time.

---

[140] GDPR, Article 47.

[141] GDPR, Article 42.2(b).

[142] *The criteria for choosing the lead authority for BCRs is laid down in the "Working Document Setting Forth a Co-operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR,* EUROPEAN COMM'N, (Apr. 16, 2018), https://ec.europa.eu/newsroom/article29/items/623056. The concept of using BCRs to provide adequate safeguards for making restricted transfers was developed by the Article 29 Working Party in a series of working documents. These form a "toolkit" for organizations. The documents, including application forms and guidance have all been revised and updated in line with GDPR.

[143] *See* EDPB list of Approved Binding Corporate Rules available at https://www.edpb.europa.eu/our-work-tools/accountability-tools/bcr_sl (last visited June 30, 2024).

[144] *But see* European Data Protection Board, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (June 4, 2019), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf.

b. Approved Certification Mechanism Together with Binding and Enforceable Commitments of the Recipient

Theoretically, if the data importer has a certification under a scheme approved by a supervisory authority, a restricted transfer can be made which must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, and which can be directly enforced. As of the writing of this paper the authors are not aware of any certification mechanism which has been approved by a supervisory authority.

c. Use of Bespoke Contractual Clauses Authorized by a Supervisory Authority

A restricted transfer can be made if a bespoke contract governing a specific restricted transfer is entered into which has been individually authorized by the ICO for the purposes of the UK GDPR or by an EEA supervisory authority of the country from which the personal data is being exported. In practice this means that prior to transferring personal data to a non-adequate country a data exporter would need to approach a supervisory authority and ask them to approve a transfer scheme (such as a contract) that deviates from the SCCs. Given the cost, complexity, and uncertainty of such a request, as well as the potential time involved to make such a request, it is not a common method for transferring personal data to a non-adequate country. While published statistics concerning the use of ad hoc approved transfers mechanisms are not available, anecdotally the authors – who have collectively facilitated thousands of cross border transfers – are not aware of any such mechanisms being utilized.

d. Trans-Atlantic Data Privacy Frameworks

As indicated above, in the discussion of adequacy decisions, the U.S. is unique insofar as it has received an adequacy decision, but only in connection with U.S. organizations that certify to participate in a voluntary program. Given that the adequacy decision depends on an organization taking an additional step, we treat it in this paper as a transfer mechanism.

The U.S. adequacy decision has a long and complex history. The U.S. first received adequacy in 2000 (prior to the enactment of the GDPR) in conjunction with a program referred to as the U.S. – EU Safe Harbor Framework ("Safe Harbor"). On October 6, 2015, the Court of Justice of the European Union ("CJEU") handed down judgment in *Schrems v. Data Protection Commissioner (Ireland)* ("Schrems") invalidating the decision of the European Commission that approved the U.S. Safe Harbor framework and had given it adequacy.[145] One of the major deficiencies cited by the CJEU was the ability of the U.S. intelligence services to gain access to transferred personal data which, in the CJEU's view, went beyond what was necessary and proportionate for the protection of national security. The CJEU also was concerned that there was a lack of any right for non-U.S. persons to seek legal remedies in the U.S. for misuse of their personal data.

[145] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:627 (October 6, 2015) (Schrems I).

In 2016, the Commission and the U.S. Department of Commerce created a new framework called the EU-U.S. Privacy Shield ("Privacy Shield").[146] The Privacy Shield was intended to replace and supplant the Safe Harbor. The CJEU issued a second opinion ("*Schrems II*") in July of 2020 invalidating the Privacy Shield.[147] As in the first *Schrems* case, the Court's principal concerns were that U.S. public authorities' use of and access to EU personal data were not restricted by the principle of proportionality, and a perceived lack of effective redress mechanisms for EU data subjects to challenge surveillance practices.

The Commission and the U.S. Department of Commerce created a third framework called the EU-U.S. Data Privacy Framework ("DPF")[148] which received adequacy status from the Commission and the UK Parliament in 2023.[149] The organization[150] responsible with challenging (and ultimately obtaining the invalidation of) Safe Harbor and Privacy Shield indicated that it will challenge DPF stating that, in its view, DPF "is a copy of Privacy Shield (from 2016), which in turn was a copy of 'Safe Harbor' (from 2000)."[151] As of the writing of this paper, the Commission's adequacy decision has not been overturned and, as a result, DPF is considered a valid transfer mechanism.

It should be noted that not all organizations may participate in DPF. It is only open to organizations that self-certify to the U.S. Federal Trade Commission ("FTC") and/or U.S. Department of Transportation.[152] This excludes some U.S. financial services institutions, common carriers such as airlines, non-profit organizations, and some telecommunication companies from participating. As of the writing of this paper, 2,860 organizations had self-certified to participate in DPF.[153] This number is significantly less than the quantity of organizations that participated in Safe Harbor and Privacy Shield, and a fraction of the organizations that utilize cross-border restricted transfers.

---

[146] Press Release, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, EUROPEAN COMMISSION, February 2, 2016, https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216.

[147] Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020) (Schrems II).

[148] *See, e.g.* https://www.ftc.gov/business-guidance/privacy-security/data-privacy-framework (last visited September 3, 2024).

[149] Press Release, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows;* EUROPEAN COMMISSION, July 10, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

[150] *See* The NOYB – European Center for Digital Rights, https://noyb.eu/en (last visited July 2, 2024).

[151] European Commission gives EU-US data transfers third round at CJEU, *New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". noyb will challenge the decision* (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

[152] *See* Data Privacy Framework (DPF) Overview, https://www.dataprivacyframework.gov/Program-Overview (last visited July 8, 2024).

[153] *See* Data Privacy Framework Program, https://www.dataprivacyframework.gov/list (last visited June 30, 2024).

3. Exceptions to the Requirement to Have an Adequacy Decision or an Approved Transfer Mechanism

If a restricted transfer is not covered by an appropriate safeguard (such as an adequacy decision or an approved transfer mechanism), it may still be possible to transfer the personal data outside of the EEA or the UK so long as an exception applies.[154] The following summarizes the available exceptions.

a. Has the Individual Given Valid Consent to the Restricted Transfer?

Under Modern Privacy Laws, consent is only "valid consent" if it is both specific and informed. As such, the individual must be provided with precise details about the restricted transfer. An organization (such as the franchisor or franchisee) must provide the following information to the individual prior to engaging in a cross-border transfer of their personal data:

- the identity of the recipient, or the categories of recipients,
- the country or countries to which the data is to be transferred,
- why it is necessary to make a restricted transfer,
- the type of data that will be exported,
- the individual's right to withdraw consent, and
- the possible risks involved in making a transfer to a country which does not provide adequate protection for personal data and without any other appropriate safeguards in place. For example, it may be necessary to explain that there will be no local supervisory authority, and no (or only limited) individual data protection or privacy rights.

As demonstrated, there is a high threshold for obtaining valid consent. The individual must also be allowed to withdraw their consent for the consent to be valid. This may mean that relying on consent as the lawful basis may not be a realistic solution for many transfers in a franchise system.

b. Is the Restricted Transfer Necessary to Take Steps Requested by the Individual to Perform the Contract?

This exception explicitly states that it can only be used for occasional restricted transfers. This means that the restricted transfer may happen more than once but not regularly. The transfer must also be necessary, which means that the core purpose of the contract or the core purpose of the steps needed to enter into the contract, cannot be performed without making the restricted transfer. It does not cover a transfer to a cloud-based IT system. An example of the necessary steps to enter into a contract would, for instance, arise if an individual wishes to reserve

[154] GDPR, Article 49.

a room in a hotel in Denver and, for this purpose, the UK travel agency may have to send the Denver hotel the name of the customer in order to hold the room.

There may also be a situation where a contract with an individual benefits another individual whose data is being transferred. This exception may only be used for occasional transfers, and the transfer must be necessary to perform the core purposes of the contract or to enter into that contract.

c. A Restricted Transfer Needs to be Made for Important Reasons of Public Interest

There must be an applicable EU member state law which states or implies that this type of transfer is allowed for important reasons of public interest, which may be in the spirit of reciprocity for international co-operation. For example, an international agreement or convention (which the UK or an EEA country has signed) that recognizes certain objectives and provides for international co-operation, such as the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism. In practice, however, this is unlikely to apply as it relates to franchise systems.

d. A Restricted Transfer is Needed as it Relates to Legal Claims

This exception explicitly states that it can only be used for occasional transfers of personal data. This means that the transfer may happen more than once but not regularly. If personal data is regularly transferred, an appropriate safeguard should be put in place. The transfer must be necessary, so there must be a close connection between the need for the transfer and the relevant legal claim. The claim must have a basis in law, and a formal legally defined process, but what constitutes a legal claim can be interpreted quite widely. It covers, for example:

- all judicial legal claims, including contract law and criminal law. The court procedure does not need to have been started, and it covers out of court procedures. It covers formal pre-trial discovery procedures, and

- administrative or regulatory procedures, such as the defense of an investigation (or potential investigation) in antitrust law or financial services regulation, or to seek approval for a merger.

This exception cannot be used if there is only the possibility that a legal claim or other formal proceedings may be brought in the future.

e. A Restricted Transfer Must be made to Protect the Vital Interests of an Individual

This exception applies where the restricted transfer must be made to protect the vital interests of an individual. The individual must be physically or legally incapable of giving consent. For example, this exception may apply during a medical emergency where the cross-border transfer of data is needed to give the medical care and therefore is less likely to apply in the context of a franchise system.

f. A Restricted Transfer is Made to a Public Register

Here, the register must be created under the law of the applicable EEA country or the UK (in the case of the UK GDPR) and must be open to either: the public in general, or any person who can demonstrate a legitimate interest. For example, this may apply in the context of registers of companies, associations, criminal convictions, land registers or public vehicle registers. Again, this is unlikely to apply in the context of a franchise system.

g. A One-Off Restricted Transfer Based on Compelling Legitimate Interests

If an organization is unable to rely on any of the exceptions outlined above, this final exception may be considered. However, it should not be relied on routinely because it is only for truly exceptional circumstances involving small quantities of personal data. It is unlikely to apply in a franchising context. It should be noted that supervisory authorities will expect that the data exporter can demonstrate that no approved transfer mechanism was available which could have been relied upon to transfer the data.

VI. OTHER NON-GDPR LEGISLATION AFFECTING PRIVACY

Under European privacy laws, an organization must provide information if it uses cookies or any other type of technology to store or gain access to information on its device, and clearly explain what its cookies do and why. Organizations must also obtain the user's consent, which needs to be clearly given. Essentially, a cookie is a small text file that is downloaded onto 'terminal equipment' (such as a computer or smartphone) when the user accesses a website. It allows the website to recognize that user's device and store some information about the user's preferences or past actions. There is an exception to the requirement for consent if the cookies are considered essential to provide an online service at someone's request (for example, to remember what is in their online cart, or to ensure security in online banking). In summary, organizations must:

- tell individuals that the cookies are there,
- explain what the cookies are doing and why, and
- obtain the individual's consent to store a cookie on their device.

If this information is communicated to the individual the first-time that cookies are set, there is no need to repeat it every time that person visits the organization's website. However, if cookie use changes, the organization may need to ask the individual for updated consent. In addition, several supervisory authorities have advised that once consent is obtained it should be resolicited after some period, ranging from six months according to some supervisory authorities to two years according to others. Although this section refers to cookies, the requirements apply to any method by which information is stored on a user's device or gains access to information on a user's device, is obtained. Spyware or any similar covert surveillance software that downloads to a user's device and tracks their activities without their knowledge is prohibited.

VII. ENFORCEMENT, PENALTIES FOR NON-COMPLIANCE

A. Enforcement and Comparing Jurisdictional Differences

1. Modern U.S. State Privacy Laws

As of the date of this paper, no complaints have been filed in court under Modern U.S. State Privacy Laws. This is likely because such laws are relatively new with several still not in effect. California (the CCPA) is the oldest statute under Modern U.S. State Privacy Laws, which became effective more than four years ago on January 1, 2020. California appears to be the catalyst for the next wave of Modern U.S. State Privacy Laws, which started with the state of Virginia going into effect almost two years ago on January 1, 2023. The states of Colorado and Connecticut continued this momentum enacting their respective state privacy laws, which laws went into effect on July 1, 2023. Other state privacy laws went into effect thereafter and/or are coming into effect in future years.

Generally, Modern U.S. State Privacy Laws authorize the Attorney General to enforce privacy legislation. Some states, however, grant concurrent jurisdiction to other agencies. For example, the CCPA created a new agency known as the California Privacy Protection Agency ("CPPA"). The CPPA is the state agency tasked with most CCPA rulemaking and other enforcement mechanisms through administrative fines while the Attorney General is responsible for levying penalties and injunctive relief.[155] As such, both the Attorney General and the CPPA have concurrent jurisdiction to enforce the CCPA. In contrast, the Colorado Privacy Act ("CPA") granted Colorado's twenty-two district attorneys the authority to enforce the CPA, but not the authority to issue their own rules.

Modern U.S. State Privacy Laws impose penalties for non-compliance in the range of $2,500-$20,000 per violation depending on the state, with the potential for even greater damages under states such as Washington and Colorado, as further explained below. Certain Attorney Generals are mailing letters to businesses with the intent of educating these businesses about the laws and their legal obligations prior to levying any penalties. Colorado's Attorney General is one example of where it is issuing warning letters to companies that are allegedly violating its privacy law.[156] Other Attorney Generals allow for "cure periods" prior to initiating any enforcement action. Below are some examples of the types and amounts of penalties that may be imposed under Modern U.S. State Privacy Laws.

a. California

As noted above, the CCPA grants enforcement authority to both the CPPA and the California Attorney General. The CPPA is empowered to enforce the CCPA and its regulations through administrative proceedings that may result in a cease-and-desist order and, possibly, administrative fines.[157] However, the Attorney General also has the authority to investigate

[155] California Privacy Protection Agency, https://cppa.ca.gov/about_us/ (last visited July 2, 2024).

[156] Colorado Attorney General, *Colorado Privacy Act*, https://coag.gov/resources/colorado-privacy-act/ (last visited July 2, 2024).

[157] CAL. CIV. CODE § 1798.155(a).

potential violations and seek the same civil penalties and injunctions. As such, any business, service provider, contractor or other person that violates this act may be subject to an injunction and liable for civil penalties of not more than $2,500 per non-intentional violation and $7,500 per intentional violation, including violations involving the personal data of minor consumers under the age of 16 years. The court may consider the cooperation and good faith of all parties involved in determining the amount of the civil penalty.[158] The Attorney General and the CPPA must deposit all civil fine proceeds in a Consumer Privacy Fund,[159] which is a special fund intended to off-set costs incurred by the courts and other agencies.[160]

b. Virginia

The Virginia Attorney General has exclusive authority to investigate and enforce the VCDPA by seeking an injunction to restrain violations and impose penalties for non-compliance of up to $7,500 per violation, and reasonable expenses including attorneys' fees.[161] However, prior to initiating any action, the Attorney General must provide a controller or processor 30 days' written notice outlining the provisions that the business has allegedly violated. If within the 30-day period the controller or processor cures the violation and gives the Attorney General a statement that the alleged violations have been cured and that no further violations will occur, no further enforcement action will be taken.[162]

c. Colorado

As noted above in this section, there is the potential for even greater damages under the CPA compared with some of the other state privacy laws. The Colorado Attorney General has both enforcement and regulatory authority under the act.[163] The CPA provides that violations are considered an unfair trade practice under the Colorado Consumer Protection Act[164] but only for Attorney General or district attorney enforcement.[165] Businesses could be subject to a civil penalty of up to $20,000 per violation for non-compliance if the violation cannot be cured within 60 days. However, prior to any enforcement action, the Attorney General must send a notice of violation to the controller if a cure is possible.[166] The process of providing notice of a violation

---

[158] CAL. CIV. CODE §§ 1798.155(a); 1798.199.55(a)(2); 1798.199.90(a).

[159] CAL. CIV. CODE § 1798.160.

[160] CAL. CIV. CODE § 1798.155(b).

[161] VA. CODE ANN. § 59.1-584(C).

[162] *Id.* § 59.1-584(B).

[163] COLO. REV. STAT. ANN. §§ 6-1-1311; 6-1-1313.

[164] COLO. REV. STAT. ANN. § 6-1-105.

[165] COLO. REV. STAT. ANN. § 6-1-1311(1)(c).

[166] Colorado Attorney General, *Colorado Privacy Act*, https://coag.gov/resources/colorado-privacy-act/ (last visited Aug. 22, 2024).

and allowing for the cure period will end as of January 1, 2025.[167] Further, the potential civil penalty maximum may be increased to $50,000 for violations committed against elderly people.[168] As such, the upper limit of civil penalties under the CPA are considerably higher than the civil penalties in some of the other states such as Virginia.

d. Connecticut

The Connecticut Attorney General has exclusive authority to enforce violations of the Connecticut Personal Data Privacy and Online Monitoring Act ("CTDPA").[169] While violations of the act do not provide a basis for a private right of action, there is an exception as it relates to application of the Unfair Trade Practices Act. The CTDPA states that violations constitute an unfair trade practice under the Unfair Trade Practices Act's private right of action,[170] which is enforceable only by the Attorney General.[171] Initial violations may result in an injunction, an order directing restitution, or both, together with reasonable attorneys' fees. The CTDPA allows businesses a 60-day cure period to correct violations without penalties through the end of 2024. However, after this cure period, civil penalties, or willful violations, will be enforced for up to $5,000 per violation.[172]

e. Utah

Both the Utah Department of Commerce's Division of Consumer Protection and the Utah Attorney General have enforcement authority under the Utah Consumer Privacy Act ("UCPA").[173] The UCPA states that violations do not provide a basis for a private right of action.[174] Violations of the act may result in monetary penalties of (a) the actual damage to the consumer, and (b) an amount not to exceed $7,500 per violation.[175] However, at least 30 days before the Attorney General initiates an enforcement action against a company, the Attorney General must provide the company with notice of the alleged violations. The business has 30 days to cure the violation from the date of receipt of this notice.[176] All money received from any such enforcement action is

---

[167] *Id*.

[168] COLO. REV. STAT. ANN. § 6-1-112(1)(a)(c).

[169] CONN. GEN. STAT. ANN. § 42-525(a).

[170] CONN. GEN. STAT. ANN. § 42-110(b).

[171] CONN. GEN. STAT. ANN. § 42-110(g).

[172] CONN. GEN. STAT. ANN. § 42-110(m)(b).

[173] UTAH CODE ANN. §§ 13-61-401; 13-61-402.

[174] UTAH CODE ANN. § 13-61-305.

[175] UTAH CODE ANN. § 13-61-402(3)(d).

[176] UTAH CODE ANN. § 13-61-402(3).

deposited into the Consumer Privacy Account for such items investigation and administrative costs incurred by the agencies in investigating the complaints alleging violations of the act.[177]

f. Washington

As noted above in this section, the Washington state privacy law allows for potentially greater damages than some of the other state privacy laws. Washington's My Health My Data Act ("MHMDA") was enacted, in part, to protect individual's health data not covered under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[178] Under the law, health related data is broadly defined to include any information that identifies, relates to, or could be used to identify a person's health condition, treatment, diagnosis, medication, biometrics, or any information derived from such data.[179] For example, a fitness mobile application that collects data on an individual's physical activity may likely need to comply with the MHMDA, including obtaining affirmative consent prior to collecting their data and grants individuals several privacy rights (such as the right to delete one's data). Section 11 of the MHMDA states that a violation of the MHMDA is an unfair and deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the Washington's Consumer Protection Act.[180] The Consumer Protection Act prohibits all "unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce".[181] Therefore, to understand allowable damages under MHMDA one must understand its connection to the Consumer Protection Act. The Consumer Protection Act provides for both (a) public enforcement by the Attorney General and (b) private actions by individuals who have suffered harm due to such practices. Under the Washington Consumer Protection Act, there are three types of damages:

- Actual damages, which may be awarded to individuals who suffer economic injury due to unfair or deceptive practices can seek actual damages, which include compensation for direct economic losses incurred,[182]

- Liquidated damages, which may be awarded in certain circumstances, which are predetermined amounts specified in the law or contract rather than being based on the actual harm suffered,[183] and

[177] UTAH CODE ANN. § 13-61-403.

[178] Pub. L. No. 104-191 (1996).

[179] WASH. REV. CODE §§ 19.373.010(4), (8), (11), (13), (15), (24)-(25).

[180] WASH. REV. CODE § 19.373.010(11).

[181] WASH. REV. CODE §§ 19.86.020; 19.86.023.

[182] WASH. REV. CODE § 19.86.090.

[183] *Id.*

- Treble damages, which may be awarded where the court finds that the defendant knowingly violated the Washington Consumer Protection Act, in which case it can award up to 3 times the actual damages to the plaintiff.[184]

Violations of the MHMDA are *per se* violations of the Washington Consumer Protection Act without any further analysis needed. Therefore, Washington is unique compared with other state privacy laws since it allows for private action by individuals, thus opening the door to the potential for increased legal action.[185]

g. Summary

As outlined in this section, penalties under Modern U.S. State Privacy Laws can quickly multiply depending on the number of violations and because Attorney Generals (and the CPPA in California) could interpret each impacted individual as equaling one violation. The potential for even greater penalties exists in the states of Washington and California (in relation to data breaches) since both laws allow individuals to initiate private actions against companies where they believe the company violated the laws.

2. GDPR and UK GDPR

National authorities may assess fines for specific violations of the GDPR and the UK GDPR, which may be applied in addition to (or instead of) further remedies or corrective powers. Both the processor and/or controller may be subject to penalties depending on which entity is responsible for the violation. The fines must be effective, proportionate, and dissuasive for each individual situation.[186] Under both the GDPR and the UK GDPR, penalties are based on 2 tier thresholds depending on the type of infringement. For example, under the GDPR, infringements of the following provisions are subject to administrative fines up to €20,000,000 (or £17,500,000 under the UK GDPR), or in the case of an undertaking up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- non-compliance with the basic privacy principles for processing personal data (such as, complying with the conditions for obtaining valid consent);
- non-compliance with the data subjects' privacy rights (such as the right to have the consumer's information deleted or erased);
- violations of the requirements pertaining to the cross-border transfer of personal data (such as failing to execute standard contractual clauses prior to exporting personal data from the EEA to the U.S.);

[184] *Id.*

[185] *See,* David A. Zetoony, *What are the damages for violating Washington's My Health My Data Act?* GREENBERG TRAURIG DATA PRIVACY DISH, June 8, 2023, https://www.gtlaw-dataprivacydish.com/2023/06/what-are-the-damages-for-violating-washingtons-my-health-my-data-act/#_ftnref2.

[186] GDPR, Article 84(1).

- violation of any obligations pursuant to Member State implementation legislation (such as processing personal data in the context of employment); and

- non-compliance with an order or limitation on processing issued by the supervisory authorities.[187]

Infringements of the following provisions are subject to administrative fines of up to €10,000,000 (£8,700,000 under the UK GDPR) or in the case of an 'undertaking' up to 2% of the total worldwide annual revenue of the preceding financial year, whichever is higher:

- non-compliance with the obligations of the controller and the processor; and

- failure to comply with the obligations of the certification body and monitoring body.

The concept of an 'undertaking' encompasses every entity engaged in an economic activity, regardless of the legal status of the entity or the way in which it is financed. An undertaking can therefore not only consist of one individual company (such as a franchisee), but also several natural persons or corporate entities. Thus, a whole group can be treated as one undertaking and its total worldwide annual turnover can be used to calculate the fine for a GDPR infringement of one of its companies.[188]

3. Comparing Private Right of Action Provisions

As of the date of this paper, most Modern U.S. State Privacy Laws do not allow for a private right of action, meaning the ability of consumers to sue a business (such as a franchisor or franchisee) directly. However, California and Washington are the exceptions to this since both state privacy laws allow consumers to directly bring legal action against businesses. Under the CCPA, consumers may bring a private right of action where there is a compromise of data due to the failure to implement and maintain reasonable security measures (a data breach). In this case, the consumer may recover either statutory damages between $100 and $750 per consumer per incident, or actual damages (which is the true damages equivalent to the loss to the consumer), whichever is more.[189] Consumers are not allowed to bring a private right of action against a company for any other alleged violation of the act.

On the other hand, Washington allows consumers to bring allegations and private rights of action for a wide range of violations beyond allegations of security breaches. For example, a consumer may bring a complaint against a business where a consumer believes the business has failed to follow the statute's affirmative consent requirements prior to processing a consumer's health-related data. This would be considered an unfair or deceptive act under Washington's Consumer Protection Act.[190]

---

[187] GDPR, Article 83(6).

[188] *See* General Data Protection Regulation (GDPR), Fines/Penalties, https://gdpr-info.eu/issues/fines-penalties/ (last visited July 2, 2024).

[189] CAL. CIV. CODE § 1798.150.

[190] WASH. REV. CODE § 19.86.020.

Under GDPR and the UK GDPR, consumers have three options for filing complaints if they believe their data protection rights have been violated: (1) lodge a complaint with their national data protection authority, (2) take legal action against the business, or (3) take legal action against the data protection authority if the consumer believes the authority has not handled their complaint correctly.[191] These laws grant consumers the right to compensation for material or non-material damage suffered. The compensation may be claimed from the entity responsible for the violation, which may be the controller or processor (franchisor or franchisee) or some combination thereof.[192]

B. Examples of Enforcement Actions

In this section, the phrase "enforcement action" is used broadly to cover both legal actions brought against businesses (such as by Attorney Generals), and investigations brought by governmental authorities (such as by Attorney Generals) against businesses that ended amicably. As of the time of writing this paper, California is the only state that has brought enforcement actions against business for violations of its law. The fact that enforcement actions by an Attorney General have only been brought by one state may be due to the relatively recent effective and enforcement dates of Modern U.S. State Privacy Laws, as well as the issuance of warning letters and opportunities to cure alleged violations as outlined above.

1. California Enforcement Actions

This section outlines enforcement actions brought by the California Attorney General and/or the CPPA under the CCPA. Currently, there are three enforcement actions against the following companies: Sephora, Door Dash, and Tilting Point Media LLC.[193]

a. Sephora

In August 2022, the first enforcement action under the CCPA was brought against cosmetic retailer Sephora Inc. The California Attorney General alleged that Sephora (a) failed to disclose to consumers that it was selling their personal information, (b) did not process consumer's opt out of sale requests leveraging global privacy controls;[194] and (c) failed to cure these allegations within the allowed for cure period.[195] In a stipulated judgment, Sephora agreed

[191] European Commission's Directorate-General for Communication, *What Should I do if I Think That my Personal Data Protection Rights Haven't Been Respected?,* https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/redress/what-should-i-do-if-i-think-my-personal-data-protection-rights-havent-been-respected_en (last visited July 9, 2024).

[192] GDPR, Article 82.

[193] State of California Department of Justice, Privacy Enforcement Actions, https://www.oag.ca.gov/privacy/privacy-enforcement-actions (last visited Aug. 24, 2024).

[194] Note that global privacy controls are a user enabled browser setting that allows users to opt out of the sale or sharing of their personal data. It is a legal requirement in California and aligns with the CCPA. This requirement varies by Modern U.S. State Privacy Laws.

[195] *Id.*

to pay $1,200,000 to resolve these allegations and was required to design a more comprehensive compliance program to ensure its adherence with the CCPA.[196]

As part of creating the more robust compliance program, Sephora was required to clarify in its online disclosures and privacy notice to include an affirmative representation that it sells data; provide mechanisms for consumers to opt out of the sale of personal data, including via the global privacy control; conform its service provider agreements to the CCPA's requirements, and provide reports to the Attorney General relating to its sale of personal data, the status of its service provider relationships, and its efforts to honor global privacy controls.[197] The Sephora settlement is notable for several reasons like:

- It highlights the broad interpretation of the "sale of personal data," including that it is relatively easy for governmental authorities to learn whether companies are complying with their interpretation of the requirement;[198]

- As the first enforcement action under the CCPA, it sends a strong message to companies that the California Attorney General is serious about protecting the privacy of California residents and it will hold companies accountable; and

- It reminds companies that it is important to cooperate and work in good faith with authorities where there is an alleged violation, especially if the company is offered an opportunity to cure the violation.

b. DoorDash

In 2021, the food delivery platform DoorDash, Inc. was subject to an enforcement action by the California Attorney General for the alleged violation of the CCPA.[199] It was alleged that DoorDash sold the personal data of its consumers without providing clear and transparent disclosures about how DoorDash intended to use their personal data. The enforcement action was resolved through settlement where DoorDash agreed to pay $375,000 as well as implement enhanced privacy measures.[200] The DoorDash settlement sends a strong message to companies

---

[196] *Id.*

[197] Press Release, *Attorney General Bonta Announces Settlement with Sephora as Part of its Ongoing Enforcement of California Consumer Privacy Act,* STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, Aug. 24, 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

[198] Note that free online tools exist that allow governmental authorities and other consumers to test whether opt out signals (like global privacy control) are being used, and if so, whether they are working as intended. For example, such testing can be conducted using the developer controls in Chrome, Firefox, and Edge, or using widgets, such as Ghostery, to provide summaries of the third parties to whom data may be transmitted from a website.

[199] Press Release, *Attorney General Bonta Announces Settlement with DoorDash, Investigation Finds Company Violated Multiple Consumer Privacy Laws,* STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, Feb. 21, 2024, (https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-doordash-investigation-finds-company).

[200] *Id.*

about the importance of being fully transparent with consumers around its collection, use and sharing of consumer's personal data.

c. Tilting Point Media

Recently in June 2024, the popular gaming company Tilting Point Media LLC was subject to an enforcement action by the California Attorney General and the Los Angeles City Attorney. It was alleged that Tilting Point Media failed to comply with both the CCPA and the federal Children's Online Protection Act ("COPPA") by collecting and sharing children's data without obtaining the necessary parental consent.[201] The CCPA incorporates the COPPA controls to further safeguard the online privacy of minors under the age of 13 by requiring website and mobile applications and other online services to obtain parental consent before collecting, using, or disclosing their personal data. The Attorney General, City Attorney and Tilting Point agreed to a $500,000 settlement.[202] One main takeaway from this enforcement action is that companies should carefully consider whether their properties (websites, mobile applications and other online services) have the capacity to collect the data of children and if so, what age screening processes are in place to ensure that consumers enter their ages accurately and obtain necessary parental consents.

2. Colorado and Connecticut Enforcement Actions

a. Colorado

Up to this point, the Colorado Attorney General has been silent on whether its office has initiated any investigations under the CPA. Like Connecticut, the Colorado Attorney General's office has focused on educating companies around the importance of complying with the CPA rather than initiating legal action against companies.

This educational versus punitive approach began at the start of 2022, when the Attorney General's office posted a series of topics for informal input on its website and solicited responses in writing and at scheduled events. This helped the office engage in a more focused dialogue, consider diverse perspectives, and address issues related to the CPA.[203] Following enactment of the statute, and as part of its enforcement effort, the Attorney General's office began mailing letters to businesses focused on informing them about the law and their legal obligations.[204] The Attorney General includes examples of these educational notices on its website to provide companies with a flavor for the law and the opportunity to engage with the office should the

---

[201] Press Release, *Attorney General Bonta, L.A. City Attorney Feldstein Soto, Announce $500,000 Settlement with Tilting Point Media for Illegally Collecting and Sharing Children's Data,* STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, June 18, 2024, https://oag.ca.gov/news/press-releases/attorney-general-bonta-la-city-attorney-feldstein-soto-announce-500000.

[202] *Id.*

[203] Colorado Attorney General, *Colorado Privacy Act (CPA)*, https://coag.gov/resources/colorado-privacy-act/ (last visited Aug. 22, 2024).

[204] *Id.*

company have any questions.[205] In addition to the educational letters, the Attorney General issued warning letters to companies it believed was not compliant with the CPA. The intent of these warning letters was to encourage companies to work in good faith with the Colorado office and resolve any alleged violations within the cure period provided (60 days).

b. Connecticut

The Connecticut Attorney General has taken a similar approach as the state of Colorado in terms of encouraging compliance through education and collaboration rather than legal action. That said, the Attorney General's office has initiated some investigations against companies. However, as far as it is known to the authors of this paper, these investigations have ended amicably without the need for enforcement or other legal action. For example, the Attorney General outlines key themes of early enforcement efforts with respect to privacy notices, matters concerning the collection of sensitive data, and heightened protection for teens' data.[206] This demonstrates Colorado's commitment to giving companies the opportunity to learn and achieve compliance through good faith efforts and collaboration.

3. GDPR and UK GDPR Enforcement Actions

In contrast to the Modern U.S. Privacy Laws, there have been a significant number of enforcement actions under the GDPR. The CMS.law GDPR Enforcement Tracker is an overview of the fines and penalties which data protection authorities within Europe have imposed under the GDPR.[207] This tracker does not list any fines imposed under national or non-European laws (with the exception of fines under the UK GDPR), under non-data protection laws (such as competition laws or electronic communication laws) and under any pre-GDPR-laws, though a limited number of fines under the 2002 ePrivacy Directive[208] are included.[209]

As of the date of this paper, there are 2,343 entries noted within this tracker, with the highest total sum of fines imposed because of non-compliance with "general data processing principles" amounting to €2,082,306,939 (noting a total of 584 fines by company).[210] One example of a "general data processing principle," which is the subject of such fines, is "data minimization," which means that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[211] The franchise business should find ways

[205] *Id.*

[206] Press Release, Report to the General Assembly's General Law Committee at 6 (Feb. 1, 2024) https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf.

[207] CMS.Law GDPR Enforcement Tracker, https://www.enforcementtracker.com/ (last visited July 2, 2024).

[208] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[209] CMS.Law GDPR Enforcement Tracker, https://www.enforcementtracker.com/ (last visited July 2, 2024).

[210] CMS.Law GDPR Enforcement Tracker, https://www.enforcementtracker.com/?insights (last visited July 2, 2024).

[211] GDPR, Article 5(1)(c).

to collect the least amount of personal data necessary to achieve the desired result while leveraging opportunities to deidentify or anonymize the data. One example of applying "data minimization" in the context of a franchisor's email marketing campaigns is to limit the data requested of the consumer to the consumer's first name and first initial of the last name (rather than the full last name) together with email address. In this way, the franchise business is demonstrating its commitment to data minimization since the franchisor may not need the consumer's full last name to run a successful email marketing campaign.

As highlighted in this section, GDPR fines can be substantial, reaching hundreds of millions in euros. The number of fines has been increasing since 2019, and in 2023, the first billion-euro fine was issued.[212] As of May 2024, authorities have issued over 2,000 violations, resulting in more than €4.5 billion in fines.[213]

VIII. CONCLUSION

Modern Privacy Laws recognize the right to protect individual's personal data, which includes the right to control how personal data is used and disclosed. Collecting and disclosing personal data may expose the franchise system to significant risks if not done properly and in compliance with Modern Privacy Laws and other applicable laws. This paper has provided foundational concepts related to data privacy to help franchisors and/or franchisees consider how best to allocate responsibility and associated risks when using personal data. Franchisors and franchisees should invest time and resources in this area of the law to mitigate any potential risk to the franchise system.

[212] CMS.Law GDPR Enforcement Tracker, https://www.enforcementtracker.com/?insights (last visited Aug. 23, 2024).

[213] *Id.*

Biographies

Beata Krakus is a partner of UB Greensfelder LLP, and a co-chair of the firm's Franchising & Distribution Practice Group. She works with franchisor clients in domestic and international franchise transactional matters, as well as related areas such as distribution and sales representative arrangements, and other commercial contracts. She has advised, structured, and prepared franchise programs for many different franchise concepts including real estate brokerages, hotels, restaurants, fitness, and health care-related systems. Prior to joining UB Greensfelder, Ms. Krakus was an associate with Sonnenschein Nath & Rosenthal LLP. She also practiced in Warsaw, Poland with the Swedish law firm of Magnusson Wahlin. Ms. Krakus is a former member of the Governing Committee of the ABA Forum on Franchising and has served in many different officer roles for the organization. She has served as an Associate Editor for The Franchise Lawyer, has herself written articles for the Franchise Law Journal and other franchise law publications, and has spoken repeatedly at the ABA Forum on Franchising annual conference, the International Franchise Association Legal Symposium, and at the International Bar Association annual conference. She is recognized by International's Who's Who of Franchise Lawyers and by Chambers USA.

Tony Marks is a seasoned attorney with extensive experience across a wide spectrum of transactional matters. Tony assists clients in structuring both domestic and international franchise and licensing programs, navigating the complexities of franchise registration and disclosure requirements, and managing the termination and renewal of franchise relationships. His expertise also extends to negotiating intricate multi-unit transactions and transfers. Tony also provides critical assessments regarding the applicability of federal and state franchise and business opportunity laws, ensuring his clients' compliance and strategic advantage in the market. Tony's experience also includes extensive work in venture capital, private equity and mergers, and acquisitions transactions. Tony is certified by the State Bar of California as a Franchise and Distribution Law Specialist and was a co-chair of the California Bar Association Franchise Law Committee.

John Pratt obtained his law degree from Oxford University and successfully completed a doctorate course in comparative law at the Université d'Aix-Marseille. Before starting Hamilton Pratt, John Pratt was managing partner at Pinsent Masons, one of the largest law firms in the UK. Hamilton Pratt represents nearly 40% of the full members of the British Franchise Association. Hamilton Pratt has ten lawyers exclusively advising on the legal aspects of franchising. John Pratt has been the Legal Advisor to the British Franchise Association, chair of the International Bar Association's International Franchising Committee, chair of the American Bar Association's International Franchising Division and chair of Euro Franchise Lawyers – the grouping of Europe's leading franchise lawyers. Who's Who Legal has listed John as Europe's leading franchise lawyer. At the American Bar Association's Franchise Forum in October 2018, he was awarded the John Baer Award for International Civility and Professionalism. In February 2022. Hamilton Pratt was awarded, at the International Franchise Association annual conference in San Diego, the "best franchise law firm" global award. John is the author of the UK's textbook on franchise law – Franchising: Law & Practice as well as other publications and lectures on international franchising throughout the world. John is a past President of Birmingham Chamber of Commerce, senior independent director at the NEC Exhibition Company and Chairman of a group of franchise businesses which includes well-known brands Kall Kwik, Recognition Express, ComputerXplorers and Tech Clean.

Jacqueline Romano is privacy counsel of Purpose Brands LLC, which is the parent company to Anytime Fitness, Basecamp Fitness, Healthy Contributions, Orange Theory Fitness, Stronger U Nutrition, The Bar Method, and Waxing the City. She provides guidance to the company and its brands on data privacy matters, which impact the business domestically and internationally. Ms. Romano joined Self Esteem Brands in 2019 and has been practicing privacy law since 2016 when she obtained her CIPP/US certification and in 2022 earned her CIPP/E certification. In addition to privacy, she provides direction to the company and its brands on other compliance matters, such as consumer protection and accessibility, and provides counsel during commercial contract negotiations. Ms. Romano received a J.D. from William Mitchell College of Law and a B.A. from the University of British Columbia.

David Zetoony is a Shareholder of Greenberg Traurig LLP, and a co-chair of the firm's United States Data Privacy and Cybersecurity Practice. He focuses on helping businesses navigate data privacy and cyber security laws from a practical standpoint. David has helped hundreds of companies establish and maintain ongoing privacy and security programs and has defended corporate privacy and security practices in investigations initiated by the Federal Trade Commission, and other data privacy and security regulatory agencies around the world, as well as in class action litigation. David receives regular recognition from clients and peers for his knowledge and experience in the fields of data privacy and security. The National Law Journal named him a “Cybersecurity and Data Privacy Trailblazer,” JD Supra recognized him four times as one of the most widely read names when it comes to data privacy, cyber security, or the collection and use of data, and Lexology identified him fourteen times as the top “legal influencer” in the area of technology, media, and telecommunications in the United States, the European Union, and in the context of cross-border transfers of information. He is the author of the American Bar Association's primary publication on the European General Data Protection Regulation (GDPR) and the American Bar Association's Desk Reference Companion to the California Privacy Rights Act (CPRA).

Appendix A: References to Modern U.S. State Privacy Laws

U.S. State	Reference
California	CAL. CIV. CODE § 1798.100, *et seq*. that were adopted on June 28, 2018, and that was amended by the California Consumer Privacy Rights Act of 2020
Colorado	Colorado Privacy Act ("CPA"), COLO. REV. STAT. ANN. §§ 6-1-1301 to 6-1-1313
Connecticut	Connecticut Data Privacy Act ("CTDPA"), CONN. GEN. STAT. ANN. §§ 42-515 to 42-525
Delaware	Delaware Personal Data Privacy Act ("DPDPA"), House Bill No. 154
Florida (limited in scope to large technology companies)	Florida Digital Bill of Rights ("FDBR"), Senate Bill 262
Indiana	IND. CODE § 24-15
Iowa	IOWA CODE ANN. §§ 715D.1 to 715D.9, and Iowa Senate File 262
Kentucky	Kentucky House Bill 15 (2024) Kentucky will eventually be codified in K.R.S. 367, but as of the date of this paper, this bill has yet to be codified (the section numbers have not been assigned)
Maryland	Maryland Senate Bill 541 (2024) Maryland will eventually be codified but as of the date of this paper, this bill has yet to be codified (the section numbers have not been assigned)
Minnesota	Minnesota Consumer Data Privacy Act ("MCDPA"), HF 4757/SF 4782
Montana	Montana, S.B. 384
Nebraska	Nebraska, Legislative Bill 1074 (2024)
New Hampshire	New Hampshire, Senate Bill 255-FN
New Jersey	New Jersey, Senate Bill No. 332 (2023)
Oregon	Oregon, Senate Bill 619 (2023)
Tennessee	TENN. CODE ANN. § 47-18-3201-3213
Texas	TEX. H.B.4
Utah	Utah Consumer Privacy Act ("UCPA"), UTAH CODE §§ 13-61-101 to 13-61-404
Virginia	Virginia Consumer Data Protection Act ("VCDPA"), VA. CODE ANN. § 59.1-575
Washington State (although limited to health-related data)	Washington My Health My Data Act ("MHMDA"), H.B. 1155

Appendix B: Types of Personal Data Under CCPA

The following chart includes the types of personal data listed under the CCPA.[214]

Types of Personal Data	
1	Account name
2	Alias
3	Audio information
4	Bank account information
5	Biometric information
6	Browsing history
7	Characteristics of protected classification under California law
8	Characteristics of protected classification under federal law
9	Consumer's interaction with an internet website, application, or advertisement
10	Credit card number
11	Debit card number
12	Driver's license number
13	Education
14	Educational information[215]
15	Electronic information
16	Email address
17	Employment
18	Employment history
19	Geolocation data
20	Health insurance information
21	Insurance policy number
22	Internet or other electronic network activity
23	IP address
24	Medical information
25	Olfactory information
26	Online identifier
27	Other financial information
28	Passport number
29	Physical characteristics or description
30	Postal address
31	Products or services considered
32	Products or services obtained
33	Products or services purchased
34	Professional related information

[214] CAL. CIV. CODE § 1798.140(v)(1) (West 2024).

[215] As defined by 34 C.F.R. § 99.

Types of Personal Data	
35	Profiles of a consumer's abilities
36	Profiles of a consumer's aptitudes
37	Profiles of a consumer's attitudes
38	Profiles of a consumer's behavior
39	Profiles of a consumer's characteristics
40	Profiles of a consumer's intelligence
41	Profiles of a consumer's predispositions
42	Profiles of a consumer's preferences
43	Profiles of a consumer's psychological trends
44	Purchasing or consuming histories
45	Purchasing or consuming tendencies
46	Real name
47	Records of personal property
48	Search history
49	Signature
50	Social security number
51	State identification number
52	Telephone number
53	Thermal information
54	Unique personal identifier
55	Visual information
56	Account log-in in combination with security code or password
57	Precise Geolocation
58	Racial or ethnic origin
59	Religious or philosophical beliefs
60	Union membership
61	Contents of email
62	Contents of mail
63	Contents of text messages
64	Genetic information
65	Biometric information
66	Information concerning sex life
67	Information concerning health
68	Information concerning sexual orientation

Appendix C: Checklist for U.S. Franchisors Entering EEA or UK Markets

Considerations	Actions
Establish what data you process	Undertake an information audit to establish: • What data is collected • Why it is collected • Who has access to it • How and where it is stored • How is the data protected • How long is it kept • How is it deleted
Determine the legal basis for your data processing activities	• Set out your legal basis for processing data[216] • Determine whether additional provisions relating to children and special categories of personal data apply[217] • Document the reason for your chosen legal basis
Appoint appropriate employees to manage data privacy and protection issues	• Designate an employee as privacy/compliance officer • Appoint a representative within the EU • Establish whether you need a Data Protection Officer and appoint one if required
Establish whether third parties (such as email hosting, cloud services, analytics software) process data on your behalf	Create a data processing agreement that clearly sets out how data is to be transferred, stored, protected, used and erased, although many businesses that process data will have their own standard form agreements
Establish what cookies and other tracking technologies you and your franchisees will use on websites	Create a cookie notice or include the applicable information within the privacy notice

[216] *See* GDPR, Article 6.

[217] See GDPR, Articles 7 - 11.

Considerations	Actions
Obtain explicit consent	• Obtain users' explicit consent to your use of tracking technologies and the storing of cookies on their devices • Consent must be explicit, informed, documented, in advance, granular, freely given and easy to withdraw