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

Helen Goff Foster
Davis Wright Tremaine LLP
Washington DC

Dawn Newton
Donahue Fitzgerald LLP
Oakland, CA

John Pratt
Hamilton Pratt
Warwick, UK

October 16 - 18, 2019
Denver, CO

©2019 American Bar Association
TABLE OF CONTENTS

I. INTRODUCTION .................................................................................................................................................. 1

II. GDPR ...................................................................................................................................................................... 1
   A. Introduction .......................................................................................................................................................... 1
   B. Summary of the GDPR ...................................................................................................................................... 2
      1. To Whom Does the GDPR Apply? .................................................................................................................. 2
      2. Is There a Change From Previous Requirements? ......................................................................................... 3
   C. Concepts ............................................................................................................................................................ 3
      1. Data Protection Principles ................................................................................................................................. 3
      2. Lawful Basis for Processing ............................................................................................................................. 4
      3. Why is the Lawful Basis for Processing Important? .......................................................................................... 4
   D. Overview of Lawful Bases for Processing ........................................................................................................... 5
      1. Summary .......................................................................................................................................................... 5
      2. When is Processing “Necessary”? .................................................................................................................... 5
      3. What Happens if a New Purpose is Required? ............................................................................................... 6
      4. Documenting the Lawful Basis ........................................................................................................................ 6
   E. Franchise Relevant Lawful Bases .......................................................................................................................... 6
      1. What Must Individuals Be Told? ....................................................................................................................... 6
      2. Consent ............................................................................................................................................................ 7
      3. Contract ........................................................................................................................................................... 7
      4. Legal Obligation ............................................................................................................................................... 8
      5. Legitimate Interests .......................................................................................................................................... 8
   F. Restricted Transfers – Transfers outside the European Economic Area (“EEA”) ......................................................... 8
      1. Introduction ....................................................................................................................................................... 8
      2. European Data Protection Board .................................................................................................................... 9
      3. What is a Restricted Transfer? ........................................................................................................................ 9
      4. What is the EEA? ............................................................................................................................................ 9
**TABLE OF CONTENTS**

(continued)

<table>
<thead>
<tr>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
</tr>
<tr>
<td>6.</td>
</tr>
<tr>
<td>7.</td>
</tr>
<tr>
<td>8.</td>
</tr>
<tr>
<td>G.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>III.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Collect</td>
<td>27</td>
</tr>
<tr>
<td>4. Sell</td>
<td>27</td>
</tr>
<tr>
<td>F. Key Requirements and Rights</td>
<td>28</td>
</tr>
<tr>
<td>1. Notice aka “Right to Know”</td>
<td>28</td>
</tr>
<tr>
<td>2. Right to Access</td>
<td>29</td>
</tr>
<tr>
<td>3. Right to Know Information that Is Sold or Disclosed</td>
<td>31</td>
</tr>
<tr>
<td>4. Right to Deletion</td>
<td>32</td>
</tr>
<tr>
<td>5. Right to Opt-Out</td>
<td>33</td>
</tr>
<tr>
<td>6. Anti-Discrimination</td>
<td>34</td>
</tr>
<tr>
<td>7. Security</td>
<td>35</td>
</tr>
<tr>
<td>8. Updating Information</td>
<td>37</td>
</tr>
<tr>
<td>G. Impact on Businesses and Compliance Issues</td>
<td>37</td>
</tr>
<tr>
<td>1. Evaluation of Applicability</td>
<td>37</td>
</tr>
<tr>
<td>2. Franchise System Triggers</td>
<td>37</td>
</tr>
<tr>
<td>3. Franchise System Challenges</td>
<td>39</td>
</tr>
<tr>
<td>4. Internal Operations Audit and Assessment</td>
<td>40</td>
</tr>
<tr>
<td>5. Update Public Notices</td>
<td>41</td>
</tr>
<tr>
<td>6. Create Internal Policies</td>
<td>41</td>
</tr>
<tr>
<td>7. Training</td>
<td>41</td>
</tr>
<tr>
<td>8. Modify and Update Vendor Agreements</td>
<td>42</td>
</tr>
<tr>
<td>9. Data Protection or Privacy Officers</td>
<td>42</td>
</tr>
<tr>
<td>H. What Does the Compliance Process Look Like?</td>
<td>42</td>
</tr>
<tr>
<td>1. Key Participants</td>
<td>42</td>
</tr>
<tr>
<td>2. Data Mapping</td>
<td>42</td>
</tr>
<tr>
<td>3. Security Assessments</td>
<td>43</td>
</tr>
<tr>
<td>4. Documenting Compliance and Reasonableness</td>
<td>43</td>
</tr>
<tr>
<td>IV. A NOTE ON OTHER APPLICABLE LAWS</td>
<td>43</td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Laws and Bills in Other States</td>
<td>43</td>
</tr>
<tr>
<td>1. Nevada</td>
<td>43</td>
</tr>
<tr>
<td>2. Washington State</td>
<td>44</td>
</tr>
<tr>
<td>3. New Jersey</td>
<td>45</td>
</tr>
<tr>
<td>B. Push for Federal Preemption</td>
<td>45</td>
</tr>
<tr>
<td>V. CONCLUSION</td>
<td>46</td>
</tr>
</tbody>
</table>

Biographies
I. INTRODUCTION

While the European Union’s General Data Protection Regulation (“GDPR”) of the European Union (“EU”) was not the first data privacy law, it certainly has had the biggest impact on companies worldwide, with its sweeping scope and the threat of severe penalties for violation. Just one month after many companies were celebrating having managed to get into compliance to the extent possible by the May 25, 2018 start date, the California legislature passed its own substantial data privacy law, which goes into effect beginning January 1, 2020. For businesses that thought the headache was over once they complied with the EU law, or that had no exposure to Europe, a new wave of compliance is on the table. And for companies in compliance with the GDPR, various data protection authorities have begun issuing the first disciplinary actions, which shed new light on what compliance really means.

With so much changing in the world of data privacy law, and the stakes so high for getting compliance right, it is no wonder that many companies feel frustrated by what can seem to be a complex and confusing process. However, compliance does not have to feel like an impossible goal, and some diligence and commitment to the processes, as outlined in this paper, can go a long way toward bringing a franchise system into compliance with both existing and future data laws.

II. GDPR

A. Introduction

“The changes we’ve managed to bring have created a better and more connected world. But for all the good we’ve achieved, the web has evolved into an engine of inequity and division; swayed by powerful forces who use it for their own agendas.” Sir Tim Berners-Lee, Creator of the World Wide Web

“My position is not that there should be no regulation. I think the real question as the internet becomes more important in people’s lives is “What is the right regulation?” Mark Zuckerberg, Chief Executive Officer and founder of Facebook

The “digital world” – an environment composed of digital services facilitated by the internet – plays an ever-increasing role in all aspects of life.

Regulation has been slow to catch up with digital developments. One aspect of such regulation is the protection of personal data. Within the EU, this has been a major focus of attention for some time, although recently the publication of its GDPR has resulted in an increased focus on data protection issues. It is likely that focus will increase, and a significant number of other countries have already legislated in this area or will do so in the relative short term.

---

1 The authors thank Donahue Fitzgerald associate Shruti Bhutani Arora for her contributions to this paper.


4 gdpr-info.eu contains the official PDF of the Regulation.
Data protection should be seen in the context of a general wish to increase the regulation of the digital world. For instance, the recently published UK House of Lords Select Committee on Communications report whose working party was led by Jason Furman, an advisor to former President Obama, set out ten recommendations to guide online regulation:

- Parity: the same level of protection must be provided online as offline;
- Accountability: processes must be in place to ensure individuals and organizations are held to account for their actions and policies;
- Transparency: powerful businesses and organisations operating in the digital world must be open to scrutiny;
- Openness: the internet must remain open to innovation and competition;
- Privacy: to protect the privacy of individuals;
- Ethical design: services must act in the interests of users and society;
- Recognition of childhood: to protect the most vulnerable users of the internet;
- Respect for human rights and equality to safeguard the freedoms of expression and information online;
- Education and awareness-raising: to enable people to navigate the digital world safely;
- Democratic accountability, proportionality and evidence-based approach.

B. Summary of the GDPR

1. To Whom Does the GDPR Apply?

Generally speaking, EU legislation takes one of two forms – either a regulation or a directive. While directives have to be implemented by each EU member state to take on the power of law in that member state, regulations, such as the GDPR, have binding legal effect in all of the EU member states without country-by-country adoption. The GDPR, being a regulation, is directly applicable in all of the EU as of 25 May 2018, although EU countries have passed their own legislation to give effect to the requirements of the GDPR.

The GDPR applies to “controllers” and “processors”. A controller determines the purpose and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. 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 – the GDPR places further obligations on controllers to ensure that their contracts with processors comply with the GDPR. The GDPR applies to processing carried out by organizations operating within the

---

5 "Regulation in a digital world" Dated 9 March 2019 (HL Paper 299).

6 GDPR Article 4(7).

7 GDPR Article 4(8).

8 GDPR Article 4(1).
the “EU and the European Free Trade Agreement (“EFTA”) countries”. It also applies to organizations outside the EU that offer goods or services to individuals in the EU.

a. **What is Personal Data?**

The GDPR applies to “personal data” meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. A wide range of personal identifiers will constitute personal data, including name, identification number, location, data or online identifier, reflecting changes in technology and the way organizations collect information about people.

The GDPR applies to both the automated processing of personal data and to manual filing systems where personal data is accessible according to specific criteria including chronologically ordered sets of manual records containing personal data.

The GDPR refers, in Article 9, to sensitive personal data as “special categories of personal data”. The special categories specifically include genetic data, and biometric data where processed uniquely to identify an individual. Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to their processing.

2. **Is There a Change From Previous Requirements?**

One of the key principles of the GDPR is that controllers and processors may only process personal data for lawful purposes, or in the words of the GDPR, if the processors and controllers have a lawful basis for processing the data. The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the “conditions for processing”. However, the GDPR places more emphasis on being accountable for, and transparent about the lawful basis for processing. The six lawful bases for processing, discussed below, are broadly similar to the old conditions for processing although there are some differences. There will be a breach of the GDPR if the controller/processor did not identify the proper lawful basis prior to processing.

The GDPR also brings in new accountability and transparency requirements and as a result it is important to record the lawful basis so that it is possible to demonstrate compliance with Articles 5(2), which is referred to at the end of the following Section C.1. People must be informed upfront about the lawful basis for processing of their personal data.

C. **Concepts**

1. **Data Protection Principles**

Under the GDPR, the data protection principles set out the main responsibilities for organizations. Article 5 of the GDPR requires that personal data shall be:

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

---

9 Norway, Iceland, Lichtenstein and Switzerland.

10 See Article 10.

11 Article 6.
(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 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 organisational 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 unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5(2) further requires that “the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

2. **Lawful Basis for Processing**

There must be a valid lawful basis in order to process personal data and that needs to be established before processing begins and should be documented. Six lawful bases for processing are set out by the GDPR in Article 6. Most lawful bases require that processing has to be necessary. Privacy notices provided to persons whose personal data is to be processed should include the applicable lawful basis for processing as well as the purposes of the processing.

3. **Why is the Lawful Basis for Processing Important?**

The GDPR contains a number of “principles” – which form the basis of the approach taken by the GDPR. Such principles require that the processing of personal data be undertaken in a lawful, fair and a transparent manner. Processing is only lawful if there is a lawful basis under Article 6 and, to comply with the accountability principle in Article 5(2), referred to in Section C. 1. above, it must be demonstrated that a lawful basis applies.

If no lawful basis applies, processing will be unlawful and in breach of the first principle. Individuals also have the right to erase personal data which has been processed unlawfully.

An individual’s right to be informed under Articles 13 and 14 requires individuals to be provided with information about the lawful basis for processing their personal data. The lawful basis for processing can also affect which rights are available to individuals. For example:
The right to erasure does not apply to processing on the basis of a legal obligation or public task – although the latter is unlikely to apply in a franchising context.

The right to portability – which is the right for individuals to obtain and reuse their personal data - only applies to processing on the basis of consent or contract.

The right to object only applies to processing on the basis of legitimate interests or public task.

D. **Overview of Lawful Bases for Processing**

1. **Summary**

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed. They are:

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

   (b) **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.

   (c) **Legal Obligation**: the processing is necessary to comply with the law (not including contractual obligations).

   (d) **Vital Interests**: the processing is necessary to protect an individual’s life.

   (e) **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.

   (f) **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.

In practice, in a franchising context, (a), (b), (c) and (f) are the relevant lawful bases.

2. **When is Processing “Necessary”?**

Other than if the individual has given his or her consent, the lawful bases for processing depend on the processing being “necessary”. This does not mean that processing always has to 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. In other words, if a business decides to obtain information about customer preferences to enable it to send marketing emails containing information about goods or services that match those preferences, but those preferences are not relevant to the goods or services actually ordered by that customer, the processing of such preferences may not be necessary.
3. **What Happens if a New Purpose is Required?**

Unless processing is based on consent, if the purpose for processing changes over time or a new purpose is added, a new lawful basis may not be required as long as the new purpose is compatible with the original purpose. If processing is based on consent, either a new consent must be obtained which specifically covers the new purpose, or a different basis for the new purpose has to be found. In other cases, in order to assess whether the new purpose is compatible with the original purpose the following should be taken into account:

- any link between the initial purpose and the new purpose;
- the context in which the data is collected – in particular, the relationship with the individual and what they would reasonably expect;
- the nature of the personal data – is it, for instance, special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards – e.g., encryption or pseudonymisation.

4. **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 with the GDPR, and have appropriate policies and processes. This means that they need to be able to show that they have properly considered which lawful basis applies to each processing purpose and can justify their decision.

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.

E. **Franchise Relevant Lawful Bases**

1. **What Must Individuals Be Told?**

The GDPR requires organizations to give individuals certain information about how their personal information will be collected and used. This is usually done by way of a privacy notice. Information about the applicable lawful basis must be included in the privacy notice provided to individuals. Under the transparency provisions of the GDPR, the information that needs to be given includes:

- the intended purposes for processing the personal data; and
- which lawful basis for the processing applies.

---

12 GDPR Article 12.
2. **Consent**

Many businesses wrongly believe that the "obvious" lawful basis is consent, but the GDPR sets a high standard for consent.\(^\text{13}\) In order to use consent as a lawful basis it will be necessary to demonstrate that the following has occurred:

- consent is the most appropriate lawful basis for processing;
- the request for consent is prominent and separate from any terms and conditions;
- individuals must positively opt in;
- pre-ticked boxes or any other type of default consent is not used;
- clear, plain language that is easily understood is used;
- the data and what is going to be done with it should be specified;
- individuals should be offered options to consent separately to different purposes and types of processing;
- the business organization and any third party controllers who will be relying on the consent;
- individuals should be told that they can withdraw their consent;
- individuals must be able to refuse consent without detriment;
- consent should not be a precondition of the provision of a service;
- 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.

If a franchisee intends to process personal data to enable the franchisee, or indeed, the franchisor, to send out marketing materials to a customer or prospective customer, this may be an appropriate area to obtain consent.

3. **Contract**

This lawful basis applies to processing personal data:

- to fulfil a contractual obligations to that person;
- because an individual has asked for something to be done before entering into a contract.

The processing must be necessary. If what is being asked for could be done without processing personal data, this basis will not apply. The decision to rely on this lawful basis should be documented. Accordingly, an enquiry of a hotel website about a possible booking would require the proposed dates of the stay to be provided, but the provision of those dates

\(^{13}\) GDPR Article 7.
would not be “necessary” if the enquiry was simply about the facilities at the hotel. Franchisees will need information about their customers in order to deliver goods or services to customers in accordance with the contract entered into by a franchisee and the customer. Franchises also need information to invoice customers for those goods or services. In this case, the contract lawful basis would apply.

4. **Legal Obligation**

This lawful basis can be used if personal data has to be processed to comply with a common law or statutory obligation, 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. For example, if a franchisor franchises liquor stores that undertake internet sales, obtaining information about the age of the person ordering the alcohol is legally required and therefore would fall within this lawful basis.

5. **Legitimate Interests**

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 interests basis. It is necessary to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- it has to be balanced against the individual's interests, rights and freedoms.

The relevant legitimate interests can be a controller's own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits so a supplier's need to have a delivery address for goods ordered online would clearly fall within this lawful basis. The processing must also be necessary. If the same result can reasonably be achieved in another less intrusive way, legitimate interests will not apply. Finally, 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. It would, for instance, be in the franchisee’s or a franchisor’s legitimate interests to enquire of a customer how well a franchisee has performed.

F. **Restricted Transfers – Transfers outside the European Economic Area (“EEA”)**

1. **Introduction**

Although the GDPR primarily applies to controllers and processors located in the EEA individuals risk losing the protection of the GDPR if their personal data is transferred outside the EEA and as a result, the GDPR restricts transfers of personal data outside the EEA – which is referred to as a restricted transfer – 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.
2. **European Data Protection Board**

The European Data Protection Board (“EDPB”), which has replaced the Article 29 Working Party, includes representatives from the data protection authorities of each EU member state and each EEA state. It adopts guidelines for complying with the requirements of the GDPR. The EDPB is currently working on its guidance in relation to restricted transfers, but no date for completion of this work has been provided.

3. **What is a Restricted Transfer?**

A restricted transfer is made if:

- the GDPR applies to the processing of the personal data being transferred. The scope of the GDPR is set out in Article 2 (what is processing of personal data) and Article 3 (where the GDPR applies). In general, the GDPR applies if there is processing of personal data in the EEA, and may apply, in specific circumstances, if processing takes place outside the EEA but relates to personal data about individuals in the EEA;
- personal data, is accessible, to a receiver to which the GDPR does not apply, usually because it is located in a country outside the EEA; and
- the receiver is a separate entity. This includes transfers to another company within the same corporate group. If personal data is sent to an employee, this is not a restricted transfer. The transfer restrictions only apply if personal data is sent to another external organisation.

4. **What is the EEA?**

The EEA countries consist of the EU member states and the EFTA States. The EU member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and, currently, the United Kingdom. The EFTA States are Iceland, Liechtenstein, Norway and Switzerland.\(^{14}\)

5. **Is a Restricted Transfer Necessary?**

A recurring theme in the GDPR is “necessity.” This theme applies to restricted transfers as well, and before making a restricted transfer it is necessary to consider whether the aim of the transfer can be achieved without actually sending personal data outside the EEA\(^{15}\).

One way of avoiding the restrictions on transfers outside the EEA is to make the data anonymous. If data is made anonymous so that it is impossible to identify individuals (even when combined with other information which is available to a receiver), it is not personal data and therefore can be transferred outside the EEA.

\(^{14}\) Although Switzerland has signed the EEA Agreement, it has not ratified it.

\(^{15}\) Please see paragraph F4 above.
6. **How is Transfer Made in Accordance With the GDPR?**

The first issue to address is whether the proposed restricted transfer is covered by an “adequacy decision”. An EU Commission “adequacy decision” is a finding by the Commission that the legal framework in place in the receiving country, territory, sector or international organisation provides “adequate” protection for individuals’ rights and freedoms for their personal data.

Adequacy decisions made prior to the GDPR coming into effect remain in force unless there is a further Commission decision which decides otherwise. The Commission plans to review these decisions at least once every four years. As at July 2019 the Commission has made a full finding of adequacy about the following countries and territories: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay.

The Commission has also made partial findings of adequacy about Canada and the US. The adequacy finding for Canada only covers data that is subject to Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. The adequacy finding for the US is only for personal data transfers covered by the EU-US Privacy Shield framework. If the Privacy Shield is used, US companies must first sign up to the framework with the U.S. Department of Commerce. The obligations applying to companies under the Privacy Shield framework are contained in the “Privacy Principles”. The Department of Commerce is responsible for managing and administering the Privacy Shield and ensuring that companies comply with their commitment. In order to be able to be certified, companies must have a Privacy Policy in line with Privacy Principles. They must renew their “membership” of the Privacy Shield annually, failing which they are no longer entitled to receive and use personal data from the EU under the Privacy Shield framework.

The Department of Commerce has a Privacy Shield list on its website ([https://www.privacyshield.gov/welcome](https://www.privacyshield.gov/welcome)) which lists those companies which are part of the Privacy Shield and the kind of personal data they use and the services they offer.

The Privacy Shield places requirements on US companies certified by the scheme to protect personal data and provides for redress mechanisms for individuals. US Government departments such as the Department of Commerce oversee certification under the scheme.

If personal data is to be transferred to a US organisation under the Privacy Shield, it is necessary to check on the Privacy Shield list to see:

- Whether the receiving organisation has a current certification; and
- Whether the certification covers the type of data to be transferred.

7. **Is the Restricted Transfer Covered by Appropriate Safeguards?**

If there is no “adequacy decision” about the country, territory or sector in respect of a proposed restricted transfer, the transfer may be able to be made subject to “appropriate safeguards”, which are listed in the GDPR aimed at ensuring that the sender and the

---

16 An up to date list of the countries which have an adequacy finding can be found on the European Commission’s data protection website.


18 GDPR Article 46 and Recitals 108-108 and 114.
receiver of personal data are legally required to protect individuals’ rights and freedoms for their personal data.

The relevant safeguards are set out below:

a. **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 (“BCRs”).

BCRs are an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group’s EEA entities to non-EEA 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 an EEA supervisory authority in an EEA country where one of the companies is based. Usually this is where the relevant EEA head office is located.¹⁹

b. **Use of Standard Data Protection Clauses Adopted by the Commission**

A restricted transfer can be made if the data exporter and the data importer have entered into a contract incorporating one of the four sets of standard data protection clauses adopted by the Commission²⁰ — known as the “standard contractual clauses” (or “model clauses”).

The standard contractual clauses 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 Commission plans to update the existing standard contractual clauses for the GDPR but it is not currently known when that will be.

Existing contracts incorporating standard contractual clauses can continue to be used for restricted transfers (even once the Commission has adopted the GDPR standard contractual clauses).

The standard contractual clauses must be used in their entirety and without amendment. Additional clauses can be included on business related issues, provided that they do not contradict the standard contractual clauses. Additional data importers or exporters can be added provided they are also bound by the standard contractual clauses.

---

¹⁹ The criteria for choosing the lead authority for BCRs is laid down in the “Working Document Setting Forth a Cooperation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR”. 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 organisations. The documents, including application forms and guidance have all been revised and updated in line with GDPR. They include: Table of elements and principles for controller BCRs (WP256), Table of elements and principles for processor BCRs (WP257), Cooperation procedure for the approval of “Binding Corporate Rules” (WP263.01), Application form BCR-C (WP264), and Application form BCR-P (WP265). See also GDPR Articles 46-47 and Recitals 108-110.

²⁰ Articles 46.(2)(d) and 93(2). To access the standard contractual clauses please see the ICO’s “Standard Contractual Clauses for Controllers to Processors” - [https://ico.org.uk/media/.../ico-guidance-controller-to-processor.docx](https://ico.org.uk/media/.../ico-guidance-controller-to-processor.docx)
c. Use of Standard Data Protection Clauses Adopted by a Supervisory Authority and Approved by the Commission.

A restricted transfer can, for instance, be made from the UK if a contract incorporating standard data protection clauses adopted by the Information Commissioner’s Office ("ICO") are used. However, for the time being neither the ICO nor any other EEA supervisory authority has adopted any standard data protection clauses.

d. Use of an Approved Code of Conduct Together With Binding and Enforceable Commitments of the Receiver Outside the EEA

If the data importer has signed up to a code of conduct, which has been approved by a supervisory authority a restricted transfer can be made. The code of conduct must include appropriate safeguards to protect the rights of individuals whose personal data transferred, and which can be directly enforced.

The GDPR endorses the use of approved codes of conduct to demonstrate compliance with its requirements, but so far no approved codes of conduct are in use.

e. Certification Under an Approved Certification Mechanism Together with Binding and Enforceable Commitments of the Receiver Outside the EEA

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.21

f. Use of 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 authorised by the supervisory authority of the country from which the personal data is being exported although currently such bespoke contracts are not being authorized, until guidance has been produced by the EDPB.

8. If a Restricted Transfer is not Covered by an Appropriate Safeguard22

If a restricted transfer is not covered by an appropriate safeguard, then it is necessary to check whether an exception applies.23 There are various exceptions discussed below.

---

21 Currently supervisory authorities are planning to produce their accreditation guidelines and requirements by the end of 2019.

22 See GDPR Article 49 and Recitals 111-112.

23 GDPR Article 49.
a. **The Individual’s Explicit Consent to the Restricted Transfer**

The individual’s consent to the restricted transfer is an exception from the general rule. Because a valid consent must be both specific and informed, the individual must be provided with precise details about the restricted transfer. A valid consent cannot be obtained for restricted transfers in general.

The individual should be told:

- The identity of the receiver, or the categories of receiver;
- 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.

Given the high threshold for a valid consent, and that the consent must be capable of being withdrawn, this may mean that using consent is not a realistic solution for franchisors who wish to transfer personal data out of the EU.

b. **The Restricted Transfer Is Necessary to Take Steps Requested by the Individual in Order to Perform or to Enter Into A Contract**

Another exception applies to the situation where a restricted transfer is necessary to take steps that have been requested by an individual to enter into or perform a contract with the individual. 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 in order to enter into a contract would, for instance, arise if an individual wishes to reserve 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.

---

24 See footnote 21 or is it ibid.

25 Please see the earlier section on consent as to what is required for a valid explicit consent under the GDPR.

26 See footnote 24.

27 This would arise, for example, if an EU travel company was asked by a customer to book/reserve a hotel room in, say, South Africa.
c. **Is a Contract With an Individual Entered Into or Contemplated Which 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.28

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

An exception applies where the public interest warrants the restricted transfer. There must be an EU or 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 EU member state or EU 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, would be a sufficient basis. In practice, this is unlikely to apply in a franchising context.

e. **A Restricted Transfer Needs to be Made to Establish if a Legal Claim is Available, to Make a Legal Claim or to Defend a Legal Claim.**

If a restricted transfer is required to determine the existence of a legal claim, to make a legal claim or to defend against a legal claim, the restricted transfer is also excepted from the regular restrictions. This exception explicitly states that it can only be used for occasional transfers. 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 relevant legal claim must have a basis in law, and a “formal legally defined process”, but what constitutes such a process 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.
- Administrative or regulatory procedures, such as the defence of an investigation (or potential investigation) in antitrust law or financial services regulation, or to seek approval for a merger.

The exception cannot be used if there is only the possibility that a legal claim or other formal proceedings may be brought in the future. Accordingly if a franchisor is in a dispute with a franchisee but there is, for instance, a 30 day cure period which has not elapsed, and the franchisor does not have evidence that the franchisee does not wish to cure, it is unlikely that, at that stage, a restricted transfer can be made.

---

28 An example of this exception would be as set out in the previous footnote but the customer would be enquiring for himself and, say, his family members and/or friends.
f. **A Restricted Transfer Has to be Made to Protect the Vital Interests of an Individual.**

If a restricted transfer is necessary to protect the vital interest of an individual who is legally or physically unable to provide consent it is exempt. This exception applies in a medical emergency where the transfer is needed in order to give the medical care required and therefore is unlikely to apply in a franchising context.

g. **A Restricted Transfer Is Made to a Public Register.**

Where the transfer is to a public register, the restricted transfer is also exempt. The register must be created under the law of an EU member state or EU law and must be open to either to the public in general, or to any person who can demonstrate a legitimate interest. For example, registers of companies, associations, criminal convictions, land registers or public vehicle registers. Again, this exemption is unlikely to apply in a franchising context.

h. **A One-Off Restricted Transfer Is Made for Compelling Legitimate Interests.**

If none of the exceptions set out above apply, this final exception may be considered. The exemption for one-off transfers for which there is a compelling legitimate interest should not be relied on routinely because it is only for truly exceptional circumstances. It is unlikely to apply in a franchising context.

i. **How Will the Rules Concerning Restricted Transfers Change if the UK Leaves the EU Without Agreement?**

There remains the continued uncertainty about how the UK’s decision to leave the EU will be implemented, and, therefore, how UK companies will be able to make a transfer from the UK to other countries in compliance with the GDPR. Restricted transfers from the UK to other countries, including to the EEA, will be subject to transfer rules to be published by the UK Government. These UK transfer rules will mirror the current GDPR rules.

The UK government has confirmed[29] that, when the UK exits the EU, transfers from the UK to the EEA will not be restricted. There will be transitional provisions for a UK adequacy decision to cover these transfers.

Rules on transfers to countries outside the EEA will remain similar to the current GDPR rules. Although the UK will make its own adequacy decisions after its EU exit, the government has confirmed that it intends to recognize existing EU adequacy decisions and, approved EU BCRs wherever possible. However, the UK government still needs to confirm that position on the recent EU adequacy decision for Japan.

The UK rules will only apply to transfer from the UK to the EEA though. Transfers from the EEA to the UK will need to comply with the GDPR transfer restrictions.

G. **Franchising Issues**

1. **Introduction**

The GDPR applies to franchisors and franchisees in the same way that it applies to other businesses, but there are a number of issues which are of particular importance in a

---

[29] See, for example, Exiting Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019.
franchising context. Perhaps, because of the international nature of franchising, the exporting of personal data (which is addressed in the previous section of this paper) is the most important issue. Nevertheless, there are other issues which are summarized in this subsection.

2. **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. As a result, franchisors will be data controllers in respect of information obtained by their franchisees on their instructions. They will also be data controllers in respect of the personal data that they collect and process – such information could include personal data relating to franchisees or complaints about franchisees that they receive. Similarly, although franchisees may be data processors (but could be data controllers jointly with the franchisor) in respect of the information that their franchisor requires them to collect, they are likely to be data controllers in respect of the information that they collect in respect of their employees, suppliers, and others, which information is being collected for the franchisee’s own commercial reasons and not because the franchisor has required it.

Specifically, in order to determine whether a franchisor or a franchisee is a data controller or a data processor it is necessary to establish who decides:

- 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 to retain the data.

All of the above decisions can only be taken by the data controller. This does not mean that if a franchisee or franchisor is a data processor that entity cannot make any decisions because it could still be a data processor and decide:

- What information technology ("IT") systems or other methods to use to collect personal data;
- How to store the personal data;
- Setting the security requirements; and
- The means to transfer the personal data from you to your client.

To put it in simple terms, if a franchisor or franchisee deals with the “technical” aspects of an operation then it will be a data processor, but if such entity interprets or exercises professional judgment in relation to the personal data it will be a data controller.
Even if the franchise agreement states that a franchisee is a data processor, that does not automatically make it so.

3. **Franchisor Advice to their Franchisees**

Inevitably, franchisees will look to their franchisor for advice and guidance concerning GDPR compliance. Of course, franchisors have a direct interest in ensuring that their franchisees are GDPR compliant, because franchisors may be responsible for any GDPR breaches by their franchisees. This is particularly true if, as is likely to be the case, franchisors are data controllers and franchisees are data processors. Further, of course, a data breach by a franchisee will have a negative impact on the system as a whole. Finally, it is clearly more efficient that franchisees should not individually incur the expenses of obtaining separate, but presumably, identical advice from a large number of GDPR experts.

Nevertheless, there is a significant danger in franchisors being too prescriptive in their instructions and requirements for their franchisees because it may be that when providing any such guidance concerning GDPR compliance, franchisors will owe their franchisees a duty of care or a similar obligation. If any such advice and guidance prove to be inaccurate franchisors could be liable to their franchisees in the tort of negligence in common law jurisdictions or the civil law equivalent. As can be seen from this paper, compliance with the GDPR is not only complex but also subject to some uncertainty in relation to its interpretation. Some franchisors have sought to address the risk of incurring liability for GDPR advice they provide by instructing or recommending a third party GDPR 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 recommendation.

In the UK, generally franchisors have adopted a “half way” approach with their franchisees by giving only very general advice setting out, in general terms, a GDPR compliance action plan containing the steps that franchisees must take. This may include the following:

a. **Being More Transparent with Individuals – Customers, Prospects and Employees**

The GDPR requires data controllers to give individuals more information at the time their data is collected – this includes explaining the legal basis for processing, data retention periods and that individuals have a right to complain to the Information Commissioner’s Office (“ICO”). Generally, franchisors will be data controllers in respect of the personal data that they and their franchisees are required to collect but franchisees could also be joint controllers and/or controllers of information that they obtain otherwise than as a requirement of their franchise contractual arrangements. Below various actions are taken that franchisors and franchise systems should consider taking, if any data collected by the franchisor or franchisees fall within the scope of the GDPR. The division of responsibility will differ among franchise systems depending on many different factors such as who collect and maintains the data and who has access to the data. Though the authors have envisioned that much of this responsibility will fall on franchisors, this may not always be the case.

(i) **Actions to Take Now**

Franchisors should take the following actions to ensure that they meet the GDPR transparency standards:

- Review their and their franchisees’ customer-facing terms and their privacy policies.
• If they or their franchisees are relying on customer consent to legitimize their processing (for example, for email marketing), they should check that the method of obtaining consent will meet the new rules. Consent requires a positive opt-in.

• If consent cannot be relied on, they should establish whether one of the alternative conditions for processing can be relied on.

• If a franchisor or franchisee employs people, they will not be able to rely on employee consent to process their data, so they will need to determine on what other legal basis they will process employee data going forward.

• Franchisor and franchisee employees will require privacy notices.

b. Demonstrating Compliance

An overarching requirement of the GDPR is the principle of “accountability”. There are new requirements (which are more limited for businesses with fewer than 250 employees) – which in practice will cover the great majority of franchisee businesses - on data controllers (and data processors) to demonstrate their compliance by fully documenting all their data-processing activities. 30

(i) Actions to Take Now

• Consider what records are kept of decision making concerning the GDPR and processing activities. Franchisors and franchisees must, for example, demonstrate their compliance by pointing to staff training, internal audits of processing and reviews of internal policies.

• Review contracts with processors to ensure that they meet the requirements of the GDPR and that franchisors and franchisees are suitably protected if there is a breach.

c. Mandatory Breach Notifications

Controllers – which, for the most part means franchisors - 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. In other words, contractual terms must be inserted requiring franchisees to notify franchisors of a data protection breach.

(i) Actions to Take Now

• Review internal systems to ensure that the new breach notification requirements can be met.

• Review processor contracts to ensure they contain obligations to report breaches to the franchisor.

• Invest in and use secure systems including the use of passwords and encryption, firewalls and current anti-virus software in relation to personal data collected and/or processed by the franchisor and its franchisees or require franchisees to do the same.

30 Articles 5(2), 24(2) and Recitals 39, 74 and 78.
• Address the “human element” through training and procedures designed to minimise the risks of hacking, phishing and other cyber security breaches.

  d. **Much Higher Penalties When Things Go Wrong**

  Businesses may face much higher penalties for non-compliance.

  (i) **Actions to Take Now**

  • Ensure that the risk of penalties for non-compliance with the GDPR are fully understood at senior management and board level and that suitable indemnities are provided by franchisees to their franchisor because, as already indicated, franchisors are likely to be controllers for the great majority of franchisee data processing.

  • Review processor contracts to ensure that liability is adequately flowed down.

  e. **Enhanced Rights for Individuals**

  The GDPR includes 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.

  Individuals 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 organisation has legal requirements to retain data or if an employer needs to hold on to data and has lawful grounds for doing so.

  (i) **Actions to Take Now**

  • Review the process (for both franchisors and franchisees) for responding to subject access requests under the GDPR where a person is entitled to request details of the personal information held about them and how it is being processed.

  • Ensure this can be supplied by both franchisor and its franchisees without delay, free of charge and in any event within one month.

  • Consider whether to change communications with individuals by a franchisor and its franchisees to ensure they are aware of their new rights.

  • Continue to ensure that franchisor and franchisees keep personal data accurate and where necessary is updated and not held for longer than necessary.

  f. **Direct Obligations on Processors**

  Previously controllers were solely responsible to data subjects and the ICO for compliance. The GDPR now imposes direct obligations on processors, including taking security measures to protect personal data and maintain records of all processing activities. Franchisors must ensure that their franchisees are aware of such change.

  Processors must not be able to subcontract processing without the controller’s prior consent. Contractual provisions must be imposed on franchisees to ensure compliance with this obligation.
(i) **Actions to Take Now**

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

**g. Privacy Policy**

The provisions of privacy policies used by a franchisor and its franchisees will need to be reviewed and possibly changed.

**h. Appointment of a Data Protection Office (“DPO”)**

A Franchisor and its franchisee will have to independently evaluate if they need to appoint a DPO. A franchisor or a franchisee must appoint a DPO if local laws require the same, or if the core activity of the franchisor or franchisee involves large scale regular and systematic monitoring of data subjects, or large scale processing of special categories of data or personal data related to criminal convictions and offences. A DPO should have expert knowledge of data protection laws and practices. A DPO must at least perform the following tasks: (a) inform and advise the applicable controller or processor and any employee who processes personal data about their obligations under the GDPR; (b) monitor compliance of the organization with the GDPR; (c) provide advice, when requested, on the Data Protection Impact Assessment (discussed below) and monitor organization’s performance pursuant to Article 35; and (d) cooperate with the data protection authorities and act as a point of contact for the data protection authorities.

**i. Data Protection Impact Assessment**

A Franchisor and its franchisee may have to conduct a data protection impact assessment where personal data may be processed using new technologies, or where processing of personal data could result in a “high degree of risk for data subjects.” The Article 29 Working Party has adopted “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679” (the “Guidelines”) clarifying requirements of the EU GDPR. According to the Guidelines, data protection impact assessment is required if an organization plans to: use new technologies; use profiling or special category data to decide on access to services; profile individuals on a large scale; process biometric data; process genetic data; match data or combine datasets from different sources; collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’); track individuals’ location or behavior; profile children or target marketing or

---

31 GDPR Article 37 and Recital 97.

32 GDPR Articles 37(5) and 37(6) and Recital 97.

33 GDPR Article 39 and Recital 97.

34 GDPR Article 35 and Recitals 90-94.

35 Article 29 Data Protection Working Party “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679” adopted on April 4, 2017 and available at https://iapp.org/media/pdf/resource_center/WP29-GDPR-DPIA-guidance_final.pdf
online services at them; or process data that might endanger the individual's physical health or safety in the event of a security breach.  

4. **Existing Franchisees**

Existing franchisees will have subsisting franchise agreements 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 GDPR 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.

In order to overcome that uncertainty, franchisors sending their new requirements concerning and advice on, the GDPR, have sought a confirmation from the franchisee that it will comply with such requirements. Typically, franchisors ask franchisees to confirm that they have: complied with the principal elements of the Franchisor’s GDPR Action Plan; and that they agree that the revised data protection clause that has been provided will replace the data protection clause in their current franchise agreement.

5. **Information for the British Franchise Association**

Membership of a European franchise association requires that franchisee information be provided as part of the membership requirement. Franchisors wishing to apply for membership should include in their franchise agreements an express provision allowing the franchisor to provide franchisees personal data to the national franchise association.

The British Franchise Association (“bfa”) believes that such contractual consent no longer constitutes valid consent for the purposes of the GDPR, but bfa still requires franchisors to pass contact details of their franchisees to the bfa. The bfa requires its members to choose which other lawful basis they wish to rely upon in order to be able to transfer their franchisees’ contact details to the bfa and the bfa suggests that this could be on the basis of “legitimate interests”.

III. **CALIFORNIA CONSUMER PRIVACY ACT**

A. **History**

When it comes to legislation there is legislative history, and then there is historic legislation. The California Consumer Privacy Act, Cal. Civ. Code §1798.100 – 1798.199 (“CCPA”), is short on the former, but long on the latter. Indeed, the statute passed the California legislature unanimously a mere week after it was introduced. Yet it is arguably the most comprehensive privacy statute ever passed in any country, and certainly the most sweeping in US law.

1. **A Fateful Cocktail Party**

What we now know as the CCPA started life as banter at a cocktail party. Alastair Mactaggart is a semi-retired California real estate developer, with no interest in, or knowledge of, privacy law or even technology. But at a cocktail party he met an engineer from Google and the two reportedly chatted about growing concerns over consumer privacy.

---

36 *Id.*

Mactaggart later summed up the engineer’s side of the story as “if people knew what we [at Google] know about them, they would be freaked out.”

On the basis of that conversation, Mactaggart formed his mission: to impose “transparency” on tech giants. He personally lead and bankrolled a successful effort to obtain the 600,000 signatures required under California law for a ballot initiative, despite arguments from industry that the initiative would place undue burden on California businesses and “cut[] off Californians from convenient services.” And at that point, the California legislature rushed the stage.

2. **One Week to Make History**

With just a week before the June 28, 2018 ballot initiative approval deadline, California Assembly member Ed Chau, and state Senator Robert Hertzberg introduced AB 375 as an alternative to the ballot initiative. Mactaggart agreed to withdraw the ballot initiative if the legislature passed and the governor signed AB 375 before the ballot initiative deadline. Without so much as pausing to verify that the legislation was free from administrative errors—such as language that refers to sections of the law that were removed or moved during the week of negotiations—the CCPA became law at 1:30 P.M. on June 28, 2018.

The wild rush to write and pass significant legislation had a predictable outcome. The statute was riddled with errors, frequently vague, and replete with impacts that the legislature had not anticipated. It was amended to cure some of these issues in 2018, and numerous additional amendments are pending as of the date of this paper.

**B. Implementation**

The CCPA will be implemented in a curious two-phase approach. The law becomes effective on January 1, 2020. Businesses are expected to be in full compliance with the law, by that date. In addition, the private right of action provided by the CCPA’s provisions related to breaches of personal information, is effective on Jan 1, 2020. Many other provisions of the law, however, are subject to regulations to be promulgated well-after January 2020 by the California Attorney General. The CCPA allows the Attorney General until July 1, 2020 to promulgate such regulations. It also prohibits the Attorney General from bringing any enforcement actions before July 2020. This already effective, but not yet enforceable, dichotomy leaves businesses guessing as to how to comply with many aspects of the statute.

**C. Related Laws**

This is not the first time that California has been at the vanguard of data protection laws. California was the first state to adopt a breach notification law in 2000. The

---

38 Id.

39 Id.

40 Id.

41 Statement by Committee to Protect California Jobs (May 20, 2018).

42 California Legislative Information, Bill History, AB 375.

43 Id.

California “Shine the Light” law, Cal. Civ. Code § 1798.83, passed in 2003, was one of the first state laws to address use of consumer information for marketing purposes. The state also boasts one of the earliest financial privacy laws, the California Financial Information Privacy Act, which became law in 2004. And, similar to these earlier California initiatives, the CCPA is the state law that launched a bevy of other state laws, as discussed in Section IV of this article.

D. Applicability

The CCPA applies to any for-profit entity that does business in California and collects consumer personal information, provided the entity meets any one of three thresholds. For an entity to be a “business” subject to the CCPA, it must:

- Have more than $25 million in annual gross revenues (the “revenue threshold”);
- Receive personal information relating to 50,000 or more California residents, devices, or households annually (the “50,000 threshold”); or
- Derive at least half of its gross revenues from the sale of personal information (the “sales threshold”).

1. For Profit Entities

The CCPA applies to any legal entity that is “organized or operated for the profit or financial benefit of its shareholders or other owners.” This means that the CCPA, like many other US privacy standards, exempts non-profits from compliance with the law. Traditionally, non-profits in the US have avoided privacy enforcement actions, due in large measure to the fact that the FTC has no jurisdiction over non-profits. The GDPR, on the other hand, contains no such exemption.

2. The Revenue Threshold

Entities that are doing business in California (e.g., those that are licensed or incorporated in California or are required to pay the California franchise tax), are subject to the CCPA if they have $25 million in annual gross revenues regardless of the source of those revenues. The statute does not restrict this threshold to revenues derived from California sales or California residents.

3. The 50,000 Threshold

Entities that do not meet the Revenue Threshold may be subject to the CCPA nonetheless if they annually buy, receive for business purposes, sell, or disclose personal information of 50,000 or more consumers, households, or devices. Entities are not required to use or share the information for the statute to apply. The mere act of collecting personal information for a business purpose is sufficient. Accordingly, businesses that maintain even

---

46 CCPA § 1798.140(c)(1).
47 In recent years, the FTC has supported legislative efforts to provide the agency with jurisdiction over nonprofits. See e.g., Prepared Statement of the Federal Trade Commission on Legislative Hearing on 17 FTC bills, (May 24, 2016).
48 CCPA § 1798.140(c).
a modest online presence may meet this annual threshold easily. For example, a simple website that collects an Internet Protocol address ("IP address") for website analytics likely would collect information on 50,000 unique devices if the site collects daily unique addresses greater than 135.

CCPA’s broad scope is further exacerbated by the fact that device and household identifiers may or may not represent one-to-one correspondence to an individual. A business may or may not be able to determine that a device identifier is associated with other identifiers it may capture (such as name, address, etc.). The statute forces businesses to assume that each device is a unique individual—resulting in significant, but unavoidable, duplication in determining the amount of personal data collected from unique consumers, devices, or households. Further, as a practical matter, device identifiers do not contain reliable information concerning the residence of the device owner. Although the definition of the term “consumer” is specific to California residents, the terms “households” and “devices” are not. Accordingly, businesses have little choice but to assume that devices could be associated with a California resident when considering whether they have the requisite number of unique interactions to meet the 50,000 threshold.

4. **The Sales Threshold**

An entity that does business in California and that fails to meet the Revenue Threshold and/or the 50,000 threshold may still be subject to the CCPA, if the entity derives 50% or more of its revenue from the sale of personal information.\(^{49}\)

5. **Applicability to Service Providers**

Analysis of the applicability of the CCPA, however, does not stop with the business that collects or receives personal information for its own business use; the CCPA also applies independently to entities that are “service providers” to other businesses subject to the CCPA. Under the statute a service provider is any entity that “processes information on behalf of the business” and is restricted, via written contract, from “retaining, using, or disclosing the information for any purpose” other than the services the entity has agreed to provide to the business.\(^{50}\)

6. **Applicability to Franchise/Brand-Licensing Relationships**

Uniquely among privacy statutes, the CCPA requires all entities that use a common brand or service mark and that control, or are controlled by, a business subject to the CCPA, to comply with the statute as well. The statute defines “control” in terms of ownership, the ability to select directors, or “the power to exercise a controlling influence over the management of a company.” The intent of this provision appears to be to provide a seamless experience for consumers who wish to exercise their CCPA rights and may not understand if it is a franchisor or franchisee that is handling their data. There is no specific guidance, however, on what it means to exercise controlling influence over management in this context. Thus, there is no clear answer as to whether the mere award of a franchise by a California franchisor subject to the CCPA makes a franchisee operating outside of California subject to the CCPA as well.

Another California privacy law, the California Financial Information Privacy Act ("FIPA"),\(^{51}\) defines control as the power to exercise “a controlling influence over the

---

\(^{49}\) CCPA §1798.140(c)(1)(C).

\(^{50}\) CCPA § 1798.140(v).

management or policies of a company.” That same regulation explicitly provides that franchisors are deemed affiliates—i.e., in control—of franchisees. Unlike the FIPA, the CCPA does not refer explicitly to franchise parties. The CCPA explicitly refers to the FIPA—information protected by the FIPA is exempt from the CCPA’s requirements.

If the CCPA is interpreted consistent with the FIPA, then entities that license brands likely would be deemed to control their licensees. Under this construct, a franchisor with no other ties to California would be required to comply with the CCPA solely because one or more of its same-brand franchisees is required to comply. Likewise, franchisees outside of California would be required to comply with the statute if their same-brand franchisor is subject to the statute, regardless of the franchisees’ location or the absence of nexus to California. Such an interpretation would not extend the statute’s requirements from one franchisee to another franchisee of the same brand, however, because neither the FIPA nor the CCPA impute compliance obligations to entities under common control. As such, a franchisee that is required to comply with CCPA does not extend its CCPA compliance obligations to other franchisees of the same brand, since peer organizations do not control, and are not controlled by, each other.

E. Key Definitions

One of the things that makes the CCPA so historic, and so difficult to apply, is the law’s sweeping approach to concepts that previously were defined more narrowly. For example, the information that the CCPA protects—personal information—is defined in the broadest possible terms. Accordingly, if you want to understand the CCPA, the “devil” is in the definitions.

1. Personal Information

The CCPA applies only to businesses that collect “personal information.” Personal information is defined as “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly with a particular consumer or household. Several aspects make this definition of privacy-protected information truly unique. For example, many US laws refer to protected consumer information as “linked, directly or indirectly” to an individual. The addition of “household” information, however, broadens the concept to encompass any information that could reasonably linked to any individual living at a common address. In addition, the phrase “is capable of being associated with” an individual or household—appears to include any information that could in anyway relate to an individual or household—regardless of whether that information could “reasonably” be linked to the individual or the household.

---

52 FIPA § 4052(g).
53 FIPA § 4052 (d)
54 See e.g., GDPR, Art. 4, which defines personal data as “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 . . .”. Similarly, the US Office of Management and Budget (which interprets the federal Privacy Act as it applies to federal agencies) defines personally identifiable information as “information that can be used to distinguish or race an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. OMB Memorandum 10-23. The Federal Trade Commission staff generally refers to personally identifiable information as that which is linked or “reasonably linkable to an individual.” FTC Staff Comment to Federal Communications Commission regarding Notice of Proposed Rule Making On the Privacy of Customers of Broadband and Other Telecommunications Services (May 27, 2016) at 9.
For example, a franchisee that annually receives the personal information of 50,000 or more California residents/employees, households or devices is subject to the CCPA. Most consumer businesses with an online presence will meet this threshold. This is due, in part, to the fact that the CCPA applies to a much broader data set than the GDPR or any US privacy law to date. The CCPA’s definition of “personal information” includes any information that “is capable of being associated with . . . a particular consumer or household.” This definition sweeps in nearly any type of information that might be collected online—including IP addresses and information collected passively through cookies and web beacons. Even information collected by a business solely for internal use is subject to the CCPA—including any data related to a California resident employee. The CCPA’s focus on collection of device identifiers also broadens its reach exponentially. Businesses that use apps or partner with app-based delivery or booking services must consider the information gleaned through those channels as though each device is a unique individual—even though a single individual may possess several devices.

This definition sweeps in nearly any type of information that might be collected online—including IP addresses and information collected passively through cookies and web beacons. Even information collected by a business solely for internal use is subject to the CCPA—including any data related to a California resident employee. Similarly, the statute’s list of personal information categories is expansive, and includes:

- Any unique personal identifier, online identifier, or IP address
- Protected classifications (such as race, gender, ethnicity, religion)
- Purchasing or consuming histories or tendencies
- Biometric information
- Browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement
- Geolocation data
- Audio, electronic, visual, thermal, olfactory, or similar information
- Professional or employment-related information
- Education information
- Inferences drawn to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.\(^{55}\)

2. **Consumer**

The CCPA provides rights and protections to “consumers.” The statute defines this term to include any natural person California resident. This definition has been the cause for consternation because it appears to include individuals who interact with businesses outside

of traditional consumer transactions or contexts, such as a business’ employees, contractors, or professional contacts.56

3. Collect

Only businesses that “collect” personal information are subject to the CCPA, but the statute defines this term broadly. Under the CCPA a business collects personal information when it buys, rents, gathers, obtains, receives, or accesses such information by any means. This definition includes both active collection of information—such as when a consumer enters information directly into an application or website—as well as passive collection, such as monitoring website activity through cookies, or by other observation of the consumer’s behavior.57

4. Sell

CCPA defines “sale” as any exchange of personal information for monetary or “other valuable consideration.”58 Accordingly, the provision of personal information does not need to be the primary objective of the data exchange for it to be a “sale” under the statute. Providing consumer personal information to a non-service provider business partner for joint marketing, marketing analytics, or other cooperative arrangements that provide joint or collective benefits could be a sale even if no money changes hands between the parties.

The statute provides four exceptions to the definition of sale. First, a business does not “sell” personal information when the consumer uses the business’ services or directs the business to interact with a third party intentionally. This exemption is limited to situations in which the business that receives the personal information does not sell the consumer’s personal information.59 Second, businesses may share consumer identifiers with third parties in order to effectuate a consumer’s request to opt-out of the sale of information.60 Third, businesses are permitted to share information with third parties as an asset as part of a merger, acquisition, bankruptcy or similar transaction.61

Finally, and perhaps most significantly, a business does not “sell” personal information when it shares personal information with a service provider—i.e., an entity that processes information on behalf of the business. For an entity to be a service provider under the CCPA, however, the entity must agree in writing that it will not use or disclose the personal information for any purpose other than providing the agreed services to the business.62

56 CCPA §1798.140(g).
F. **Key Requirements and Rights**

The CCPA establishes five specifically enumerated consumer rights. In addition, the statute imposes related requirements which implicate security practices. Businesses subject to CCPA compliance are required to comply with each of these.

1. **Notice aka “Right to Know”**

In part because of how poorly the statute is currently written, as discussed above in Section III(A), the “Right to Know” subsumes two separate business obligations which, in practice, are very different from one another. One of those obligations overlaps with the “Right to Access” which is separately described in Section III(F)(2), below. In this section of the paper, we discuss only the notice obligation, which is described by statute as follows:

A business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.63

Businesses can comply with this requirement in a number of ways. A publicly available privacy notice can outline this information. For companies that collect a variety of different information and use it for different purposes depending on the type of goods or services a consumer requests, it is important that the disclosure is detailed enough to allow consumers to review what will be collected from them and how it will be used in different circumstances. For example, a hotel may collect different information for registration (e.g., name, address, email, or payment information), than for its on-site spa services (recent health concerns or physical ailments, pregnancy). Its privacy notice should explain to consumers which information will be collected under what circumstances.

It is important to note that, regardless of where or how, you make your privacy notice generally available, the CCPA requires that the notice be provided “at or before the point of collection.” Just-in-time consent or acknowledgments for specific types of data collection, although not required by the statute, can be an effective tool to support your privacy notice. This can take the form of checking or unchecking a box beside a fillable blank for email addresses which says, “Please add me to your newsletter so I can receive updates and special offers,” or a statement on a check-out display which states that if a customer enters their mobile number, the company will use it to text them when their order has shipped. In cases when a business obtains personal information from an entity other than the individual consumer, compliance with the CCPA point of collection notice requirement becomes more difficult. For example, if a franchisee provides a franchisor with personal information about California resident consumers, the franchisor may have an obligation to provide notice to the affected consumers, even though the franchisor has no direct relationship with those consumers

The statute does not require a written notice so, technically, a verbal disclosure such as a salesperson’s explanation of how particular information will be used would satisfy the notice requirement. However, a written notice constitutes the best practice for evidentiary reasons.

---

The prohibition contained in this section of the CCPA is also important. A company which collects a consumer’s name and email address for the sole stated purpose of sending a purchase receipt may not subsequently use that email address for marketing. While many businesses are likely to guard against this situation by overstating the purposes for which they collect information, there are both legal and practical curbs against doing so too broadly. First, the statute requires that a business state the purpose for which categories of information “shall” be used, which implies that a business may be out of compliance if it simply lists an expansive, hypothetical series of purposes in order to allow it to do anything it may happen to want to do in the future with that information. Second, privacy watchdogs are likely to create negative publicity around companies which publicly state that they will use personal information for extremely broad purposes unrelated to the core reason for disclosure, and this may influence some consumer’s decision making.

2. **Right to Access**

   a. **Consumer Right**

   As noted in the prior section, this right is described in two separate statutory provisions within the CCPA. It is found in both Sections 1798.100 and 1798.110. The language in Section 1798.100 provides as follows:

   A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

   Separately, Section 1798.110 provides that a consumer has the right to request the categories of information a business has collected about them, the categories of sources from which the personal information was collected, the business or commercial purpose for collecting or selling the information, the categories of third parties with whom the business shares the information, and the specific pieces of personal information collected about that consumer.

   In order to assist consumers in making such a request, businesses are required to provide at least two methods for submitting requests. Somewhat bizarrely, one of these two methods must be a toll-free phone number, even though many businesses subject to the law do not already have a toll-free number and will need to obtain one simply for this purpose, and that it is likely that much of the verification of these requests will probably need to happen through means other than by phone. Another method, if the business has a website, is “a Web site address.”

---

64 Cal. Civ. Code §1798.100(a).


67 Id. There is a pending amendment to clarify that a “web site address” is an email address (not a fillable form on a web page), and to exempt businesses which operate entirely online and directly with consumers from having to maintain a toll-free phone number. AB-1564 Consumer privacy: consumer request for disclosure methods (2019-2020).
The business is also obligated to provide this information without charging the consumer within 45 days of receiving a “verifiable consumer request.” However, it is not required to respond to more than two requests from a consumer in any 12-month period.

Part of the intent behind this provision is to allow for data portability. The statute provides that information must be delivered by mail or electronically, but if delivered electronically it must be “to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance.” Data portability issues are unlikely to affect most restaurants, hotels or many other types of retail franchise businesses, but this could have an impact on systems where some of the “stickiness” of the consumer relationship revolves around a difficulty in moving information from one business to another, such as, hypothetically, tax preparation, consumer preferences with respect to janitorial services, or similar industries.

b. Verifiable Requests

For businesses, the most challenging aspect of compliance with this section is avoiding improper disclosure. A business is only obligated to provide this information when it receives “a verifiable consumer request.” It is incumbent on businesses to avoid disclosing customer information to the wrong person either through an innocent wrongful disclosure (i.e., accidentally sending John Smith of Minnesota information to requester John Smith of Michigan), or through malicious inquiries (i.e., scammers purporting to be Jeff Bezos and requesting his data).

A verifiable consumer request is defined as a request by a consumer, a minor’s parent or guardian, or an authorized representative “that the business can reasonably verify, pursuant to regulations adopted by the Attorney General… to be the consumer about whom the business has collected personal information.”

The statute specifically calls for the California Attorney General to establish “rules and procedures” no later than July 1, 2020 for how to make a verifiable consumer request. Among the factors the AG’s office is intended to consider are “minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business…” One relatively obvious method for verifying a consumer’s identity is requiring that the request be made through a password-protected account with the business which belongs to that consumer, but alternate mechanisms are needed to deal with situations where a consumer does not have an account.

The issue of verifiable identities raises a number of questions. Will businesses that currently allow consumers to make purchases without creating an account need to change

---

70 Cal. Civ. Code §1798.100(d).
71 Id.
72 Cal. Civ. Code §1798.100(c).
75 Id.
that requirement in order to enhance their ability to comply? If a single account is used by more than one person in a household, can it be used to verify identity? In the event of a data breach in which passwords are at risk, is a business still justified in relying on accounts to verify identity? If a business has relatively little information about a consumer, can it reasonably verify their identity, and will this lead businesses to collect more information in order to be in a position to verify requests?

The answers to most of these questions are not yet clear. With respect to isolated transactions where the business does not want to save data, however, there is a silver lining. Businesses are not required to save any information collected for a “single, one-time transaction,” and no disclosure is required as long as the business did not, in fact, retail or sell such information, or maintain it in a matter that would link it to other consumer data.76

c. Readily Useable Format

Another compliance challenge is that the information must be provided in a “readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.”77 A company may not require a consumer to create an account for this purpose.78 In practice, this may raise questions about which formats count as readily useable and whether companies will have to reformat information before providing it to a consumer, which would create an additional cost of compliance.

3. Right to Know Information that Is Sold or Disclosed

The CCPA’s treatment of a consumer’s right to know what information has been sold or disclosed is very similar to the right to access of the information collected. The CCPA requires that, in response to a verifiable consumer request, a business must disclose (1) the categories of information it has collected; (2) the categories of information it has sold and the “categories of third parties to whom the person personal information was sold”; and (3) the categories of personal information that the business disclosed “for a business purpose.”

The substantial use of the term “categories of information” suggests that a business is not required to provide the actual information it sold or disclosed to a third party. The requirement is likely satisfied by disclosure of more general information, such as, “We disclosed your name, address, phone number and account number to a third-party banking entity which provides financing to us, for the purpose of obtaining financing.”

This provision also contains a restriction on the third party. “A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.”79

76 Cal. Civ. Code §1798.100(e).


78 Id.


4. **Right to Deletion**

a. **Requirement**

The CCPA also codifies a consumer right to require a business to delete information the consumer has provided to them.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.\(^{81}\)

Like the disclosure obligation, this provision also requires that consumers submit a verifiable request. All the concerns and issues related to verifying the identity of a requester as described in Section III(F)(3) apply to this right as well.

The most obvious reason for this section is to allow consumers to prevent a company from continuing to monetize that consumer’s data and to prevent the business from continuing to use it for marketing purposes. To ensure that companies are not compelled to delete information they require in order to conduct business, the statute includes a list of exemptions from the requirement to delete, including completing a pending transaction, complying with a legal obligation, protecting against security incidents, protecting free speech, and safeguarding scientific or historical research for the benefit of the public.\(^ {82}\)

Many of the carve-outs in this section make it clear that a business does not have to delete a consumer’s data in situations where it would harm the business. For example, because a business is allowed to retain data to complete transactions requested by consumers, a consumer could not make a purchase under “final sale” conditions, and then demand deletion of their personal information before the product ships so as to void the transaction. Likewise, it appears that a business could retain consumer purchase information for historical accounting purposes in order to provide support for its revenue numbers in the event of an audit or maintain a record of purchasers in order to fulfill warranty obligations.\(^ {83}\)

b. **Compliance Challenges**

In addition to the challenge posed by verifying the identity of a consumer requesting data deletion, a related issue for many businesses is ensuring that they can find all the locations where such data exists in order to complete the deletion. Some businesses with streamlined Customer Relationship Management or “CRM” systems and highly consistent operations may have no issues identifying where a particular consumer’s information

---


83 How broadly these exemptions will be read is unclear at present. Because a company is allowed to maintain personal information “to enable solely internal uses that are reasonably aligned with the expectations of the consumer...” [Cal. Civ. Code §1798.105(d)(7)] it stands to reason that a company could maintain a list of purchasers and their contact information for use solely in the event of a product recall. However, there is a pending amendment to allow a new motor vehicle dealer and the manufacturer to retain purchaser information for warranty and recall repair purposes. AB-1146 California Consumer Privacy Act of 2018: exemptions: vehicle information (2019-2020). This amendment suggests that perhaps the language in section (d)(7) does not protect the right to retain information in case of warranty claims or product recall notices or repairs, thus necessitating the amendment for the motor vehicle industry.
resides. But it will be a different story for many other businesses which may operate with a combination of updated and legacy systems or multiple offices which use different methods for data recordation and storage.

Businesses will be well-served by ensuring that their systems are searchable and that their staff are using information in a uniform manner so that consumer data coming into the businesses for a particular purpose can be readily located and has not “cross-contaminated” any other systems where the company might not think to look for it. This requires a combination of smoothly operating systems and employee training.

Although the CCPA does not use the terms “controller” and “processor” like the GDPR does, this general concept is carried through into the CCPA with the obligation for businesses to direct their service providers to also delete information under this section. The need to be able to direct a service provider such as a marketing company to delete certain information will require businesses to evaluate the terms of key contracts with service providers to whom they disclose personal information of consumers. In some instances, businesses will need to revise these agreements to ensure that their providers will delete information if necessary.

5. **Right to Opt-Out**

The CCPA also confers a limited right to opt out on consumers. The right to opt out is limited to opting out of having a business sell the consumer's information, rather than a right to opt out of unwanted uses of the information.

(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.\(^{84}\)

Companies that are subject to this provision of the CCPA are required to add a “clear and conspicuous” link on their website home page which says “Do Not Sell My Personal Information.”\(^{85}\) This link must provide access to a page which allows a consumer to opt-out of the sale of their personal information. Businesses are prohibited from requiring the consumer to create an account in order to direct the business not to sell their information.\(^{86}\)

An opt-out direction lasts for a minimum of 12 months, after which time the business may “request[] that the consumer authorize the sale of the consumer’s personal information.”\(^{87}\) Note that a year after the initial opt-out, the business may make this request, but the opt-out is not reversed or deleted.

---

\(^{84}\) Cal. Civ. Code §1798.120(a)-(b).

\(^{85}\) Cal. Civ. Code §1798.135(a), but see discussion in Section III(G)(3)(c), below, regarding setting up a California-only homepage for California consumers.

\(^{86}\) Id.

Because most companies do not engage in the sale (or transfer for value) of the majority of personal information they collect, this right is unlikely to have an enormous impact on the average businesses’ day to day operations. However, unless a franchisor and franchisee enter into an agreement specifying that their exchange of information is not a sale and is in the nature of one party acting as a service provider to the other, there is some risk that a consumer might try to characterize the sharing of this information as a sale, subject to this section. For example, if a franchisee collects guest survey information at the behest of the franchisor and dutifully provides the information to the franchisor, this could be interpreted as a transfer of data for consideration. Contractual language establishing that the franchisee acts as a service provider in this transaction will help to avoid creating liability in this situation.

At the same time, however, it could have a significant impact on the ability of the company to transfer customer lists or related data in a merger or acquisition transaction. In preparation for this, many companies will want to update their privacy notices to alert consumers that their data may be “sold” as part of this type of transaction.

a. **Special Rules for Minors Aged 13 - 16**

The right to opt-out converts to a right to opt-in for minors between the ages of 13 and 16. The business must first obtain these consumers’ affirmative authorization for the sale of their personal information.\(^88\)

In many instances, a business does not know the age of its consumers. There is no specific requirement imposed by the CCPA that businesses collect age information about their consumers, but the statute does provide that a business which “wilfully disregards” consumers’ ages will be deemed to have actual knowledge of their ages. Thus, a company that has reason to suspect that certain consumers are under age 17 should comply with the opt-in rules, or conduct additional diligence to determine ages.

b. **Special Rules for Minors Under 13**

There is a similar opt-in procedure for the personal information of children under age 13, but it is controlled by their parent or guardian.\(^89\)

6. **Anti-Discrimination**

A concern raised by many privacy advocates is that businesses that have been accustomed to monetizing consumer data will try to discriminate against consumers who do not want to allow their data to be used, either by refusing to engage with them at all, or by increasing prices substantially in an attempt to dissuade the consumer from protecting their data. CCPA tackles this with an anti-discrimination provision which narrows the instances in which a business may “upcharge” a consumer for exercising its rights. It prohibits the business from denying goods or services, charging different rates, manipulating discounts, or providing a different level or quality of goods to a consumer who exercises their rights.\(^90\)

Consequently, a company is prohibited from only providing goods or services to customers who agree to

\(^{88}\) Cal. Civ. Code §1798.120(c).

\(^{89}\) Id.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

This section eliminates a company's ability to refuse service to those who opt out. However, section (a)(2) would permit a company which can establish the value of the consumer's data, to charge a higher price in some limited situations.

Among the many confusing aspects of the CCPA is this phrase at the end of section (a)(2): "the value provided to the consumer by the consumer's data." No one is entirely sure what this means, since in some contexts a consumer's own data would be invaluable and in other contexts it might have little or no value. Some legal experts have opined that this appears to be a drafting error and that the statute was intended to refer to the value provided to the business by the consumer's data. This makes more sense and would permit a company to offer consumers who permit their data to be used to benefit from a discount calculated by the value the business reasonably expects to receive from having the ability to use that personal data.

7. **Security**

At first glance, CCPA does not appear to impose any security requirements. However, the CCPA includes a specific reference to "the duty to implement and maintain reasonable security procedures and practices" as follows:

(a) (1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.91

This provision allows a consumer a private right of action in the event of a data breach. However, it appears to set up a potential defense for some companies. If a company exercises reasonable security protocols, appropriate to the nature of the information it collects, and despite these reasonable security measures it still suffered a data breach, under a plain reading of the statute that company should not be liable to consumers under this statute.

Not every unauthorized access or disclosure of Personal Information is subject to the CCPA private right of action, however. The private cause of action applies only to access or disclosure of a subset of Personal Information, as defined in California's breach

---

notification law. Specifically, this provision will apply to access or disclosure of an individual’s first name or first initial and last name in combination with any of the following:

- Social Security Number;
- Driver’s license number or California identification card number;
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
- Medical information; health insurance information; or
- Information or data collected through the use or operation of an automated license plate recognition system.92

In addition, under CCPA’s “cure provision,” a consumer must inform the Business via written notice 30 days prior to bringing the civil action, and the Business will have the opportunity to cure the violation(s). If a Business is actually able to cure the violation(s) and provides the consumer an express written statement that the violation(s) were cured and that no further violation(s) shall occur, then the action for statutory damages will not advance.93

It remains to be seen how courts will interpret this reference to “reasonable security procedures.” There are, however, some practices that have been recognized as a minimum threshold in order to establish reasonable security procedures and practices in other contexts, which may prove instructive. The California Attorney General previously identified the Center for Internet Security’s Critical Security Controls (“CIS-20”) framework as “minimum level of information security that all organizations that collect or maintain Personal Information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”94 The development, testing, and implementation of a written information security program (“WISP”), including an Information Security Governance Policy, an Incident Response Plan, and a Business Continuity and Disaster Recovery Plan, also helps to demonstrate reasonable security. These policies should document the actual measures employed—such as physical security protocols, passwords, encryption, two-factor authentication, firewalls, vendor audits, penetration testing, employee training, and limiting access to Personal Information—to secure data. Finally, the designation of a senior-level enterprise-wide official that oversees these policies and practices, such as a Chief Information Security Office, will also demonstrate reasonable practices and oversight of information security controls.95

92 CCPA § 1798.83(h). Note that draft legislation has been proposed, AB 1130, which would expand the definition of personal information that is subject to breach notification, to include passport numbers and biometric data. Available https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1130.

93 CCPA § 1798.150. Note that a bill amending CCPA’s consumer remedies has been proposed, SB 561, expanding the civil right of action to extend to any CCPA violation (as opposed to instances in which nonencrypted or nonredacted Personal Information… is subject to unauthorized access and exfiltration, theft or disclosure…”). See SB 561 and CCPA § 1798.150 (a)(10). We consider adoption of this amendment unlikely prior to January 2020.


95 Some regulations specify that a Chief Information Security Officer (“CISO”) must fill this role. See New York State Department of Financial Services’ Cybersecurity Requirements for Financial Services Companies.
8. Updating Information

While most businesses will undoubtedly want to treat compliance as a one-time exercise which can be completed and put in the rear-view mirror, the CCPA specifically makes compliance an ongoing process. It requires that information about consumers’ rights, methods for submitting requests under the CCPA, and a list of the categories of information the business has collected about consumers in the preceding 12 months, be included in an updated privacy notice or website every 12 months.\(^\text{96}\)

The disclosure of the categories of information actually collected in the preceding 12 months requires companies to not merely assess whether any stated policies in public-facing documents have changed, but to affirmatively track the information collected throughout the year, to the extent that any new or different information was collected. Hypothetically, even isolated pilot programs and unique customer transactions might be disclosable pursuant to this section.

G. Impact on Businesses and Compliance Issues

1. Evaluation of Applicability

As a preliminary step, franchise systems will need to evaluate whether they are subject to compliance requirements. Businesses above the revenue threshold or that engage in the routine and continuous sale or transfer of data may have an easy answer. Similarly, small systems or businesses with little or no interaction with California may be able to rule themselves out quickly.

For other businesses with not-insubstantial California contacts, the evaluation may be significantly more challenging and will involve questions that companies are not used to asking. While CRMs may track how many California contacts a company has, this is generally not a top question for most businesses. In addition, when it comes to names and email addresses which lack any city or state affiliation, it may be impossible to establish whether they are California consumers or not. As a result, the evaluation may hinge on information the company does not have and its internal risk evaluation.

2. Franchise System Triggers

a. Loyalty Programs

The majority of franchise systems are headquartered outside of California and do not consider themselves to be California businesses. Their loyalty programs, however, are likely to result in the collection of significant volumes of California consumer data, potentially resulting in the collection of enough data to push the franchisor over the top of the CCPA threshold. Depending on the structure of the loyalty program, in many cases it may be the non-California franchisor that is subject to compliance and not any of its smaller, individually owned franchisee units actually operating in California, if no individual unit’s operations result in the collection of the threshold volume of data.

b. Management Arrangements

In some industries, such as the hotel business, one company will serve as the manager of a group of businesses operating under the same mark. This manager may coordinate or be in charge of functions like marketing and CRM, reservations systems, and

more, and be in a position of collecting larger amounts of data on behalf of the group it manages than any individual unit.

In this scenario, it is possible that the management company will do business in California and collect the requisite number of contacts to trigger compliance obligations. Because the management company is not an affiliate of the businesses it manages (typically), its compliance obligations will not place the managed property directly subject to the CCPA, but to the extent that the management company shares personal data with that property, the management company will need to ensure that it has contractual authority to require deletion or disclosure of uses of that personal data.

c. **Franchisor Access to Franchisee Systems**

Even in the absence of loyalty programs, many franchise systems are set up to permit the franchisor to access and even download significant amounts of materials on franchisee computer systems. In instances where a non-California franchisor that is not otherwise obligated to comply with the CCPA engages in downloading of information from franchisee systems, it might trigger CCPA compliance simply from its policing of franchisee computer systems.

d. **Multi-Unit Franchisees**

Depending on the business type, both individual and multi-unit franchisees operating in California may also be affected. Franchisees such as hotels with high revenues will hit the revenue threshold for compliance. Smaller franchisees such as fast casual restaurants may serve enough people to hit the 50,000 threshold either as an individual unit, or across multiple units owned by the same person or entity.

As discussed elsewhere in this paper, where the franchisee is subject to the CCPA compliance but its franchisor is not, the franchisee is likely to have significant concerns about issues like website compliance, privacy notices, sharing of consumer information, the handling of deletion requests, and how to handle disclosure of the purposes for which personal information was used, if it is possible that the franchisor has made uses of the information that it does not want to disclose to the franchisee.

e. **Mergers and Acquisitions**

CCPA requires businesses to tell a consumer how it will use their personal information. In order to avoid any future challenge to that company’s ability to transfer customer data to an acquiring company, businesses would be well served by advising consumers that they reserve the right to transfer personal data to a successor in interest or a business that acquires all or the majority of the assets of the business. Because consumers have the right to opt out of having their personal information sold, the seller should scrub any data it transfers to a buyer against its opt out list. As a due diligence item, the buyer should ensure that the seller has maintained an opt out list and has performed this step before transferring any data.

Although most franchise systems do not engage in the sale or transfer of consumer data, one instance in which most will sell data is in the event of an acquisition. Therefore, there are some scenarios in which a company not otherwise subject to CCPA compliance might become subject to it as a result of an exit in which the customer data is heavily valued.
3. **Franchise System Challenges**

   a. **Unequal Concern Within the System**

   One of the likely critical challenges in dealing with CCPA compliance will be getting all parties on the same page. As businesses have seen with GDPR compliance, the costs of data privacy and security compliance programs can be significant, with many businesses experiencing costs exceeding $50,000, and some of the largest businesses seeing costs in excess of $1 million.\(^\text{97}\)

   One anticipated issue with CCPA compliance is that, for many franchise systems, not all parties in the franchise system relationship will be equally impacted by it. California-based franchisees may be anxiety-ridden over their non-California franchisor’s lack of attention and focus on compliance issues, worried that the franchisor will use information collected by the franchisee for purposes beyond what is permitted, or frustrated that the franchisor has failed to properly update the privacy notices or software the franchisee is obligated to use. Non-California franchisees may be unhappy with their franchisor’s decision to spend significant amounts of money on overhauling the system’s CRM protocols in order to protect the franchisor, or a select group of California franchisees, rather than on other aspects of the system. In some instances, franchisors may be more aware of compliance requirements than their California franchisees, and policing compliance may be a significant source of frustration.

   These issues will be exacerbated by the statute’s yoking together of franchisees and franchisors, as described in Section D. 6 above. If a franchisor seeks to maintain the argument that they do not have “management control” as described by the CCPA, and therefore is not the same “business” as its franchisees—the next challenge will be: how can the franchisor and franchisee still exchange personal information without implementing an opt-out for such exchanges? In this situation, the franchisor and franchisees will have to agree on whether each partner is a “service provider” or “third party” under the law. The advantage to structuring the relationship as a service provider is that it eliminates an opt-out requirement. But this comes at a price: service providers cannot use the data they collect or process for their own purposes or benefit. Accordingly, a franchisee that agrees to collect or share information with the franchisor as a service provider, would lose the ability to use that same information for its own purposes. On the other hand, if there is no service provider agreement between the parties, one or both will be responsible for implementing an opt-out. Some systems are likely to overcome these issues through good communication and education. Others, however, will struggle with compliance and may face reluctance from various parties to engage in the steps required to achieve a compliant outcome.

   b. **Marketing Systems Dictated by Unaffected Franchisor**

   One place where challenges likely will arise is with a heavily-used marketing system imposed by a franchisor which is not itself affected by the CCPA, while some of its multi-unit franchisees are. In some instances, both the franchisor and its marketing vendors may have limited understanding of the CCPA’s compliance obligations, and a franchisee’s insistence that the marketing approach mandated by the franchisor violates California law may fall on deaf ears.

   Franchisors with California franchisees who are likely to be affected by the law should anticipate that they may need to change privacy notices on websites which franchisees are required to use, to point-of-sale systems which collect consumer data for

purposes beyond single-use transactions, and that they may be prohibited from using email address or other contact information for marketing purposes without having proof of prior notice to consumers about the use of their data.

c. **One-Size Fits All Policies or Special Policies for Affected Entities?**

In instances where not all the parties are equally affected, franchise systems will face the question of whether to try to make the entire system compliant, or to attempt to carve out the California data or California entities that are affected, in order to avoid having to change anything for a large portion of the system. For example, a business might elect to segregate its California consumer data so that marketing is no longer sent to those email addresses, rather than update its policies in a manner which would legitimize using those email addresses for marketing purposes.

The statute itself anticipates that some businesses may adopt special policies at least in some regards. The “Do Not Sell My Personal Information” link is allowed to be on a special website “dedicated to California consumers,” so long as the company “takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.”

As a general observation, the authors doubt that special policies are the best approach for most systems for several reasons. First, many businesses struggle when there is no one-size-fits-all approach to various operations, and small errors can create significant liabilities. Second, the cost of maintaining two separate approaches to data can, in the long run, exceed the cost of the overhaul to a new policy throughout the system. Third, there is a reasonable chance of either a federal data privacy law, or of additional states adopting similar data privacy and security laws that will quickly make a patchwork approach untenable. Nevertheless, for companies struggling with implementing compliance by 2020, a California carve-out may be a viable temporary solution.

4. **Internal Operations Audit and Assessment**

Many of the CCPA compliance steps echo those used for GDPR compliance. This includes the first major step, which is conducting a review of existing systems and evaluating compliance. Questions to ask will include the following:

- Have we provided the required notice to all consumers prior to or at the time of collection of their information?
- Do we have a list of all the purposes for which we collect information, and all the information we collect?
- Does our public-facing privacy notice reflect all the required disclosure information? Is it easy to read and understand, or could it be misleading?
- Do we have uniform systems, or do different business units follow different procedures? If the latter, should those be made uniform or not?
- Do we have any security problems? Is our physical and digital security at the level it should be?

---

• Do we collect information from children? Is there a significant risk that we are collecting information from children without adequately verifying ages?

• Who will be in charge of consumer requests? What mechanisms have we established for receiving requests?

• What system(s) do we have for verification?

• Do we have a privacy officer or other person within our business who is responsible for privacy compliance?

One critical element of this process is mapping where data is stored. In response to a verifiable consumer request for information under the CCPA, a company must provide information to a consumer within 45 days. To avoid a company-wide search for data, a business needs to know where to look for that information. Some businesses have streamlined and highly connected systems which may make this a relatively straightforward task, but many others store information in both legacy and modern databases which do not connect to one another, in a blend of physical and digital formats (sometimes depending on the training or preferences of different staff members), and in ways which could make it difficult to confirm if the data relates to the same consumer or represents a different consumer. Part of this audit and assessment process must include identifying where consumer data will be stored and, if necessary, creating more uniform procedures for data intake and storage to support future compliance.

5. **Update Public Notices**

As discussed above, public-facing privacy notices are a key way to communicate to the public what data will be collected and how it will be used. Systems which want to use collected email addresses for marketing will rely on this disclosure. Businesses should evaluate all the instances in which they collect information, what information is collected and the purposes for collection, and provide a careful, clear and easy to understand disclosure which is not subject to a consumer’s later objection that they were not adequately notified of how their information would be used.

6. **Create Internal Policies**

Internal policies create a framework for ensuring that the company’s employees will handle data in the proper ways and will not use or share information except as appropriate. These policies are also critical for ensuring that consumer requests are responded to timely, that difficult requests are elevated to the attention of the proper individuals, and that data breaches (and potential breaches) are brought to the immediate attention of the proper individuals to mitigate harm to the public.

Internal policies may take the form of additional pages in an employee handbook; of a separate, stand-alone set of guidelines used in training; of a set of emergency response protocols used by certain managers in the event of particular events; or all of the above.

7. **Training**

Training is critical to ensure the implementation of policies and ongoing compliance with them. It is particularly important as a tool for bringing attention to the importance of compliance and helping all parties understand why some existing systems may have been changed. In franchise systems, training may include both employees within a single organization and training across all franchisee units.
8. **Modify and Update Vendor Agreements**

For the reasons discussed elsewhere, it is important that vendors with access to or possession of certain data have obligations to safeguard it and to refrain from sharing it without the consent of the appropriate parties. Vendors including but not limited to CRM systems, marketing companies, loyalty program administrators, registration system technology platforms, third-party delivery companies and others can be part of the critical web of vendors whose agreements will need to require that if a proper deletion request is made, the appropriate information will be deleted by all parties.

9. **Data Protection or Privacy Officers**

Finally, the company should evaluate whether it needs a data protection or privacy officer (collectively, a “DPO”). DPOs are not required by the CCPA, but many companies subject to the GDPR may already have one, in which case that person may be an ideal person to also take charge of CCPA compliance. Alternatively, some companies have found that their compliance efforts are significantly helped by having a dedicated person who is relatively senior in the organization’s structure, and who is responsible for overseeing ongoing compliance issues related to this and other questions of data security.

H. **What Does the Compliance Process Look Like?**

1. **Key Participants**

   Compliance is typically led by the company's privacy officer, if the business is established enough to have one. Other key participants likely include senior IT staff, operations personnel, risk and legal.

   It can be very helpful to include a Director of Marketing or Chief Marketing Officer, since the marketing department may be the most significantly impacted by consumer opt-outs and limitation on the use of data for reasons other than the consumer’s original transaction. Human Resources (“HR”) may play a significant role with respect to employee training regarding compliance and in many organizations it will be critical to have HR’s support with respect to future disciplinary actions or terminations for an employee’s violation of critical security protocols.

   A critical mistake that some businesses make is delegating compliance to mid-level management without sufficient upper management involvement, or without senior management fully understanding the complexity of issues involved in data privacy matters. If a portion of the C-suite is not involved at least through periodic briefings, or if the compliance team is too junior to fully comprehend the impact of their decisions on the business as a whole, the outcome is sometimes that, after a substantial investment in review and planning, the compliance group’s solutions are rejected by upper management and the process restarts with new guidance as to what systems or methods are vital and cannot be altered. In the authors’ experience, the involvement of someone with a detailed familiarity with the development of processes which can be audited and tested can be valuable to help create processes which can be documented and audited for compliance.

2. **Data Mapping**

   Data mapping is an internal audit process intended to identify what personal information the business collects, and how it is stored, used and shared. This information is critical to disclosure of personal data collected, the uses the business makes of that information, and determining where an individual’s data might exist if that person makes a subject access request.
This review can also reveal system vulnerabilities, inconsistencies in the way different departments (or even different employees) handle various tasks, and the existence of stored data that no one remembered existed. Among the things to look for are systems or procedures that should either be improved from a security standpoint (e.g., lock up files containing customers’ social security numbers) or streamlined to improve future CCPA compliance (e.g., all employees need to use the CRM system rather than personal rolodexes or a non-networked digital address book so customer data can be easily located in the event of a future subject access request). In conducting this review, businesses should remember that the inquiry goes beyond digital records and includes paper files as well.

3. **Security Assessments**

The data mapping process may automatically identify certain security issues. The company should separately consider its physical and digital security and ensure that it has on staff, or has retained as a consultant, information technology specialists with the appropriate degree of knowledge to advise the company regarding current best practices related to its computer systems.

According to a recent study, 56% of data breach incidents originated from a malicious outsider and another 34% were the result of accidental loss (the latter was down from 47% in the prior year). Companies should consider whether their systems offer reasonable protection from malicious outsiders. They should also consider how to train their employees to reduce or avoid accidental loss, which can include losing a device or files mistakenly sent to the wrong person. Policies requiring immediate reporting of lost data, permitting remote data wiping, prohibiting certain information from being taken offsite, and clear breach response protocols can be useful.

4. **Documenting Compliance and Reasonableness**

Once the company has addressed its vulnerabilities to the best of its abilities, the final step is production of external facing privacy notices that comply with the notice requirements of the CCPA and internal facing documentation summarizing the steps the company has taken, its internal protocols, its security measures, and documenting its processes to show its compliance.

IV. **A NOTE ON OTHER APPLICABLE LAWS**

For good or ill, the CCPA has transformed the legislative dialogue on consumer privacy, resulting in a crush of other states jumping into the fray to propose their own privacy laws. To date, 14 state legislatures have proposed cross-sector privacy statutes in 2019. But, since the CCPA passed in 2018, only one state—Nevada—has passed a cross-sector privacy statute. Two other states—Washington and New Jersey—seem tantalizingly close to becoming the third in the trend. Inevitably, both houses of the US Congress have followed suit with a variety of proposed bills, ostensibly to head off development of a state-law “patchwork” of privacy regulations.

A. **Laws and Bills in Other States**

1. **Nevada**

---


100 These states include Hawaii, Maryland, Massachusetts, Nevada, New Hampshire, New Mexico, New Jersey, New York, North Dakota, Oregon, Rhode Island, Texas, Vermont, and Washington.
Nevada’s new privacy law creates a limited right of opt-out for the sale of information collected online. The scope of the Nevada law is narrow when compared to the CCPA. The Nevada statute applies only to website “operators.” It also applies only to information collected online and that is identifying or maintained in identified form. And the statute provides only a right of opt-out; there is no right of access or deletion available under the new Nevada law. Compliance with this new Nevada law is required by October 1, 2019.

2. Washington State

While most of the state privacy legislation proposed in 2019 appeared modelled on the CCPA, Washington’s proposed statute was the outlier. The proposed Washington Privacy Act (“WPA”) drew more directly from the GDPR rather than the CCPA. For example, unlike the CCPA, the WPA does not exclude non-profit entities. Instead, it would cover all legal entities (except state and local governmental entities) that conduct business in Washington or produce products and services that are intentionally targeted to Washington residents, provided that they meet specific criteria. These criteria narrow the likely scope of the WPA to only businesses that either: (1) control or process data of 100,000 consumers or more; or derive over 50 percent of gross revenue from the sale of personal information and process or control personal information of 25,000 consumers or more.

Like GDPR, the WPA relies on a business’ defined role as a “controller” or a “processor.” Controllers (who determine “the purposes and means of processing of personal data”) would be responsible for complying with the obligations set forth in the WPA, while processors (who act on behalf of the controller) would have to follow the instructions of the controller and assist the controller in meeting its obligations.

The WPA would give consumers the right to access personal data concerning the consumer that the controller holds and, in certain circumstances, require the controller to provide the data in a “structured, commonly used, and machine-readable format.” The WPA also would require controllers to correct inaccurate personal data and, in certain listed situations, to delete personal data at the request of the consumer. Under the WPA, consumers would be able to object to and restrict the processing of their personal data under certain circumstances. A controller would be required to stop processing when the consumer objects to direct marketing, but could continue processing for a purpose other than direct marketing, provided the purpose was “compelling legitimate ground” to do so. The bill also would require a controller to notify any third party that received a consumer’s personal data that the consumer has requested to correct, delete, or restrict the processing of the data.

The WPA stands apart from other state law attempts at comprehensive privacy regulation by taking direct aim at automated decision making and other uses of artificial intelligence. The WPA would prohibit controllers from subjecting consumers to decisions “based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer.” These effects would include the “denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.”

101. Specifically, a first and last name; a home or other physical address which includes the name of a street and the name of a city or town; an electronic mail address; a telephone number; a social security number; an identifier that allows a specific person to be contacted either physically or online; any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable. S. B. 220, 80th Leg. ( Nev. 2019) (Effective Oct. 1, 2019).

The WPA also would restrict the use of facial recognition technology.\textsuperscript{103} Specifically, controllers that use such technology for profiling would be required to provide meaningful human review of any decisions based on the technology where such decisions produce the “legal effects” and “similarly significant effects.” Controllers also would be required to obtain consent from consumers before using such technology. A consumer would be deemed to “consent” by entering a physical premises where such notice is conspicuously displayed, or using online services on which such notice has been conspicuously provided. Processors that provide facial recognition services would be required to (i) provide information about the capabilities and limitations of the technology, and (ii) include in contracts with controllers a requirement that such technology not be used to unlawfully discriminate.

Though the WPA is modeled after the GDPR, there are several notable differences. The WPA does not require an initial lawful basis for processing; however, it does allow consumers the opportunity to restrict processing or withdraw consent in situations other than those allowed under the GDPR. Moreover, the GDPR’s requirement to conduct Data Protection Impact Assessments is limited to situations where processing creates a high risk to the rights and freedoms of natural persons; the WPA would require risk assessments for all processing of personal data.

Ultimately, the Washington legislature failed to agree on the precise parameters of the bill before the end of the 2019 legislative session. It seems likely, however, that some version of the WPA will re-emerge in 2020.

3. **New Jersey**

New Jersey, unlike Washington State, enjoys the advantage of a two-year legislative session. As a result, its privacy bill, New Jersey Assembly Bill 4902 (Companion: Senate Bill 2834) (“NJ AB4902”), proposed earlier in 2019, remains viable.

NJ AB4902 would require operators of commercial websites to provide consumers with access to any personally identifiable information disclosed to a third party within the last 12 months. Such disclosure would include the names and contact information for every third party that received the consumer’s personal information. In addition, operators would be required to allow consumers to opt-out of disclosures of their information to third parties. The bill is limited in scope and would apply only to the operators of websites, not to any other entities that may receive, use, or disclose consumer information collected online.

**B. Push for Federal Preemption**

Multiple members of the US Congress have asserted their intentions to put forward privacy legislation, but little consensus has emerged. Despite a number of hearings over the last year on privacy issues, no comprehensive bill or even a common approach—appears to be moving forward. To date, six bills have been introduced that would set forth broad federal obligations regarding the collection, storage, and disclosure of consumer data.\textsuperscript{104} None of

\textsuperscript{103} The bill defines “facial recognition” to mean a “technology that analyzes facial features and is used for the unique personal identification of natural persons in still or video images.”

these bills has progressed since it was introduced. Despite bipartisan support for the idea of comprehensive privacy legislation, the how and why of such an act remain in dispute.

Disagreement over federal pre-emption of state law may be one factor delaying advancement of any bill. House Speaker Nancy Pelosi (D-CA) recently drew a line in the sand on this issue during a Recode Decode Podcast on April 12, 2019 saying “the Republicans would want pre-emption of state law. Well, that’s just not going to happen. We in California are not going to say, ‘You pass a law that weakens what we did in California.’ That won’t happen.”

V. CONCLUSION

Despite the dismay data privacy laws inspire in most business owners, there can be little doubt that increased privacy and accountability to consumers are new, permanent features of the commercial landscape. What was once limited to financial and healthcare sectors is now being introduced to many other types of businesses, ranging from technology giants to smaller businesses with limited capacity to adapt to new requirements.

While these laws and proposed laws differ from one another, which makes compliance challenging, there are some core tenets that can aid compliance under the majority of them:

- **Transparency.** Companies should be prepared to tell individuals what data the company collects, and how it is used and shared. They should adopt a company philosophy that accepts transparency rather than tries to find ways around it.

- **Uniformity.** Companies that use streamlined, uniform methods of operation will have the easiest time describing their processes, disclosing the data they collect and use, identifying how and with whom they share data, enforcing opt-out decisions, and complying with production or deletion requirements.

- **IT.** Having a strong understanding of how the company's technology systems work is critical to compliance under some data privacy laws. The importance of competent information technology professionals who understand the company’s systems and these laws cannot be overstated.

- **Training.** Solid employee training helps reinforce uniform operation methods and reduces the risk of accidental data breaches caused by employee error.

- **Vendor Management.** Many breaches are the result of a smaller company or vendor’s substandard compliance. Diligence in the selection, vetting, and formation of a contractual relationship with a vendor is critical to avoid having a vendor become the weak link.

Many of these tools, particularly uniformity and training, are part of most franchise systems’ DNA. Although the authors do not anticipate that many systems will be delighted by the increasing burden of privacy compliance, out of all companies franchise systems may be among the best positioned to prepare for and adapt to the changing laws over time.

---

BIOGRAPHIES

HELEN GOFF FOSTER

Helen Goff Foster, CIPP/US and CIPP/E, is a partner in Davis Wright Tremaine’s Technology + Privacy & Security practice in Washington, D.C. She has enjoyed a diverse career in privacy, cybersecurity, and consumer protection law—spanning two decades, four federal agencies, the White House, and private law practice. A former FTC attorney, Helen thrives at the intersection between consumer protection and emerging technologies.

Helen helps clients in the hospitality, retail, technology, communications, and financial services, industries avoid and mitigate regulatory investigations of data-driven marketing practices, integration of new technologies, and personal data use. While at the FTC, she wrote some of the agency’s first information privacy and safeguarding regulations. In private practice, she has represented clients successfully in FTC investigations and inquiries relating to social media, gift card programs, deceptive food advertising, and credit reporting. She brings 20 years of practical experience to advising on more recent privacy and cybersecurity developments as well, including the California Consumer Privacy Act (CCPA), the E.U. General Data Protection Regulation (GDPR), and the New York Department of Financial Services (NY DFS) Cybersecurity Regulations. She is a co-chair of DWT’s FinTech working group, a member of the firm’s Artificial Intelligence team, and credentialed as a Certified Ethical Hacker.

DAWN NEWTON

Dawn Newton is a partner in the Bay Area law firm of Donahue Fitzgerald LLP. She heads its franchise practice and co-chairs the firm’s Intellectual Property group. She primarily represents franchisors in start-up and emerging franchise brands and operates as their outside general counsel. In addition, she represents technology companies and manufacturers in protecting their trademarks worldwide. Dawn has been actively involved in advising franchisors in connection with privacy law compliance for the past two years, in industries including hospitality, technology platforms, retail businesses, and the food service industry. Dawn is a member of the Governing Committee of the ABA Forum on Franchising and co-chaired the 40th Annual Meeting of the Forum in Palm Desert, California. She currently serves as the Forum’s Program Officer. She is a co-editor of The Annotated Franchise Agreement published in 2018, and in 2010 she was honored to be a recipient of the Forum’s Future Leader Award. Dawn is recognized as a Certified Specialist in Franchise and Distribution Law by the State Bar of California’s Board of Legal Specialization and is a Past Chair and Commissioner of the Franchise and Distribution Law Advisory Commission of that Board. She has been named a Best Lawyer in Franchising in the San Francisco region since 2013 by Best Lawyers in America® and has also been recognized in the International Who’s Who in Franchise Law. Dawn is a frequent speaker on franchise and intellectual property matters.

JOHN H PRATT

John obtained his law degree from Oxford University and afterwards successfully completed a doctorate course in comparative law at the Universite d’Aix- Marseille. He is the senior partner of Hamilton Pratt, Europe’s largest specialist franchise law firm. He is the immediate past Legal Advisor to the British Franchise Association and a past Chair of the International Bar Association’s International Franchise Committee and Director of the American Bar Association’s International Franchising Division. He is currently Chair of Euro Franchise Lawyers. He has written “Franchising: Law & Practice”, “The Franchisor’s Handbook” and contributed chapters to a number of franchise publications. He is the joint editor of a recently published American Bar Association publication on franchising in Europe. Who’s Who Legal in 2017 and 2018 rated 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.