「GDPR・CCPA・CPRAの主要論点比較」

（2021年10月12日（火）（米国西部）/2021年10月13日（水）（日本）
オンラインセミナー「CCPA解説オンラインセミナー」
ジェトロ・サンフランシスコ事務所・ロサンゼルス事務所様御主催
（北加日本商工会議所様御協力））

S&K Brussels 法律事務所
事務所代表・マネージングパートナー
弁護士（日本・NY・ブリュッセル（B-List））
杉本 武重
+81 3 6429 8040 / +1 347 259 2661
takeshige.sugimoto@sandkbrussels.com

S&K Brussels

© S&K Brussels LPC 2021

本日のテーマ

S&K Brussels

© S&K Brussels LPC 2021

I. CCPA vs CPRA
（赤字はCPRAによる修正・拡張の説明）
（緑字は参考資料①の関連事例への言及）

S&K Brussels

© S&K Brussels LPC 2021

CPRAによって修正・拡張されるCCPA とは、消費者に消費者の権利を与え、当該「消費者」の「個人情報」を処理する「事業者」に義務を負わせる法律

消費者の権利	事業者の義務
1. 知る権利	(1) 利用目的の通知義務：①通知事項、②通知の態様、③目的外利用の禁止、④保持期間限定の義務 (2) 知る請求への対応義務：①知る権利による開示事項、②知る権利の行使方法、③受領確認、④対応期限、⑤費用、⑥本人確認（消費者請求の検証義務）、⑦請求を拒絶する場合 (3) プライバシーポリシーの開示：①開示方法、②記載事項
2. 削除請求権	削除請求への対応義務：①受領確認、②対応期限、③本人確認、④削除請求への対応、⑤削除請求への回答、⑥例外要件
3. 訂正請求権	訂正請求への対応義務
4. 個人情報の売却または共有に対するオプトアウト権	オプトアウト手続：①オプトアウト権に関する通知、②オプトアウト権行使への対応
5. 未成年者のオプトイン権	未成年者についてのオプトイン手続
6. センシティブ個人情報の利用・開示の制限権	制限請求の手続
7. 権利行使を理由として差別されない権利	①権利行使を理由とする差別の禁止、②個人情報の取得等への金銭的なインセンティブの付与
8. 全般	①売却先・共有先である第三者、個人情報の開示先であるサービス提供者・契約受託者との契約締結義務（個人情報を開示する場合の責任の移転）、②研修義務、③記録管理義務、④個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務、⑤データ保護影響評価の実行義務

© S&K Brussels LPC 2021

CPRAによって修正・拡張されるCCPAの適用範囲：「事業者」への該当性

次の＜テスト1＞、＜テスト2＞、＜テスト3＞または＜テスト4＞に該当する場合には、「事業者」に該当し、CCPA/CPRAの適用を受ける。

＜テスト1＞

要件①　消費者（カリフォルニア州の住民）の個人情報を取得（第三者が自身のために個人情報を取得する場合も含む）し、単独または共同でその処理の目的と手段を決定し、カリフォルニア州で事業を行っている、利益または金銭的便益を目的とする主体であること

要件②　以下の3つの事由のいずれかを充足すること

(A) 暦年の1月1日時点で、前暦年の年間総収入（annual gross revenues）が2500万米ドルを超えていること

(B) 10万件以上の消費者または世帯の個人情報を、年間ベースで、単独若しくは組み合わせで購入若しくは売却または共有する。

(C) 消費者の個人情報の売却または共有から年間収入の50%以上を得ている。

＜テスト2＞

テスト1に該当する事業者を支配し、または、当該事業者により支配され、かつ、当該事業者と共通のブランドを有し、当該事業者が消費者の個人情報を共有する主体

＜テスト3＞

各事業者が少なくとも40%の持分を有する事業者で構成されるジョイントベンチャーまたはパートナーシップ

＜テスト4＞

カリフォルニア州で事業を行う者で、テスト1、テスト2またはテスト3の対象とならず、CPRAに準拠、拘束されることに同意することを自主的にカリフォルニア州プライバシー保護局に証明する者

S&K Brussels

© S&K Brussels LPC 2021

1. 知る権利
(1) 利用目的の通知義務
①通知事項

事業者は個人情報の取得時点までに以下の事項を消費者に通知しなければならない（事例1、12、16(1) 、22(2)、27）。

- 取得される個人情報の種類の一覧
- 取得される個人情報の種類の事業上または商業上の利用目的
- （個人情報を売却または共有している場合には）「Do Not Sell or Share My Personal Information」というタイトルのリンク（事例10(2)）
- 取得されるセンシティブ個人情報の種類の一覧
- 取得されるセンシティブ個人情報の種類の事業上または商業上の利用目的およびその情報が売却または共有されるかどうか
- （センシティブ個人情報を取得している場合には）「Limit the Use of My Sensitive Personal Information」というタイトルのリンク
- 事業者がセンシティブ個人情報を含む個人情報の各種類の保持を意図する期間、または、それが可能でない場合、当該期間を定めるために利用される基準
- プライバシーポリシーへのリンク

S&K Brussels

© S&K Brussels LPC 2021

1. 知る権利
(1) 利用目的の通知義務
②通知の態様：内容

通知は、消費者にとって読みやすく、理解できる態様にて作成されるとともに、消費者に提供されなければならず、かつ、次の内容を遵守することが義務付けられる。

- 平易で、直截な表現を用い、技術的または法的な専門用語を避けること
- 通知に対して消費者の注意を惹き、かつ（もし利用する場合は小さな画面上でも）通知を読みやすくするフォーマットを用いること
- 通常の業務の過程において、契約条件、免責事項、売却告知その他のカリフォルニア州の消費者に対する情報を提供する際に用いている言語で利用可能であること
- 障害のある消費者にとって合理的にアクセス可能であること

S&K Brussels

© S&K Brussels LPC 2021

1. 知る権利
(1) 利用目的の通知義務
②通知の態様：通知の形の例

通知は、個人情報を取得する時点またはそれより前に消費者にとって容易に利用可能な状態に置かれていなければならない。

個人情報の取得の場面設定	通知の形の例
事業者がオンラインで個人情報を取得している場合	事業者のウェブサイトの導入ページおよび個人情報が取得されるすべてのウェブページに通知への目立つリンクを設置すること
事業者がモバイルアプリを通じて個人情報を取得している場合	モバイルアプリのダウンロードページおよびアプリ内に通知へのリンクを設置すること
事業者がオフラインで個人情報を取得している場合	個人情報を取得するフォームに通知内容を記載すること、紙で通知すること、または通知がオンライン上どこに掲示されているのかを消費者に明確に知らせること
事業者が電話越しでまたは実際に消費者と会って個人情報を取得している場合	口頭で通知すること

S&K Brussels

© S&K Brussels LPC 2021

1. 知る権利
(1) 利用目的の通知義務
③目的外利用の禁止、④保持期間限定の義務

事業者の義務	内容
③目的外利用の禁止	■ 事業者は、個人情報の取得時の通知において開示されている利用目的と実質的に異なる目的のために個人情報を利用してはならない。 ■ 事業者による消費者の個人情報の取得、利用、保持および共有は、個人情報が取得または処理された目的を達成するため、または個人情報が取得された文脈と適合するその他の開示された目的のために、合理的に必要であり、かつ、比例的であるものとし、またこれらの目的と適合しない方法でさらに処理してはならない。
④保持期間限定の義務	■ 事業者は消費者の個人情報またはセンシティブ個人情報を、その情報が取得されるための開示された各目的のために、その開示された目的に合理的に必要とされる期間よりも長い期間保持してはならない。

S&K Brussels

© S&K Brussels LPC 2021

1. 知る権利
(2) 知る請求への対応義務
①知る権利による開示事項

- 消費者は、個人情報を取得する事業者に対し、以下の事項を自身に開示するよう請求でき、事業者はその消費者から検証可能な消費者請求を受領する場合、これらの情報を消費者に開示しなければならない。また、事業者が個人情報を売却または共有し、もしくは事業目的のために開示する場合には、消費者が開示するよう請求できる事項は拡大する。
- CPRA規則が採択された場合、消費者は事業者に対し、求められた情報を12か月間分以上開示するよう請求できる。事業者は当該情報を提供することが不可能であることを証明する場合、または不相応な努力を伴う場合を除き、当該情報を提供することが求められる。
- 求められた情報を12か月間分以上開示するよう請求する消費者の権利と、そのような情報を提供する事業者の義務は、2022年1月1日以降に取得された個人情報にのみ適用される。

開示請求の相手方	開示を請求できる事項
個人情報を取得する事業者	■ 過去12か月以内に当該消費者について事業者が取得した個人情報の種類 ■ 前記個人情報が取得された情報源の種類 ■ 前記個人情報の取得・売却・共有の事業上または商業目的 ■ 事業者が個人情報を開示する第三者の種類 ■ 当該消費者について事業者が取得した個人情報の具体的内容
個人情報を第三者に売却または共有し、または事業目的で開示する事業者	■ 過去12か月以内に当該消費者について事業者が取得した個人情報の種類 ■ 過去12か月以内に個人情報が売却・共有された個人情報の種類ごとに、売却・共有された個人情報の種類、および個人情報が売却・共有された第三者の種類 ■ 過去12か月以内に事業者が事業目的のために開示した当該消費者に関する個人情報の種類、および個人情報が開示された第三者の類型

© S&K Brussels LPC 2021

1. 知る権利
(2) 知る請求への対応義務
②知る権利の行使方法、③受領確認、④対応期限、⑤費用

義務項目	内容
②知る権利の行使方法	■ 事業者は、消費者が開示請求する方法を最低2通り準備する必要があり、少なくとも、着信課金用電話番号を含める必要があるのが原則である（事例3(2)、7(2)、12(4)、18(2)、21(2)、25(2) ）。 ■ オンラインでのみ運営され、かつ消費者と直接関係を有する事業者は、着信課金用電話番号の設定は不要であり、電子メールアドレスのみが求められる。 ■ 消費者が事業者に登録したアカウントがある場合には当該アカウントを通じることとし、そのようなアカウントがない場合には消費者の選択に従って郵送または電磁的方法による。 ■ 電磁的方法により提供される場合、その情報は持ち運び可能であるものとし、技術的に可能な範囲で当該消費者がその情報を障害なくして他の主体に移転できる容易に利用可能な形式でなければならない。 ■ 認定代理人による請求に対応することが求められる（事例13(1)、14(1)）。
③受領確認	■ 受領から10営業日以内に受領確認を行うとともに、本人確認の手続と回答の見通し時期を消費者に伝える必要がある（ただし、事業者がその間に開示請求に応諾するまたは拒絶する場合はこの限りでない）。 ■ サービス提供者が知る請求を受けた場合には、サービス提供者は、事業者に代わって請求に応じるか、サービス提供者への請求であるため応じられない旨を消費者に知らせる必要がある。
④対応期限	■ 事業者は、開示請求を検証するのに必要な期間にかかわらず、原則として検証可能な消費者請求の受領から45日以内に無償で開示に応じなければならない。 ■ 請求の複雑性および数を考慮して、合理的に必要な場合には、請求の受領から45日以内に、消費者に対し、請求に回答するために45日超を要する理由とともに通知の上、その期間をさらに45日間延長することができる。
⑤費用	■ 事業者は、要求された情報を無料で提供しなければならない（事例7(3)、12(3)）。消費者からの要求に明らかに根拠がないか過度である場合、事業者は消費者に合理的な料金を課すか、要求に応じることを拒否できる。事業者は、検証可能な消費者要求が明らかに根拠のないまたは過度のものであることを証明する責任を負う。

© S&K Brussels LPC 2021

1. 知る権利
(2) 知る請求への対応義務
⑥本人確認（消費者請求の検証義務）、⑦請求を拒絶する場合

義務項目	内容
⑥本人確認（請求の検証義務）	■知る請求が事業者に対してなされた場合にも、原則として、事業者は直ちに対応義務を負うわけではなく、当該請求が検証可能なものであることが、事業者が知る請求への対応義務を負う要件とされている。 ■事業者は、知る請求または削除の請求を行う消費者が事業者による情報取得の対象の個人であることを検証する合理的な方法を定め、文書化し、遵守する。 ■消費者がアカウントを有していない場合、情報の性質に応じて、それぞれ**合理的な水準の確からしさ**（例：少なくとも消費者から提供される2つの情報が事業者が保有している情報と合致すること）と、**合理的に高い水準の確からしさ**（例：少なくとも消費者から提供される3つの情報が事業者が保有している情報と合致することに加えて所定の宣誓書が提供されること）が求められる。
⑦請求を拒絶する場合	■事業者は、ある消費者についての具体的な個人情報の開示を請求された場合に本人確認ができない場合には、請求者に対して具体的な個人情報を開示してはならず、また、本人確認ができない旨を請求者に伝えなければならない。 ■事業者は、ある消費者についての個人情報の種類の開示を請求された場合に本人確認ができない場合には、請求者に対して個人情報の種類の開示の請求を拒絶することができ、また、本人確認ができない旨を請求者に伝えなければならない。 ■連邦法もしくは州法との抵触またはCCPAに規定された例外を理由に具体的な個人情報の開示請求の全部または一部を拒絶する場合には、事業者は、請求者に対して拒絶理由を通知・説明しなければならない。

© S&K Brussels LPC 2021

1. 知る権利
(3) プライバシーポリシーの開示：①開示方法

- 事業者は、プライバシーポリシー等を通じて所定の事項を開示しなければならない。
- プライバシーポリシーは、事業者のウェブサイトまたはアプリのダウンロードもしくはランディングページ上の「privacy」という単語を用いた明確なリンクを通じて、オンラインで掲出されなければならない（但し、事業者がウェブサイトを運営していない場合には、オンラインで掲示することは求められていないが、消費者が明確に利用できるようにしなければならない。）。
- 少なくとも12か月に1回その情報をアップデートしなければならない。

S&K Brussels

© S&K Brussels LPC 2021

1. 知る権利
(3) プライバシーポリシーの開示：②記載事項（事例3(1)、5(1)、7(1)、12(2)、14(2)、19、20、21(1)、22(1)、24、25(1)、26）

記載事項（CCPA規則およびCPRA条文に基づき作成。CPRA規則によって異なる内容となる可能性がある）

- 過去12か月間に消費者について収集した個人情報の種類
- 個人情報の収集源の種類
- 個人情報の収集、売却または共有の事業上または商業目的
- 個人情報を開示する第三者の種類（売却、共有または事業目的で開示した個人情報の種類ごと）（事例4）
- 過去12か月間に第三者に売却または共有した消費者の個人情報の種類（売却または共有していない場合にはその旨）
- 過去12か月間に第三者に事業目的で開示した個人情報の種類（消費者の個人情報を事業目的で開示していない場合にはその旨）
- 事業者が16歳未満の消費者の個人情報を売却または共有しているとの現実の認識を有しているか否か
- 事業者が16歳未満の消費者の個人情報を売却または共有しているとの現実の認識を有している場合にはオプトイン権を行使するプロセスの説明
- 消費者に知る権利、削除請求権、訂正請求権、オプトアウト権、センシティブ個人情報の利用・開示の制限権および差別を受けない権利がある旨
- 検証可能な消費者の知る請求、削除請求または訂正請求の提出方法の指示、（もしあれば）オンライン上の請求フォームまたは請求のためのポータルへのリンク
- オプトアウト権の通知の内容、またはオプトアウトのページのリンク（事例13(2)）
- センシティブ個人情報の利用・開示の制限権の通知の内容、またはセンシティブ個人情報の利用・開示の制限のページ
- 消費者請求を確認するために用いる手続（消費者が提供しなければならない情報を含む）の一般的な説明
- 権利行使のための代理人を指定する方法の指示
- 最終更新日
- 連絡先
- 受領した知る請求、削除請求、訂正請求、オプトアウト請求、制限請求の件数およびそれらの請求に対する対応または拒絶の状況、ならびにそれらの請求に対して実質的に対応するまでに要する日数の中央値をまとめたマトリックス（年間1000万件以上の個人情報を購入し、商業目的で受領し、売却し、または商業目的で共有している場合に限る）

© S&K Brussels LPC 2021

1. 知る権利
(3) プライバシーポリシーの開示：②記載事項：「事業目的」

事業目的：事業者の経営上の目的またはその他の通知された目的のため、または第1798.185条第(a)項第(11)号に従って採択された規則で定義されているサービス提供者または契約受託者の業務上の目的のための個人情報の使用を意味する。ただし、当該使用が、個人情報が取得されもしくは処理される目的、または個人情報が取得された文脈と適合するその他の目的を実現するために合理的に必要であり、かつ、比例的である場合をいう。事業目的とは以下である。

(1)一意の訪問者に対する広告表示回数の計測、広告表示の位置と質の検証、ならびに当該仕様および他の基準への遵守の監査。
(2)消費者の個人情報の使用がその目的に対して合理的に必要であり、かつ比例的に行われる範囲で、セキュリティと完全性の確保を支援するため。
(3)既存の意図された機能を損なうエラーを特定および修復するためのデバッグ。
(4)消費者と事業者の進行中のやりとりの一部として示される個別化されていない広告を含むがこれに限定されない短期の一時的な使用（ただし、消費者の個人情報が第三者に開示されず、かつ、消費者についてのプロファイル作成またはその時のやりとり以外における消費者の経験のその他の改変に使用されない場合をいう。）
(5)事業者の代わりのサービスの実施（これには、事業者のためのアカウントの維持もしくは提供、カスタマー・サービスの提供、注文および取引の処理もしくは履行、顧客情報の検証、支払いの処理、解析サービスの提供、保管の提供、または類似サービスの提供を含む。）
(6)クロスコンテキスト行動広告を除く、広告およびマーケティングサービスを消費者に提供すること（ただし、広告およびマーケティングの目的で、サービス提供者または契約受託者が事業者からまたは事業者に代わって受け取るオプトアウトされた消費者の個人情報と、サービス提供者または契約受託者が他の者もしくは複数人から、または事業者に代わって受け取る個人情報を組み合わせたり、自らの消費者とのやりとりから取得したりしてはならない。）
(7)技術開発およびデモンストレーションについての内部的研究を行うこと。
(8)事業者により所有され、製造され、事業者のために製造され、または事業者により管理される、サービスまたはデバイスの品質または安全性を検証もしくは維持し、また、事業者により所有され、製造され、事業者のために製造され、または事業者により制御されるサービスまたはデバイスを改善、アップグレードまたは向上するための活動を行うこと。

© S&K Brussels LPC 2021

2. 削除請求権
削除請求への対応義務：①受領確認、②対応期限

消費者は、事業者に対し、その事業者が取得した自身に関する個人情報を削除するよう請求する権利を有する。	
①受領確認	受領から10営業日以内に受領確認を行うとともに、本人確認の手続と回答の見通し時期を消費者に伝える必要がある（事例6）。
②対応期限	■ 消費者から削除請求権を行使された事業者は、原則として、削除請求権を行使された日から45日以内にその消費者の個人情報を自身の記録から削除し、かつ、全てのサービス提供者または契約受託者に対してその消費者の個人情報をその記録から削除するよう通知し、事業者がそのような個人情報を売却したか、または共有したすべての第三者に対して、消費者情報の削除が不可能であるか不相応の努力を要する場合を除いて、これを削除するように通知する。 ■ 合理的に必要な場合には、請求の受領から45日以内に消費者に通知の上、その期間をさらに45日間延長することができる。 ■ 事業者は、削除請求を提出した消費者の個人情報が売却されないようにするため、法律を遵守するため、または本巻で認められる範囲内のその他の目的のためにのみ、削除請求の機密記録を保持することができる。

© S&K Brussels LPC 2021

2. 削除請求権
削除請求への対応義務:③本人確認、④削除請求への対応、⑤削除請求への回答

消費者は、事業者に対し、その事業者が取得した自身に関する個人情報を削除するよう請求する権利を有する。	
③本人確認	1. 知る権利(2) 知る請求への対応義務⑤本人確認(請求の検証義務)と同様。
④削除請求への対応	以下のいずれかの方法に基づく対応をとる必要がある。 ▪ 既存のシステム(アーカイブシステムおよびバックアップシステムを除く)に存在する当該個人情報を永久かつ完全に削除する。 ▪ 当該個人情報を非識別化する。 ▪ 当該消費者の情報を消費者情報集合体とする。
⑤削除請求への回答	事業者は、削除要求への回答に際して、削除請求に応じたか否かを消費者に知らせる必要がある。 ▪ 削除請求に応じる場合には、請求の記録を保持する旨を消費者に知らせる必要がある。 ▪ 削除請求を拒絶する場合には、消費者の請求に応じない旨と、法律で禁止されていない限り、その理由を消費者に通知する必要がある。事業者は、消費者の削除請求を拒絶する場合であって、かつ、消費者がまだオプトアウト請求を行っていない場合には、消費者に対し、個人情報の売却についてオプトアウトを希望するか確認するとともに、オプトアウトに係る通知の内容またはリンクをその回答に含めなければならない。

© S&K Brussels LPC 2021

2. 削除請求権
削除請求への対応義務：⑥例外要件

事業者または、事業者、別のサービス提供者、または契約受託者との契約に従い役割を担うサービス提供者もしくは契約受託者が、以下の目的のために、消費者の個人情報を保持する必要が合理的にある場合、その事業者、サービス提供者または契約受託者は、消費者の削除の請求に従うことは求められない。

(1)個人情報が取得された取引を完了する目的、保証書の、または連邦法に従い行われた製品のリコールの条件を満たすため、消費者から請求される、もしくは消費者との継続的なビジネス関係の文脈の中で消費者によって合理的に予想される、商品もしくはサービスを提供する目的、または、それ以外に事業者と消費者の間の契約を履行する目的。
(2)消費者の個人情報の利用がその目的に対して合理的に必要であり、かつ比例的に行われる範囲で、セキュリティと完全性の確保を支援する目的。
(3)既存の意図された機能を妨げる過誤を特定し、修復するためにデバッグする目的。
(4)表現の自由を行使し、他の消費者がその表現の自由に係る権利を行使する権利を確保し、または法律で定めるその他の権利を行使する目的。
(5)刑法第2部第12巻第3.6章（第1546条から開始）によるカリフォルニア電子通信プライバシー法を遵守する目的。
(6)他のすべての適用ある倫理およびプライバシー法を遵守した、またはこれに適合した、公共のまたは同領域の専門家の評価を受ける科学的、歴史的または統計的調査に従事する目的。ただし、事業者による情報の削除が、調査を完了する能力を不可能にする、または、著しく損なうおそれがある場合であって、消費者のインフォームド・コンセントがある場合に限る。
(7)消費者と事業者の関係に基づき、消費者の期待に合理的に適合した、かつその消費者が情報を提供した文脈に適合した内部での利用のみを可能にする目的。
(8)法的義務を遵守する目的。

S&K Brussels

© S&K Brussels LPC 2021

3. 訂正請求権
訂正請求への対応義務

- 消費者は、個人情報の性質および個人情報の処理の目的を考慮して、消費者についての不正確な個人情報を保持する事業者に対して、そのような不正確な個人情報を訂正するように請求する権利を有する。
- 不正確な個人情報を訂正するために検証可能な消費者請求を受領した事業者は、CPRA規則に従って、消費者によって指示される不正確な個人情報を訂正するための商業的に合理的な努力をする。

S&K Brussels

© S&K Brussels LPC 2021

4. 個人情報の売却または共有に対するオプトアウト権

オプトアウト手続：①オプトアウト権に関する通知（事例10(1)、15(1) 、16(2)）

消費者は、消費者の個人情報を第三者に売却または共有する事業者に対して、その消費者の個人情報を売却または共有しないように指示する権利を有する。

①オプトアウト権に関する通知	■ 個人情報の売却または共有に対する消費者のオプトアウト権の説明 ■ （個人情報を売却または共有している場合には）「Do Not Sell or Share My Personal Information」というタイトルページへの明示的なリンクを設けることを含む2つ以上の権利行使方法の用意（事例4(1)、18(1)、22(3)、23(1)、25(3)） ■ プライバシーポリシー等においてオプトアウト手続の説明と、そのタイトルページへのリンクを設けなければならない（事例11）。
「**売却**」の定義	金銭またはその他の価値のある対価のために、事業者が第三者に対して、消費者の個人情報を、売却し、賃貸し、公表し、開示し、広め、利用可能にさせ、転送し、または、その他口頭で、書面で、電子的もしくはその他の方法により伝えること。「売却」という語義から理解されるものよりも広い意味を有し、何らかビジネス上のメリットがある個人情報の移転については「金銭その他の価値ある対価のため」に個人情報を開示するものとして、広く「売却」に該当する可能性がある。
「**共有**」の定義	事業者がクロスコンテキスト行動広告のため、金銭またはその他の価値のある対価のためであるか否かにかかわらず、金銭が交換されない事業者の利益のためのクロスコンテキスト行動広告用の事業者と第三者との間の取引を含め、消費者の個人情報を第三者に、共有し、賃貸し、公表し、開示し、広め、利用可能にさせ、転送し、または、その他口頭で、書面で、電子的もしくはその他の方法により伝えること ■「**クロスコンテキスト行動広告**」：明確にブランド化された事業者のウェブサイト、アプリケーション、またはそれ以外の消費者が意図的にやりとりしている事業者のサービスから得られた消費者の個人情報に基づいて、消費者を対象として広告活動すること（例：消費者がインターネットで検索した内容に関連する商品について、当該消費者に特別に表示される広告）
「売却」および「共有」の例外	以下の場合はオプトアウト権の対象から除かれている。 (A)消費者の意図に従った第三者への移転、(B)オプトアウト権の行使があったことを知らせるための移転または消費者のセンシティブ個人情報の利用を制限した消費者の識別子を消費者のセンシティブ個人情報の利用を制限した事実を該当者に警告することを目的とした移転、(C)サービス提供者または契約受託者への移転、(D)M&Aに伴う移転

© S&K Brussels LPC 2021

4. 個人情報の売却または共有に対するオプトアウト権
オプトアウト手続：②オプトアウト権行使への対応

消費者は、消費者の個人情報を第三者に売却または共有する事業者に対して、その消費者の個人情報を売却または共有しないように指示する権利を有する。

対応期限	■ 消費者からオプトアウト権の行使を受けた事業者は、オプトアウト権の行使を受けた日から15営業日以内で、実務上可能な限り速やかにオプトアウト要求に対応しなければならない（事例17）。 ■ 具体的には、その消費者の個人情報の売却または共有を停止するとともに、オプトアウト権の行使を受けた後その消費者の個人情報の売却または共有を停止するまでの間に第三者に個人情報を売却または共有した場合には、当該第三者に対してオプトアウト権が行使された事実と、当該個人情報の売却または共有の停止を通知しなければならない。 ■ 同様にサービス提供者も事業者に代わって個人情報を売却または共有することはできなくなる。 ■ 事業者は、その後最低12か月間は、その消費者に個人情報の売却または共有の承認を要請することができない。 　■ 売却の承認は、消費者がオプトインの請求を行い、その後オプトインの選択を確認する仕組みであるダブル・オプトインの仕組みが採用されており、共有の承認についても同様となるものと考えられる。 ■ オプトアウト請求への対応にあたっては本人確認は要求されない（事例23(2)）。

© S&K Brussels LPC 2021

5. 未成年者のオプトイン権

未成年者についてのオプトイン手続

- 事業者が消費者が16歳未満であるという認識を実際に有していた場合、その事業者は、消費者が13歳以上16歳未満の場合には当該消費者自身が、または消費者が13歳未満の場合には当該消費者の親または保護者が、積極的に消費者の個人情報の売却または共有を認めていない限りは、消費者の個人情報を売却または共有しない（事例15(2)）。
- 消費者の年齢を意図的に無視する事業者は、その消費者の年齢について認識していたとみなされるため、16歳未満の者の個人情報を売却または共有する可能性がある事業者は、どのように年齢を確認するかを検討する必要がある。
- 未成年者の個人情報の場合にその未成年者である消費者の個人情報を売却または共有する同意を得ていない事業者は、消費者がその後にその個人情報の売却または共有について同意する場合を除き、消費者の個人情報を売却または共有することが禁止される。
  - 「**同意**」：消費者が自由に与えた具体的な情報に基づく明確な意思表示であり、消費者もしくはその法定後見人、代理権を持つ者、または消費者の後見人として行動する者が、声明または明確な肯定的行動によって、狭く定義された特定の目的のために自分に関連する個人情報を処理することに合意すること
    - 個人情報の処理に関する記述を含む一般的または広範な利用規約またはそれに類する文書を、他の無関係な情報と一緒に受諾しても、同意とはならない。
    - コンテンツの上にカーソルを置いたり、ミュートしたり、一時停止したり、閉じたりしても、同意とはならない。
    - ダークパターンを利用して得られた同意は、同意とはならない。
    - 「**ダークパターン**」：ユーザーの自主性、意思決定、または選択を妨害したり、損なわせたりする実質的な効果を持つように設計または操作されたユーザーインターフェース（CPRA規則によってさらに定義される）

S&K Brussels

© S&K Brussels LPC 2021

6. センシティブ個人情報の利用・開示の制限権

- 消費者についてのセンシティブ個人情報を取得する事業者に対して、いつでもセンシティブ個人情報の利用を以下の範囲に制限するよう指示する権利を有する。
  - A) サービスまたは商品を求める平均的な消費者によって合理的に求められる当該サービスまたは商品を提供するため
  - B) 以下のサービスを実施するために必要な範囲
    - 消費者の個人情報の利用がその目的に対して合理的に必要であり、かつ比例的に行われる範囲で、セキュリティと完全性の確保を支援するため。
    - 消費者と事業者の進行中のやりとりの一部として示される個別化されていない広告を含むがこれに限定されない短期の一時的な利用（ただし、消費者の個人情報が第三者に開示されず、かつ、消費者についてのプロファイル作成またはその時のやりとり以外における消費者の経験のその他の改変に利用されない場合をいう。）
    - 事業者の代わりのサービスの実施（これには、事業者のためのアカウントの維持もしくは提供、カスタマーサービスの提供、注文および取引の処理もしくは履行、顧客情報の検証、支払いの処理、解析サービスの提供、保管の提供、または類似サービスの提供を含む。）
    - 事業者により所有され、製造され、事業者のために製造され、または事業者により管理される、サービスまたはデバイスの品質または安全性を検証もしくは維持し、また、事業者により所有され、製造され、事業者のために製造され、または事業者により制御されるサービスまたはデバイスを改善、アップグレードまたは向上するための活動を行うこと。
  - C) CPRA規則によって認められる範囲

S&K Brussels

© S&K Brussels LPC 2021

6. センシティブ個人情報の利用・開示の制限権

- 事業者は、前ページのA)、B)およびC)によって認められる場合を除いて、消費者から、消費者のセンシティブ個人情報を利用しない、または開示しないように指示を受けた場合、消費者がその後追加的な目的のための消費者のセンシティブ個人情報の利用または開示に対する同意を提供しない限り、消費者からの指示を受領した後、その他の目的で消費者のセンシティブ個人情報を利用または開示することを禁止される。
- 「**センシティブ個人情報**」: 以下の1.から4.の個人情報
  1. 以下の情報を明らかにする個人情報
     - ソーシャルセキュリティ番号、運転免許証番号、州IDカード番号、パスポート番号、
     - アカウントへのアクセスを可能とするセキュリティ・コード若しくはアクセス・コード、パスワード、又は認証情報と組み合わせられた、アカウント・ログイン情報、金融機関口座情報、デビットカード情報、クレジットカード情報
     - 正確な位置情報
     - 人種的または民族的起源、宗教または哲学上の信念、労働組合への加入状況
     - 郵便・電子メール・テキストメッセージの内容（事業者がこれらの通信の受信者として意図されている場合を除く）
     - 遺伝データ
  2. 消費者を一意的に識別することを目的としたバイオメトリック情報の処理
  3. 消費者の健康に関連して収集および分析された個人情報
  4. 消費者の性的生活や性的指向に関連して収集および分析された個人情報

S&K Brussels

© S&K Brussels LPC 2021

7. 権利行使を理由として差別されない権利

義務	内容
①権利行使を理由とする差別の禁止	■ 事業者は、消費者がCCPA上の消費者の権利を行使したことを理由として消費者を差別しない（以下を含むがこれに限られない。）。 ■ 消費者に対する商品またはサービスの提供の拒否。 ■ ディスカウントもしくはその他の特典の利用、またはペナルティを課すことを含め、商品またはサービスに異なった価格または料金を請求すること ■ その消費者に対して異なったレベルまたは質の商品またはサービスを提供すること。 ■ 異なる価格もしくは料金の商品もしくはサービス、またはレベルもしくは質の商品もしくはサービスを消費者が受領することを示唆すること。 ■ 従業員、求職者、または独立契約受託者に対して、本巻に基づく権利を行使したことを理由として報復行為を行うこと。 ■ 提供される商品またはサービスの価格またはレベルの違いが消費者のデータにより事業者に提供される価値に合理的に関連している場合に、事業者が消費者に異なる価格もしくは料金を請求すること、または消費者に異なるレベルもしくは質の商品もしくはサービスを提供することを禁止するものではない。 ■ 事業者がロイヤルティ、報酬、上位機能、割引、またはクラブカードプログラムを提供することを禁止するものではない。
②個人情報の取得等への金銭的なインセンティブの付与	■ 事業者は、個人情報の取得、個人情報の売却・共有、または個人情報の保管について、消費者に対する補償としての支払いを含む金銭的インセンティブを申し出ることができる。事業者は、価格または相違が消費者のデータにより事業者に提供される価値と合理的に関連している場合、消費者に対して商品またはサービスの異なる価格、料金、レベルまたは品質を申し出ることもできる。 ■ 事業者は、消費者が、金銭的インセンティブ・プログラムの重要な条件を明確に述べ、かつ、消費者によりいつでも撤回されることができ、事前のオプトインの同意を与えた場合にのみ、消費者に対し金銭的インセンティブを実施する（事例8）。 ■ 消費者がオプトイン同意を提供することを拒否した場合、事業者は、次回消費者にオプトインの同意を提供することを請求するまで最低12か月間、またはCPRA規則によって規定されるまで待つものとする。

© S&K Brussels LPC 2021

8. 全般：①売却先・共有先である第三者、個人情報の開示先であるサービス提供者・契約受託者との契約締結義務（個人情報を開示する場合の責任の移転）

- 消費者の個人情報を取得し、それを第三者に売却したり、第三者と共有したりする事業者、または事業目的のためにサービス提供者または契約受託者に個人情報を開示する事業者は、当該第三者、サービス提供者、または契約受託者と以下の通りに契約を締結する必要がある。
  - (1)個人情報が、制限的かつ特定の目的のためにのみ、事業者によって売却または開示されることを明記する。
  - (2)本巻に基づく該当する義務を遵守するように第三者、サービス提供者または契約受託者に義務付け、また当該者に対し、本巻で要求されるものと同レベルのプライバシー保護を提供することを義務付ける。
  - (3)第三者、サービス提供者または契約受託者が、本巻に基づく事業者の義務と整合する方法で移転された個人情報を使用することを確保するために、合理的かつ適切な措置を講じる権利を事業者に付与する。
  - (4)本巻に基づく義務をもはや達成できないと第三者、サービス提供者または契約受託者が判断した場合には、事業者に通知することを義務付ける。
  - (5)前記(4)号に基づくものを含む、個人情報の無権限での使用を阻止し、是正するための合理的かつ適切な措置を、通知の上で講じる権利を事業者に付与する。

S&K Brussels

© S&K Brussels LPC 2021

8. 全般：①売却先・共有先である第三者、個人情報の開示先であるサービス提供者・契約受託者との契約締結義務（サービス提供者・契約受託者の要件）

事業者が他の者に個人情報を開示する場合、開示先がCCPA/CPRAに違反して個人情報を利用した場合の責任の所在が問題となり得る。事業者は、その開示先との間で契約を締結することにより、開示先を第三者ではなく、サービス提供者か契約受託者に位置付けることができれば、開示先がCCPA/CPRA違反を行う意図があることを事業者が実際に認識しているか、または認識すべき理由がある場合を除き、開示先のCCPA/CPRAに規定する制限に違反する個人情報の利用について責任を負わない（事例2、5(2)）。

概念	定義
「第三者」	以下のいずれでもない者を意味する。 ■ (1)本巻のもとで消費者が意図的にやりとりし、かつ、消費者と事業者の進行中のやりとりの一部として消費者から個人情報を取得する事業者。 ■「意図的なやりとり」：複数の意図的なやりとりを介して、消費者が該当者のウェブサイトを訪問したり、該当者から商品やサービスを購入したりするなど、該当者とやりとりしたり、該当者に個人情報を開示したりしようとする場合（コンテンツの上にカーソルを置いたり、ミュートしたり、一時停止したり、閉じたりしても、消費者が個人とやりとりしようとしていることにはならない。） ■ (2)事業者へのサービス提供者、または ■ (3)契約受託者
「サービス提供者」	事業者に代わって個人情報を処理し、かつ、事業目的のために書面の契約により事業者からまたは事業者に代わって受領する消費者の個人情報を処理する者を意味し、次ページの事項を事業者との契約により禁止する場合 ▪ 定義から営利性の要件が削除されたため、非営利団体も「サービス提供者」に該当し得る。
「契約受託者」	事業者との書面による契約に基づき、事業者が事業目的のために消費者の個人情報を利用できるようにする者であって、当該契約が次ページの各事項の要件を満たす場合

© S&K Brussels LPC 2021

8. 全般：①売却先・共有先である第三者、個人情報の開示先であるサービス提供者・契約受託者との契約締結義務（サービス提供者・契約受託者の要件）

サービス提供者の要件の一部である契約の要件	契約受託者の要件の一部である契約の要件
事業者との契約により、以下を禁止する。人が、	当該契約は(A)契約受託者が以下を行うことを禁止する。
(A)個人情報を売却しまたは共有し、	(i)個人情報を売却または共有すること。
(B)当該契約で事業目的以外の目的のために、個人情報を保持し、使用しまたは開示すること（事業者との契約またはその他本巻で認められたものによって事業目的以外の商業目的のために個人情報を保持し、使用しまたは開示することを含む）	(ii)契約で定められた事業目的以外の目的のために個人情報を保持、使用、または開示すること（それには、契約で定められた、または本巻で許可されている事業目的以外の商業目的のために個人情報を保持、使用、または開示することを含む。
(C)サービス提供者および事業者との直接の事業関係外の情報を保持し、使用し、または開示し、もしくは	(iii)契約受託者と事業者との直接的な取引関係以外で、情報を保持、使用、または開示すること、もしくは
(D)事業者からまたは事業者に代わってサービス提供者が受領する個人情報、別の者からまたは別の者に代わって受領する個人情報を組み合わせること、または消費者とのやりとりから取得することを含む。	(iv)契約受託者が事業者との書面による契約に基づき受領した個人情報と、契約受託者が他の者もしくは複数人から、または事業者に代わって受け取る個人情報を組み合わせたり、自らの消費者とのやりとりから取得したりすること。
ただし、サービス提供者が、第1798.185条第(a)項第(10)号により採用される規則で定められた事業目的を行うために個人情報を組み合わせることができる場合とするが、本条第(e)項第(6)号によるものおよびカリフォルニアプライバシー保護局により採用された規則を除く。	ただし、契約受託者は本条第(e)項第(6)号およびカリフォルニア州プライバシー保護局によって採択された規則に規定されている場合を除き、第1798.185条第(a)項第(10)号に従って採択された規則に定義されている事業目的を実行するために個人情報を組み合わせることができる。
N/A	(B)契約受託者が(A)の制限事項を理解し、それを遵守するという契約受託者が作成した証明書を含む。
この契約は、サービス提供者との合意に基づき、事業者が、少なくとも12か月に1回、手動による継続的見直しや自動スキャン、定期的な評価、監査、その他の技術的および運用的テストを含むがこれらに限らない対策を通じて、サービス提供者の契約への準拠を監視することを許可することができる。	(C)契約受託者との合意に基づき、事業者が、少なくとも12か月に1回、手動による継続的見直しや自動スキャン、定期的な評価、監査、その他の技術的および運用的テストを含むがこれらに限らない対策を通じて、契約受託者の契約への準拠を監視することを許可する。

© S&K Brussels LPC 2021

8. 全般：②研修義務 / ③記録管理義務

■ 以下の義務はいずれもCCPA規則において規定されたものであり、CPRAにおける義務がどのようなものとなるかはCPRA規則の内容による。

事業者の義務	内容
②研修義務	事業者のプライバシープラクティスまたは事業者による CCPA の遵守に関する消費者からの問い合わせを担当する全ての者は、CCPA ならびに本規則内の要件および CCPA ならびに本規則のもとで消費者が権利行使するためにどのように案内するかについて知識を持っておかなければならない。
③記録管理義務	▪ 事業者は CCPA による消費者請求および事業者が当該請求にどのように対応したかについての記録を少なくとも 24 ヶ月間保持しなければならない。記録は、チケットまたはログのフォーマットで保持することができる。 ▪ ただし、チケットまたはログに請求の日、請求の性質、請求がなされた方法、事業者が請求に対応した日、対応の性質、ならびに請求が全部または一部拒否された場合は拒否の根拠が含まれる場合に限る。

S&K Brussels

© S&K Brussels LPC 2021

8. 全般：④個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務

- 消費者の個人情報を取得する事業者は、第1798.81.5条に従って、個人情報の無権限または違法なアクセス、破壊、利用、改変、または開示から個人情報を保護するために、個人情報の性質に適した合理的なセキュリティ手続きおよびプラクティスを実施するものとする。
  - 2016年2月に公表された”California Data Breach Report 2012-2015”（https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ）30頁においてカリフォルニア州の当時の司法長官（現・米副大統領Kamala D. Harris氏）は20の「CISコントロール」を「合理的なセキュリティ」の最低限の基準と述べている。
- また、Section 1798.150の「私的訴訟権」条項は、合理的なセキュリティ手順および慣行を実施し、維持するための事業者の義務を示している（近時のCCPA上の私的訴訟権に基づく訴訟の動向は、「参考資料④：CCPA訴訟の動向」を御参照）。

S&K Brussels

© S&K Brussels LPC 2021

8. 全般：⑤データ保護影響評価の実行義務

- 消費者の個人情報の処理が消費者のプライバシーやセキュリティに重大なリスクをもたらす事業者に以下のことを請求する規則を定めている。
  1. サイバーセキュリティ監査を年1回実施する。
  2. 個人情報の処理に関するリスク評価をCPPAに提出する。
     - これには、処理にセンシティブ個人情報が含まれているかどうか、および処理から得られる利益を特定し、また当該処理に対する潜在的リスクと当該利益を比較検討する。これは当該処理を制限または禁止することを目的とする。
     - 但し、消費者のプライバシーへのリスクが処理の結果として消費者、事業者、他の利害関係者、および一般人への利益を上回る場合とする。

S&K Brussels

© S&K Brussels LPC 2021

II. CPRA vs VCDPA & CPA

© S&K Brussels LPC 2021

施行日程・適用範囲(「事業者」/「管理者」の定義)

	カリフォルニアプライバシー権利法(CPRA: California Privacy Rights Act)	バージニア消費者データ保護法(VCDPA: Virginia Consumer Data Protection Act)	コロラドプライバシー法(CPA: Colorado Privacy Act)
施行日	2023年1月1日	2023年1月1日	2023年7月1日
適用範囲(「事業者」/「管理者」の定義)	「事業者」:カリフォルニア州で事業を行う営利団体で、消費者の個人情報を収集または処理し、次のしきい値の1つを満たす者 1. 前年の年間総収益が2500万ドルを超えている。 2. 毎年、10万人以上の消費者または世帯の個人情報を購入、売却、または共有している。 3. 消費者の個人情報の売却または共有から年間収益の50%以上を得ている。	「管理者」:バージニア州で事業を行ったり、バージニア州の住民を対象とした製品やサービスを製造し、かつ以下に該当する者 1. 年間10万人以上の消費者の個人データを管理または処理する。 2. 年間2万5,000人以上の消費者の個人データを管理または処理し、個人データの売却による収益が総収益の50%を超えている。	「管理者」:コロラド州で事業を行っている、またはコロラド州の住民を意図的に対象として商品もしくはサービスを製造もしくは提供している管理者で、以下を満たす者 1. 1年間に10万人以上の消費者の個人データを管理または処理している 2. 個人データの売却から収益を得たり、商品またはサービスの価格の割引を受けたりし、かつ2万5,000人以上の消費者の個人データを処理または管理している。
非営利組織	「事業者」には含まれないが、「サービス提供者」、「契約受託者」または「第三者」に該当する限度で規制対象となる。	VCDPAの適用を受けない。	「管理者」に該当し得る。

© S&K Brussels LPC 2021

適用範囲(「消費者」の定義)

	CPRA	VCDPA	CPA
「消費者」	2017年9月1日時点におけるカリフォルニア州の規則(Code of Regulations)第18巻の第17014条において定義されたカリフォルニア州の住民である自然人	個人又は世帯の文脈でのみ行動する、バージニア州の住民である自然人	個人又は世帯の文脈でのみ行動する、コロラド州の住民である自然人
「役職員等の雇用関連個人情報」および「取引先の従業員の個人情報」への適用の有無	■ 事業者の役職員等や取引先の従業員はいずれも「消費者」から除外されていない。**したがって、役職員等の雇用関連個人情報および取引先の従業員の個人情報はいずれもCPRAの適用対象となる。** ■ いずれの個人情報も2023年1月1日までCPRA一部規定の適用猶予の対象となっている。 ■ 詳細は「参考資料②:BtoB企業が収集している個人情報とCPRAの適用関係」を御参照。	■ 商業上又は雇用の文脈で行動する自然人は、「消費者」から除外されている。 ■ 従業員等の個人データやB to B の文脈で得た取引先担当者の個人データは、VCDPA の対象からは外れる。	■ 商業上又は雇用の文脈で行動する自然人は、「消費者」から除外されている。 ■ 従業員等の個人データや B to B の文脈で得た個人データは CPA の適用対象外となる。

© S&K Brussels LPC 2021

執行と制裁：司法長官による執行

CPRA	VCDPA	CPA
■ 事業者、サービス提供者、契約受託者またはその他の者は、各違反に対して差止命令および$2,500以下、または意図的な違反および未成年者の消費者の個人情報に関する違反ごとに$7,500ドル以下の民事制裁金を科される。 ■ 2023年1月1日以降、治癒期間が保証されないこととなった。カリフォルニア州司法長官オフィスによって公表された27の執行事例はいずれも民事制裁金の賦課には至っていないものの、同日以降は民事制裁金の賦課につながりうることを意味する（「参考資料①：カリフォルニア州司法長官によるCCPA執行事例」を御参照）。	■ 司法長官には、VCDPAの違反を実施する調査権限および排他的な権限がある。司法長官は、措置を開始する前に、申し立てられた違反を是正するための30日間の期間を管理者または処理者に提供する必要がある。 ■ 管理者または処理者が申し立てられた違反を是正しなければ、司法長官は措置を開始し、各違反につき差止命令および最高$7,500の民事制裁金が科される可能性がある。 ■ 司法長官は、調査と準備の費用で負担した費用（弁護士費用を含む）について、合理的な費用の返還を受けることができる。	■ 司法長官および地方検事には、CPAを実施する排他的な権限がある。実施は、州の名においてまたは州の居住者に代わって行われる。司法長官は、2025年1月1日に失効する終了条項に基づき、措置を開始する前に、申し立てられた違反を是正するための60日間の期間を管理者または処理者に提供する必要がある。2025年1月1日以降は、是正期間は提供されない。 ■ CPAへの違反は、欺瞞的な取引慣行を構成するため、コロラド州消費者保護法に従って違反1件につき$20,000の罰金が科される。

© S&K Brussels LPC 2021

執行と制裁

	CPRA	VCDPA	CPA
行政執行	CPRAに違反する事業者、サービス提供者、契約受託者またはその他の者は、各違反に対して$2,500以下、または意図的な違反および、16歳未満であることを事業者、サービス提供者、契約受託者またはその他の者が知っていた消費者の個人情報に関する違反ごとに$7,500ドル以下の罰金がCPPAによる行政執行措置により科される。CPPAに関しては「IV. CPRAによるカリフォルニアプライバシー保護局（CPPA: California Privacy Protection Agency）の創設」を御参照。	×	×
私的請求権	■ 合理的なセキュリティ手順と慣行を実施し維持する義務に事業者が違反した結果として、カリフォルニア州のデータ侵害法の、Section1798.81.5(d)(1)(A)に定める、自身の暗号化されておらず、かつ修正されていない個人情報、もしくはパスワードまたはセキュリティ上の質問との組み合わせの電子メールアドレスおよびそのアカウントへのアクセスが許可される返答が、無権限アクセス、流出、窃取または開示の対象となった消費者は、違反1件につき消費者1人あたり$100以上$750以下または実際の損害額のいずれか大きい方の金額で損害賠償を求めるため、差止命令による救済または宣言的救済、もしくは裁判所が適切と判断するその他の救済を求めるため、民事訴訟を提起することができる。 ■ 法定損害賠償のための訴訟では、消費者は申し立ての違反について事業者に30日前の書面による通知を提供することが要求され、申し立ての違反が是正された場合、個々の法定損害のための訴訟を提起することはできないが、データ侵害後の合理的セキュリティ手続・慣行の実施及び維持が当該データ侵害に関して「治癒」を構成しないことを明確化した。	×	×

© S&K Brussels LPC 2021

消費者の権利

CPRA	VCDPA	CPA
1. 知る権利（データポータビリティの権利を含む）	○ 知る権利（管理者が消費者の個人データを処理しているかどうかを知る権利）、アクセス権（管理者が処理した個人データにアクセスする権利）、データポータビリティの権利	○ アクセス権（消費者は、管理者が消費者に関する個人データを処理しているかどうかを確認し、そのようなデータにアクセスする権利）
2. 削除請求権	○	○
3. 訂正請求権	○	○
4. 個人情報の売却または共有に対するオプトアウト権	○ ターゲット広告、個人データの売却またはプロファイリングをオプトアウトする権利	○ ターゲット広告、個人データの売却、またはプロファイリングをユニバーサルオプトアウトメカニズムによりオプトアウトする権利
5. 未成年者のオプトイン権	○ COPPAの検証可能な保護者の同意要件に準拠している管理者および処理者は、VCDPAに基づく保護者の同意を得る義務に準拠しているとみなされる。既知の子供の親または法的保護者は、その子供に属する個人データの処理に関して、子供に代わって消費者の権利を発動することができる。	○ 管理者は、最初に子供の親または法的保護者から同意を得ない限り、既知の子供の個人データを処理してはならない。
6. センシティブ個人情報の利用・開示の制限権	○ 管理者は、消費者の同意を得ることなくセンシティブデータを処理することは禁止されており、既知の子供に関するセンシティブなデータを処理する場合は、児童オンラインプライバシー保護法に準拠しなければならない。	○ 管理者は、消費者の同意を得ない限り、消費者のセンシティブなデータを処理しないものとする。
7. 権利行使を理由として差別されない権利	○ 管理者は州および連邦消費者差別禁止法に違反して個人データを処理したり、VCDPAに基づく権利の行使を理由として消費者を差別してはならない。消費者がオプトアウトする権利を行使した場合、または提供が消費者による真のロイヤルティ、報酬、プレミアム機能、割引、またはクラブカードプログラムへの自発的な参加に関連している場合は、管理者は（無料提供を含む）異なる価格、料金、レベル、品質、選択の商品やサービスを提供することを妨げられない。	○ 管理者は、個人データを、消費者に対する違法な差別を禁止する州法または連邦法に違反して処理しない。

© S&K Brussels LPC 2021

事業者の義務：1. 知る権利(2) 知る請求への対応義務

CPRA	VCDPA	CPA
②知る権利の対応方法	▪ 管理者は、消費者が権利行使の要求を提出するための1つ以上の安全で信頼性の高い方法をプライバシー通知に記載しなければならない。 ▪ 使用する方法では、消費者が通常どのように管理者とやり取りするか、かかる要求の安全で信頼性の高い通信の必要性、および要求を認証する管理者の能力を考慮する必要がある。 ▪ 管理者は、消費者が権利を行使するために新しいアカウントを作成することは求めてはならないが、既存のアカウントを使用するように消費者に要求することができる。	▪ 消費者は、プライバシー通知に記載されている方法で要求を送信することで、権利を行使することができる。方法では次の点を考慮する必要がある。 ▪ (1)消費者が通常管理者とやり取りする方法 ▪ (2)要求に関する安全で信頼性の高い通信の必要性 ▪ (3)要求を行う消費者の身元を認証する管理者の能力。 ▪ 管理者は消費者が権利を行使するために新しいアカウントを作成することは求めてはならない。ただし、管理者は、消費者に既存のアカウントを使用するよう求めることができる。
④対応期限	▪ 管理者は、45日以内に消費者要求に対応する必要がある。 ▪ 特定の要件が満たされている場合、この期間は一回だけさらに45日延長することができる。	▪ 管理者は要求に対するあらゆる対応について、45日以内に消費者に知らせるものとする。 ▪ 特定の状況では、この45日間の回答期間はさらに45日間延長することができる。

S&K Brussels

© S&K Brussels LPC 2021

事業者の義務：1. 知る権利(2) 知る請求への対応義務

CPRA	VCDPA	CPA
⑤費用	▪ 管理者は、1人の消費者につき年間最大2回まで、消費者の要求に応じて情報を無料で提供する必要がある。 ▪ 管理者は、消費者からの要求に明らかに根拠がないか、過度の、または繰り返しである場合、消費者に合理的な料金を課すか要求に応じることを拒否することができるが、要求に明確な根拠がなく、過度であり、または繰り返しの性質であることを立証する責任は管理者にあるものとする。	▪ 管理者は、要求された情報を年1回無料で提供する。12か月以内に追加の要求がある場合は、管理者は追加料金を請求することができる。
⑦請求を拒絶する場合	▪ 管理者が消費者要求への対応を拒否する場合、管理者は要求を受領してから45日以内に理由と決定に不服を申し立てる方法についての指示を消費者に知らせるものとする。 ▪ 管理者が商業的に合理的な努力を払っても要求を認証できない場合、管理者は措置を開始する要求に従う必要はなく、消費者および消費者の要求を認証するために合理的に必要な追加情報を要求することができる。 ▪ 管理者は、要求への対応を拒否したことに対する消費者の不服申し立てのプロセスと、申し立てが拒否された場合に、消費者が司法長官に連絡して苦情を提出するためのオンラインでの仕組みか他の方法を確立する必要がある。	▪ 管理者が消費者要求への対応を拒否する場合、管理者は要求を受領してから45日以内に理由と決定に不服を申し立てる方法についての指示を消費者に知らせるものとする。 ▪ 管理者が商業的に合理的な努力を払っても要求を認証できない場合、管理者は消費者の権利行使の要求に従う必要はなく、要求を認証するために合理的に必要な追加情報の提供を要求することができる。 ▪ 管理者は、消費者要求への対応を拒否したことに対して消費者が不服申し立てを行う内部プロセスを確立する必要がある。消費者が不服を申し立てたい場合、消費者は管理者が要求の拒否を通知した後、合理的な期間内に行う必要がある。不服申し立てのプロセスは明示的で使いやすいものでなければならない。 ▪ 管理者は不服申し立ての受領後45日以内に不服申し立ての結果を消費者に知らせ、その根拠となる理由を説明した文書を提供する。特定の状況ではこの45日間の期間はさらに60日延長することができる。

© S&K Brussels LPC 2021

事業者の義務

CPRA	VCDPA	CPA
1. 知る権利 (3) プライバシーポリシーの開示	管理者は、以下の事項を含む、合理的にアクセス可能で、明確で、意味のあるプライバシー通知を消費者に提供する必要がある。 (1)管理者が処理する個人データの種類 (2)個人データの処理の目的 (3)管理者の決定への不服申立を含む消費者の権利を行使する方法、 (4)第三者と共有する個人データの種類 (5)管理者が個人データを共有する第三者の種類	管理者は、以下を含む、合理的にアクセス可能で、明確で、意味のあるプライバシー通知を消費者に提供する必要がある。 (1)管理者または処理者が収集または処理する個人データの種類 (2)個人データの種類を処理する目的 (3)消費者が権利を行使しうる方法および場所 (4)管理者が第三者と共有する個人データの種類 (5)管理者が個人データを共有する第三者の種類
4. 個人情報の売却または共有に対するオプトアウト権：オプトアウト手続	管理者が個人データを第三者に売却する場合、またはターゲット広告のために処理する場合に、開示が必要である	管理者が第三者に個人データを売却したり、ターゲット広告のために個人データを処理したりする場合、管理者はそのような売却または処理を明示的に開示し、消費者がオプトアウトできる方法も開示するものとする。

S&K Brussels

© S&K Brussels LPC 2021

事業者の義務：8. 全般：①売却先・共有先である第三者、個人情報の開示先であるサービス提供者・契約受託者との契約締結義務（個人情報を開示する場合の責任の移転）

VCDPA	CPA
▪ 処理者は、管理者の指示に従い、管理者がその義務を果たすのを支援する必要がある。 ▪ 処理者のデータ処理手順を管理するため、管理者とデータ処理者間で契約を結ぶ必要がある。また、この契約では処理者に以下のことを要求する。 1. 個人データを処理する者がそれぞれ機密保持義務を負うことを確保する。 2. 保持が法律で義務付けられている場合を除き、管理者の指示に従って、サービスの提供後に要求に応じてすべての個人データを削除するか、管理者に返却する。 3. 管理者の要求に応じて、処理者がCDPAの義務を遵守していることを示すために必要なすべての情報を管理者に提供する。 4. 管理者による合理的な評価を許可し、これに協力するか、資格のある独立した評価者が、処理者のポリシーや技術的および組織的な措置の評価を行うよう手配し、管理者の要求に応じて当該評価の報告書を提出する。 5. 契約受託者に対し、書面による契約に従い、個人データに関する処理者の義務を果たすように要求する。 6. ある者が管理者または処理者のいずれとして機能しているかについての判断は、個人データを処理する文脈に応じた事実に基づく。個人データの特定の処理に関して管理者の指示に準拠し続ける処理者は、処理者であり続ける。	▪ 処理者は、管理者の指示に従い、管理者がその義務を果たすのを以下の方法によって支援する必要がある。（1）消費者の権利行使要求に管理者が対応するのを支援するための適切な措置を講じる。（2）違反通知およびシステムセキュリティに関連して管理者がセキュリティ義務を果たすのを支援する。（3）管理者が必要な保護評価を実施および文書化できるようにするため、必要とする情報を管理者に提供する。 ▪ さらに、処理者による処理は、処理者と管理者間の次のことを規定する拘束力のある契約によって規律される必要がある。 1. 処理の性質と目的を含む、処理者に適用される指示。 2. 処理期間と処理対象の個人データの種類。 3. 個人データを処理する者がそれぞれ、データに関して機密保持義務を負うという要件。 4. 管理者が契約受託者を使用するのは、当該契約受託者にデータに関する処理者の義務を満たすように要求する契約に基づく場合のみとするという要件。また、処理者は、管理者に異議を唱える機会を提供しなければならない。 5. 適切なセキュリティの確保のために技術的および組織的対策を維持するための、管理者と処理者間の責任の割り当て。 6. 個人データの保持が法律で義務付けられている場合を除き、管理者が、処理者にサービスの提供終了時にすべての個人データを削除または返却することを要求するかどうか。 7. 処理者はこの法律を遵守していることを示すために必要なすべての情報を管理者に提供するという定め。 8. 処理者は、管理者または監査人による合理的な監査および検査を許可し、これに貢献するものとする。

© S&K Brussels LPC 2021

事業者の義務:8. 全般:⑤データ保護影響評価の実行義務

CPRA	VCDPA	CPA
▪ 消費者の個人情報の処理が消費者のプライバシーやセキュリティに重大なリスクをもたらす事業者に以下のことを請求する規則を定めている。 1. サイバーセキュリティ監査を年1回実施する。 2. 個人情報の処理に関するリスク評価をCPPAに提出する。 ▪ これには、処理にセンシティブ個人情報が含まれているかどうか、および処理から得られる利益を特定し、また当該処理に対する潜在的リスクと当該利益を比較検討する。これは当該処理を制限または禁止することを目的とする。 ▪ 但し、消費者のプライバシーへのリスクが処理の結果として消費者、事業者、他の利害関係者、および一般人への利益を上回る場合とする。	▪ 管理者は、個人データに関する以下の各処理活動のデータ保護影響評価を実施し、文書化する必要があ (1) ターゲット広告 (2) 個人データの売却 (3) 特定の状況でのプロファイリング (4) センシティブなデータ (5) 消費者に害を及ぼすリスクが高い処理活動 ▪ VCDPAでは、データ保護影響評価の要件に関してさらに詳しい情報が記載されている。 ▪ 司法長官は、遵守に関する管理者のデータ保護影響評価を要求し、評価することができる。	▪ 管理者は、害を及ぼすリスクが高い処理活動を実行する際に、データ保護影響評価を実施する必要がある。消費者に「害を及ぼすリスクが高い」処理には、次のようなものがある。 1. プロファイリングが以下のリスクをもたらすターゲット広告 a. 消費者に対する不公平または欺瞞的な扱い、不当に異なる影響 b. 消費者への金銭的または物理的な損害 c. 合理的な人にとって気分を害するものであるような、消費者の孤立もしくは隔離状態、または私的な事情もしくは関心事への侵入 d. 消費者へのその他の実質的な損害 2. 個人データの売却 3. センシティブなデータの処理 ▪ 管理者は、データ保護影響評価を要求に応じて司法長官に提供する必要がある。司法長官は遵守のための当該評価を評価することができる。

© S&K Brussels LPC 2021

III. CPRA vs EU GDPR

© S&K Brussels LPC 2021

米国国内の事業者にGDPRが直接適用される場面（域外適用）

【EEA域外（米国内）】　　【EEA域内】

EEA域内に所在するデータ主体に対する商品またはサービスの提供に関連して行われる個人データの処理

■ メールマガジンを配信するため、氏名・メールアドレス等を管理

EEA域内で行われるデータ主体の行動のモニタリングに関連して行われる個人データの処理

■ Webサイト上からクッキー情報を取得して個人の嗜好等を分析して行動ターゲティング広告を配信

事業者/非営利団体A（管理者）

個人

直接適用（GDPR3条2項）。
事業者/非営利団体AはEU代表者を選任する義務等のGDPR上の義務を負う。例えば、GDPRに対応したクッキー同意管理バナーのウェブサイトへの導入、プライバシーポリシーの整備等

GDPR違反に対する制裁金の上限額には、①1000万ユーロ以下または事業者である場合は前会計年度の全世界年間売上高の2%以下のいずれか高い方と、②2000万ユーロ以下または事業者である場合は前会計年度の全世界年間売上高の4%以下のいずれか高い方の2つのレベルが定められている。

GDPR

直接適用（GDPR3条1項）。
当該事業者Bの兄弟会社C（ECサイトの運営主体ではない）が、欧州市場に対するマーケティングキャンペーンを主導

事業者Bの兄弟会社C

事業者B（管理者）

個人

EEA域内の管理者または処理者の拠点の活動に関連した個人データの処理
事業者Bは、欧州を含めたグローバルな市場に対してECサイトを展開（当該ECサイトに関するデータ処理はすべて米国内のサーバ上で実施）

S&K Brussels

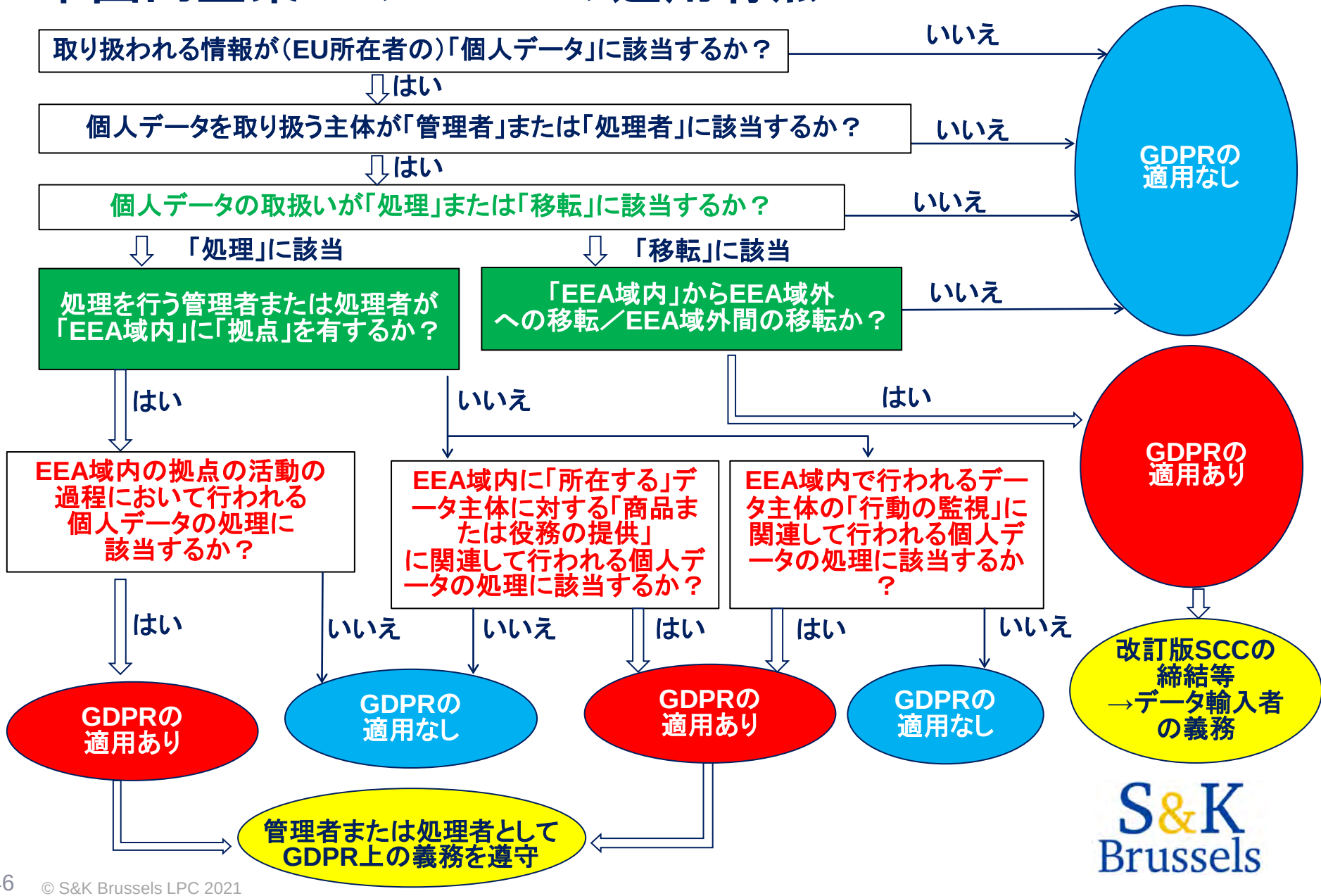
© S&K Brussels LPC 2021

米国国内の事業者にGDPRが直接適用される場面（域外適用）

拠点の所在地	処理行為	適用事例
EEA域内に拠点あり	EEA域内の管理者または処理者の拠点の活動に関連した個人データの処理	▪ 米国国内の事業者Bが欧州を含めたグローバルな市場に対してECサイトを展開（当該ECサイトに関するデータ処理はすべて米国内のサーバ上で実施）、当該事業者Bの兄弟会社C（ECサイトの運営主体ではない）が、欧州市場に対するマーケティングキャンペーンを主導し、これにより米国国内の事業者Bが欧州市場から収益をあげている。
EEA域内に拠点なし	EEA域内に所在するデータ主体に対する商品またはサービスの提供に関連して行われる個人データの処理	▪ 米国国内の事業者がゲームアプリをEEA域内所在のプレイヤーに配信し、プレイヤーの氏名・課金履歴等を収集 ▪ ユーロ決済可能で英語表記があり、EU向け配送に言及しているECサイトで顧客の住所・氏名・口座情報等を収集 ▪ 米国内の事業者/非営利団体Aが、EEA域内所在の個人に対してメールマガジンを配信するため、氏名・メールアドレス等を管理
	EEA域内で行われるデータ主体の行動のモニタリングに関連して行われる個人データの処理	▪ 米国国内の事業者がEEA域内に所在する個人から、アプリで位置情報を取得して分析 ▪ 米国国内の事業者がWebサイト上からクッキー情報を取得して個人の嗜好等を分析して行動ターゲティング広告を配信 ▪ 米国国内の事業者が、ウェアラブル端末（スマートウォッチ等）を通じてEEA域内に所在する個人の健康関連情報を取得・管理

© S&K Brussels LPC 2021

米国内企業へのGDPRの適用有無



© S&K Brussels LPC 2021

CPRA上の事業者の義務は、基本的に、GDPR上の管理者の義務にほぼ包摂されており（◎：ほぼ同一、〇：実質的に同一、△：対応する義務であるが、詳細には違いがある）、GDPRはCPRAよりもさらに重い義務を事業者に対して課する。GDPRの適用を受ける米国内の法的主体は、CPRA対応とは別に、GDPR対応を行う必要がある。

CCPA/CPRA上の事業者の義務	CPRA上の事業者の義務に対応するGDPR上の義務
利用目的の通知義務	◎情報通知義務
知る請求への対応義務	〇アクセス権、データポータビリティ権の行使への対応義務
プライバシーポリシーの開示	〇情報通知義務
削除請求への対応義務	〇削除権行使への対応義務
訂正請求への対応義務	〇訂正権行使への対応義務
オプトアウト手続	△処理に対する異議権
未成年者についてのオプトイン手続	〇情報社会サービスとの関係において子どもの同意に適用される要件
センシティブ個人情報の利用・開示の制限請求の手続	△処理の制限の権利
権利行使を理由とする差別の禁止	△明文の規定はないが、管理者はデータ主体の権利の行使を容易にする義務があり、権利行使を理由とする差別はこの義務に違反すると考えられる
個人情報の取得等への金銭的なインセンティブの付与	△処理の法的根拠としての同意の有効要件
売却先・共有先である第三者、個人情報の開示先であるサービス提供者・契約受託者との契約締結義務	〇データ処理契約の締結
研修義務	〇個人データの安全性
記録管理義務	〇記録義務
個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務	〇個人データの安全性
データ保護影響評価の実行義務	〇データ保護影響評価の実行義務

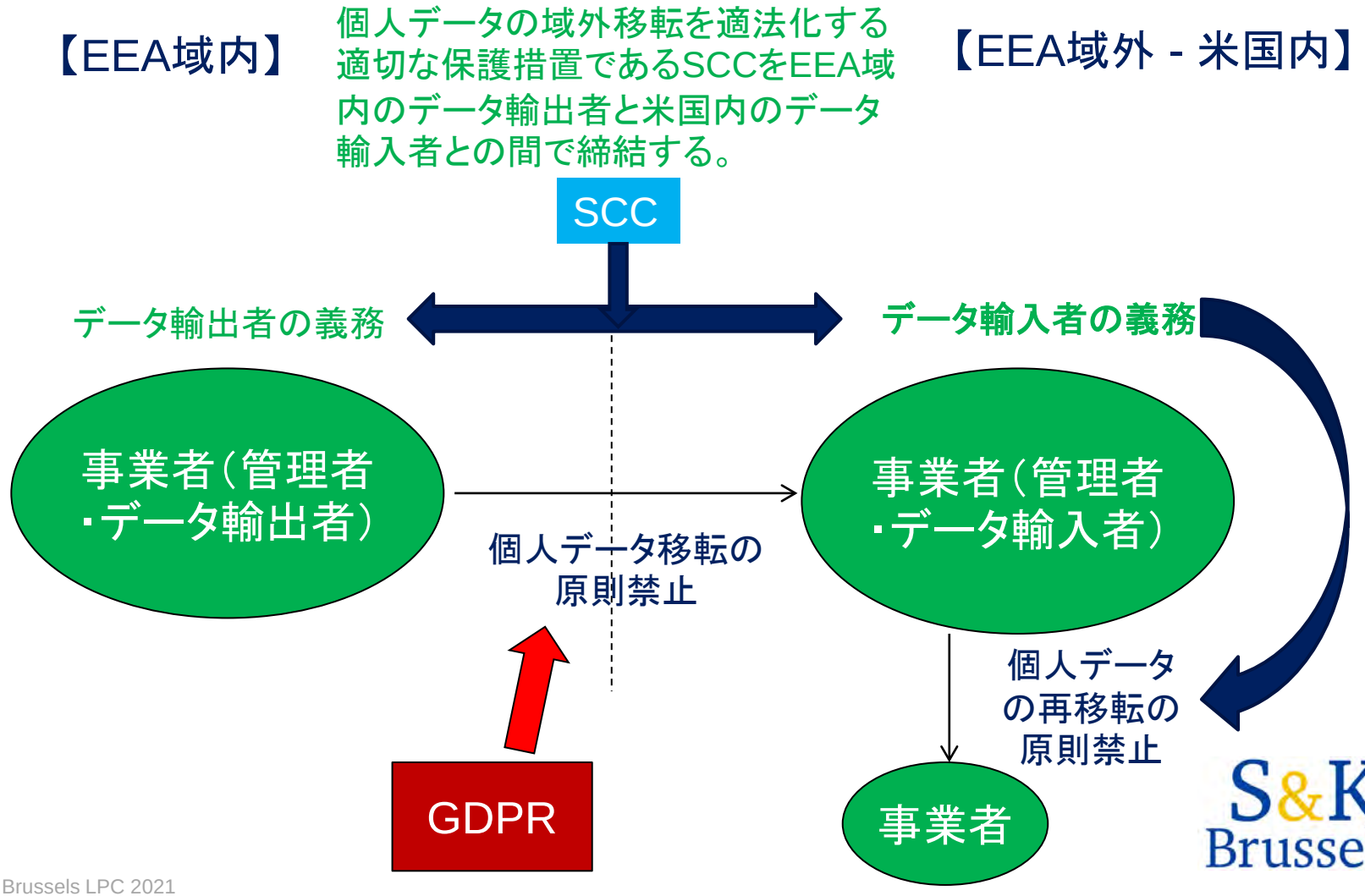
© S&K Brussels LPC 2021

GDPRにあってCPRAにない事業者の義務

GDPR上の義務	内容
1. 個人データ処理の適法性の確保	EUでは、個人データの処理は原則違法とされており、取得・利用を含め個人データのあらゆる形態の運用について以下のいずれかの法的根拠が必要とされている。 1. データ主体の同意：データ主体が、一つまたは複数の特定の目的のために、自身の個人データ処理に同意した場合 2. 契約の履行：データ主体が当事者となっている契約の履行のために当該処理が必要な場合、または契約締結前のデータ主体の要求に応じて手続をとるために当該処理が必要な場合 3. 法的義務の遵守：管理者の法的義務を遵守するために処理が必要な場合 4. 重要な利益の保護：データ主体または他の自然人の重要な利益を保護するために処理が必要な場合 5. 公共の利益：公共の利益または管理者の公的権限行使のために行われる業務遂行において処理が必要な場合 6. 正当な利益：管理者または第三者によって追求される正当な利益のために処理が必要な場合
2. センシティブデータの処理の原則禁止	特別な種類の個人データの処理と、有罪判決および犯罪と関連する個人データの処理は原則として禁止されている。
3. GDPR遵守の確保および説明のための措置	管理者は、GDPRに従って処理がなされることを確保し、かつ、そのことを説明できるようにするための適切な技術的および組織的措置を講じなければならない。また、これらの措置はレビューを行い、必要に応じて最新のものに改める必要がある。
4. データ侵害の通知義務	■ 個人データの侵害が発生した場合には、個人データの侵害により自然人の権利および自由に対するリスクが生じる可能性がない場合を除き、管理者は、不当な遅滞なく（可能であれば、侵害を認知してから遅くとも72時間以内に）、個人データの侵害の事実等を管轄監督当局に通知しなければならない。 ■ 処理者は、侵害を認知した後、不当な遅滞なく管理者に通知しなければならない。 ■ 個人データの侵害が自然人の権利および自由に対して高いリスクをもたらす可能性がある場合には、管理者は、不当な遅滞なく、個人データの侵害をデータ主体にも連絡しなければならない。
5. データ保護責任者	GDPRにおける重要な概念であるアカウンタビリティの中心的機能と、GDPRの遵守を容易にする機能を果たすほか、関係するステークホルダー（監督当局、データ主体および組織内の各部門）の仲介者としての役割を果たすことが期待されている機関であって、一定の場合に、管理者および処理者が選任を義務付けられるもの。米国連邦データプライバシー法案（民主党案COPRA、共和党案SAFE DATA Act）にはデータプライバシーオフィサー・データセキュリティオフィサーの選任が義務付けられている（「V. 米国連邦データプライバシー法案の行方」御参照）。
6. EU代表者の選任	EEA域内に拠点を持たない管理者または処理者であっても、①EEA域内に所在するデータ主体に対する商品またはサービスの提供に関連して行われる個人データの処理、または②EEA域内で行われるデータ主体の行動の監視に関連して行われる個人データの処理についてはGDPRが適用され、管理者または処理者は、書面でEU代表者を指名しなければならない。

© S&K Brussels LPC 2021

米国国内の事業者が、欧州委員会のデータ移転契約のひな型であるSCC（Standard Contractual Clauses：標準契約条項）の締結を求められ、SCC上のデータ輸入者の義務を負う場合



© S&K Brussels LPC 2021

SCC上のデータ輸入者の義務の内容（モジュールI　管理者－管理者）

データ保護措置

目的の制限：データ輸入者は、移転の特定の目的のためにのみ個人データを処理する

透明性：データ主体が権利を効果的に行使できるようにするために、データ輸入者は、直接またはデータ輸出者を介して、データ主体に一定の情報を通知する

正確性とデータの最小化：個人データが正確で、必要に応じて最新の状態に保たれているように努める。処理の目的に関連して、不正確な個人データを遅滞なく削除または修正するために、あらゆる合理的な措置を執る。個人データが適切かつ関連性があり、処理の目的に関連して必要なものに限定されていることを確保する

保管の制限：処理される目的のために必要な期間を超えて個人データを保持しない

処理のセキュリティ：

- 偶発的または違法な破壊、損失、改ざん、無権限の開示またはアクセスにつながるセキュリティ違反に対する保護を含む、個人データのセキュリティを確保するために、適切な技術的および組織的措置を実施する。
- ANNEX IIで規定する技術的および組織的措置について合意
- 個人データ侵害により、自然人の権利および自由が損なわれる危険性がある場合、データ輸入者は、データ輸出者および管轄監督当局の双方に、遅滞なく通知
- 個人データ侵害により、自然人の権利および自由が損なわれる危険性が高い場合、データ輸入者は、個人データ侵害およびその内容について、必要であればデータ輸出者との協力の上、該当するデータ主体に遅滞なく通知
- 個人データ侵害に関連する事実すべてについて、その影響および講じられた是正措置を含めて文書化するとともに、その記録を保持

© S&K Brussels LPC 2021

SCC上のデータ輸入者の義務の内容（モジュールI　管理者－管理者）

データ保護措置

センシティブデータ：移転するデータにセンシティブデータが含まれる場合、データ輸入者は、データの特定の性質やリスクに応じて、特定の制限および／または追加の保護措置を適用する

再移転の制限：個人データをEU外（データ輸入者と同じ国内または別の第三国）に所在する第三者に開示しない。当該第三者がSCCにおけるものと同様の再移転の禁止の制限を受けている場合は除く。以下の場合にのみ、データ輸入者は再移転を行うことができる。

- 欧州委員会の十分性認定の恩恵を受ける国への移転
- 第三者が、処理に関して、適切な保護措置を確保している。
- 第三者がデータ輸入者との間で本条項と同レベルのデータ保護を保証する拘束力のある契約を締結し、データ輸入者がデータ輸出者にこれらの保護措置の写しを提供する。
- 特定の行政、規制または訴訟における手続を行う上で、法的請求を立証、行使または防御するために必要
- データ主体または別の自然人の重大な利益を保護するために必要である。
- その他の条件に1つも該当しない場合には、データ輸入者がデータ主体に対し、再移転の目的、受領者の身元、およびそのような移転において適切なデータ保護措置が講じられないことにより生じうる危険性を説明した上で、特定の状況における再移転について、データ主体の明示的な同意を得ている。

SCCの遵守に関する説明責任：管轄監督当局の要請に備えて、処理活動に関する適切な文書化が必要。

© S&K Brussels LPC 2021

SCC上のデータ輸入者の義務の内容（モジュールI　管理者－管理者）

データ主体の権利行使対応

- データ輸入者は、データ輸出者の支援に関係する場合、個人データの処理および本条項に基づく権利の行使に関連するデータ主体からの問い合わせおよび要求には、不当な遅滞なく、かつ問い合わせまたは要求を受け取ってから1か月以内に対応するものとする。
- データ輸入者は、当該問い合わせ、要求およびデータ主体の権利の行使を促進するための適切な措置をとるものとする。データ主体に提供される情報は、明確かつ平易な言語を用いて、わかりやすく、容易にアクセスできる形で提供されるものとする。

公的機関によるアクセスがある場合の現地法および義務

- データ越境移転影響評価（SCCの遵守に影響を与える現地法・実務）
- データ輸出者・データ主体への通知
- 適法性とデータ最小化の審査

データ主体への損害賠償責任

管轄監督当局の管轄権に服することに合意

© S&K Brussels LPC 2021

まとめ：GDPRコンプライアンスの対応事項と対応方法

対応事項	対応方法
データマッピング	データマッピングアセスメントレポートの作成
処理の法的根拠の確保	処理行為の記録、同意書、プライバシーポリシーにおける法的根拠の開示
処理行為の記録	処理行為の記録の作成
データ主体への情報通知義務	プライバシーポリシーの作成または個別のプライバシー通知
データ主体の権利行使への対応	データ主体の権利行使対応マニュアルの策定
適切な技術的・組織的措置の実施	セキュリティ規程、セキュリティデータマッピング
個人データ侵害への対応	データ侵害通知マニュアルの策定
データ処理契約の締結・変更	管理者・処理者間のデータ処理契約の締結
データ保護責任者（**DPO**: Data Protection Officer）・EU代理人の選任	DPO/EU代理人それぞれの選任義務の検討と、選任義務がある場合には適任者の選任
データ保護影響評価の実施	データ保護影響評価のテンプレートの作成とそれに基づく影響評価の実行
越境移転規制対応	データ輸出者・データ輸入者の間でのSCCの締結とSCC上の義務を履行するための社内体制の整備

© S&K Brussels LPC 2021

IV. CPRAによるカリフォルニアプライバシー保護局（CPPA: California Privacy Protection Agency）の創設

© S&K Brussels LPC 2021

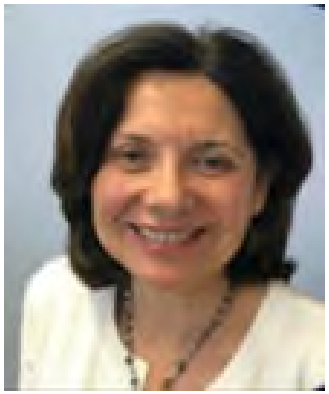
カリフォルニアプライバシー保護局（CPPA: California Privacy Protection Agency）の創設

- **CPPA**:CPRAの実施および執行と制裁金の賦課を担当する新当局。委員長を含む5名の委員によって構成される委員会（委員長・委員のプロフィールは、カリフォルニア州知事のウェブサイト（https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/）を参照し作成）。

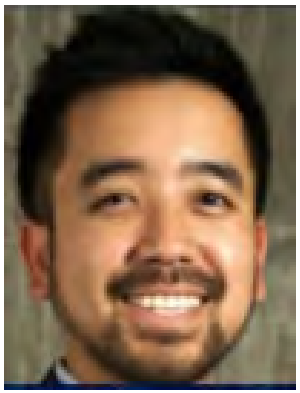
Lydia de la Torre委員
加州上院議長によって指名。サンタクララ大学ロースクール教授でサンタクララローブライバシー認証プログラムを共同で率いた。Squire Patton Boggsの前オフカウンセル。EUのGDPRを含む国際的なデータ保護の論点の専門家。

John Christopher Thompson委員
（民主党）Newsom加州知事によって指名。2020年よりLA 2028の政府関係部門のシニアヴァイスプレジデントを務める。

Jennifer M. Urban委員長（無所属）
Newsom加州知事によって指名。
2009年よりカリフォルニア大学バークレー校ロースクール法律の臨床学教授などを歴任する。



Angela Sierra委員
Xavier Becerra前加州司法長官によって指名。
公民権部門のChief Assistant Attorney General。公民権部門のChiefとして消費者保護部のプライバシー室を監督し2019年のEquifaxの事件を含む州を跨ぐデータ侵害和解に関与



Vincent Le委員
加州下院議長指名。Greenlining Instituteの Technology Equity attorneyを務め、消費者プライバシーに注力。

（注：上の写真は、委員長および各委員の所属する団体のウェブサイト等から引用したものである。）

S&K Brussels

© S&K Brussels LPC 2021

CPRAのタイムライン

日程	関連イベント
2020年11月3日	CPRA住民投票
2020年12月	役職員等の雇用関連個人情報および取引先の従業員の個人情報に関するCPRA一部規定の適用猶予に関する規定等の発効。カリフォルニアプライバシー保護局（**CPPA**: California Privacy Protection Agency）の創設に向けた動きの開始
2021年7月1日	CPPAによるCPRA規則のドラフトの開始
2021年7月	CCPA不遵守の通知を送信しそれに対して各企業が講じた措置の実例を公表（参考資料①：カリフォルニア州司法長官によるCCPA執行事例）。消費者がCCPAに違反した可能性のある事業者に対して送付するための不遵守の通知をドラフトすることを助けるツールを公表（参考資料③：カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool）
2021年9月22日	CPPAは「2020年CPRAに基づく規則制定案に関する予備的コメントの募集について」を公表し、同年11月8日を締切として、CPRA規則案の作成にあたって関連論点に関するパブリックコンサルテーションを実施
2021年10月8日	ニューサム加州知事がCCPAとCPRAを改正する2つの法案（Assembly Bill 694：CPRAを改正し、定義や免除に関する項目を技術的に変更。AB825:カリフォルニア州データ漏洩通知法上の個人情報の定義に遺伝子データを追加）に署名し法律を制定
2022年1月1日	12か月のlook back期間の開始（CPRA上の事業者の義務は2022年1月1日以降に取得した個人情報に関して適用される）
2022年7月1日	CPPAによるCPRA規則の採択期限
2023年1月1日	CPRA適用開始日。**役職員等の雇用関連個人情報および取引先の従業員の個人情報に関するCPRA一部規定の適用猶予に関する規定の失効**
2023年7月1日	CPRA執行開始日

© S&K Brussels LPC 2021

CPRAコンプライアンスへのロードマップ

- CPPAによって今後発表されるニュースにも注意を払いつつ、主に以下のような項目（CPRA規則の内容を踏まえてレビュー・確定の必要がある）について、CPRAへのコンプライアンス対応を進めていく必要がある。

1. CPRAを踏まえたデータマッピングの実行/既に実行したCCPAを踏まえたデータマッピングのCPRAに対応したアップデート（データマッピング質問票については、「参考資料⑤：CPRAデータマッピング質問票－人材採用の例での回答）」を御参照）
   （1）「個人情報」の定義の新しい例外が適用されるかを特定する
   （2）個人情報の転送が「共有」と見なされるかどうかを評価する
   （3）取得している「センシティブ個人情報」を特定する
   （4）事業者のプライバシー通知における追加の開示の請求に対応した情報を取得
   （5）事業者が行う個人情報の転送を洗い出し評価して、各受領者との間で締結すべき契約の内容を確定する
2. データマッピングの結果を踏まえたコンプライアンス文書の作成
   （1）プライバシー通知およびオプトアウトリンクの更新
   （2）第三者、サービス提供者、および契約受託先との契約を確認および更新する
   （3）個人の権利手続きと対応資料を更新する
   （4）個人情報の取得と保持に関連する社内慣行を確認する
   （5）個人情報処理活動における同意の役割と方法を評価する
3. 今後公表されるCPRA規則の内容の把握と解釈

S&K Brussels

© S&K Brussels LPC 2021

今後公表されるCPRA規則の内容の把握と解釈

- CPPAによって、CCPA規則（CCPA Regulation）と同様にCPRA規則を策定するための新しいルール作成プロセスが開始した。これは2022年7月1日までに最終決定される必要がある。遅くとも来年はじめにはCPRA規則ドラフトが公表される可能性が高い。
- CPPAは、2021年9月22日付「2020年CPRAに基づく規則制定案に関する予備的コメントの募集について」を公表し、同年11月8日を締切として、CPRA規則案の作成にあたって以下の各論点に関するパブリックコンサルテーションを実施中。
  1. 消費者のプライバシーまたはセキュリティに重大なリスクをもたらす処理。事業者が実施するサイバーセキュリティ監査とリスク評価
  2. 自動的意思決定
  3. CPPAが実施する監査
  4. 消費者の削除請求権、訂正請求権、知る権利
  5. 個人情報の売却または共有を拒否する権利、およびセンシティブ個人情報の使用および開示を制限する消費者の権利
  6. センシティブ個人情報の使用および開示を制限する消費者の権利
  7. 消費者の知りたいことに応じて提供される情報（具体的な情報項目）
  8. 定義と種類

S&K Brussels

© S&K Brussels LPC 2021

1. 消費者のプライバシーまたはセキュリティに重大なリスクをもたらす処理。事業者が実施するサイバーセキュリティ監査とリスク評価

- CPRAは、「消費者の個人情報を処理することにより、消費者のプライバシーまたはセキュリティに重大なリスクをもたらす」事業者に対し、1）年次サイバーセキュリティ監査の実施、2）個人情報の処理に関する定期的なリスク評価の同局への提出を義務付ける規制を発行するようCPPAに指示している。
  - 事業者による個人情報の処理が、「消費者のプライバシーまたはセキュリティに対する重大なリスク」をもたらす場合。
  - 毎年のサイバーセキュリティ監査を行う企業に求められることは、監査で何をカバーすべきか、監査が「徹底しており、独立している」ことを保証するためにどのようなプロセスが必要か。
  - リスク評価で何をカバーすべきか、リスク評価を提出する頻度、消費者の個人情報やセンシティブ個人情報を処理する際のリスクとベネフィットをどのように比較検討すべきかなど、CPPAにリスク評価を提出する事業者に求められるべきこと。
  - 事業者が消費者情報を処理することによる「消費者のプライバシーに対するリスクが利益を上回る」場合、および消費者のプライバシーまたはセキュリティに重大なリスクをもたらす処理が制限または禁止されるべき場合。

S&K Brussels

© S&K Brussels LPC 2021

2. 自動的意思決定

- CPRAは、消費者の「事業者による自動的意思決定技術の使用に関するアクセス権およびオプトアウト権」を規定する規制を定めている。
  - どのような活動が「自動化された意思決定技術」および／または「プロファイリング」に該当するとみなされるべきか。
  - 事業者の自動的意思決定技術の使用に関する情報に、消費者はいつアクセスできるべきか、また、アクセスを容易にするために消費者と事業者はどのようなプロセスを踏むべきか。
  - 自動化された意思決定プロセスに関わる「論理に関する意味のある情報」を提供するために、事業者は何をしなければならないかを含め、アクセス請求に応じて事業者が消費者に提供しなければならない情報について。
  - 自動化された意思決定に関する消費者のオプトアウト権の範囲と、オプトアウトを容易にするために消費者と事業者が従うべきプロセスについて。

S&K Brussels

© S&K Brussels LPC 2021

3. CPPAが実施する監査

- CPRAは、事業者が法律を遵守しているかどうかを監査する権限を政府機関に与えている。
- 監査権限を定義するための規則
  - CPPAの監査権限の範囲はどうあるべきか。
  - CPPAが監査権限を行使する際に従うべきプロセスと、監査対象となる事業者を選定するために用いるべき基準。
  - 消費者の個人情報を監査人への開示から保護するために、CPPAが採用すべきセーフガードについて。

S&K Brussels

© S&K Brussels LPC 2021

4. 消費者の削除請求権、訂正請求権、知る権利

- CCPAは、事業者が保有する個人情報を管理するための一定の権利を消費者に与えている。これには、個人情報の削除請求権、どのような個人情報が収集されているのかを知る権利、その個人情報にアクセスする権利、どのような種類の個人情報が誰に売却または共有されているのかを知る権利などがある。CPRAはCCPAを改正し、不正確な個人情報の訂正を要求する権利を新たに追加した。司法長官は、知る権利と削除請求権を促進するための規則と手続きを定めた規則を採択した。CPRAはさらに新たな訂正する権利を促進するための規則と手続きを定めた規則を規定する。
  - 消費者が不正確な個人情報の訂正を要求するために必要な、新しい規則や手続き、または既存の規則や手続きの変更。
  - 消費者が自分の個人情報の訂正を求めることができる頻度とその状況
  - 訂正要求に対して事業者がどのように対応しなければならないか、不正を防止するために事業者がとるべき措置を含む。
  - 要請への対応が「不可能、または不釣り合いな努力を要する」ため、または要請の対象となる情報が正確であるために、事業者が請求に対する措置を講じる義務を免除されるべき場合。
  - 事業者が個人情報の訂正要求を拒否した場合に、消費者が事業者との記録に書面による追記を提供する権利。

S&K Brussels

© S&K Brussels LPC 2021

5. 個人情報の売却または共有を拒否する権利、およびセンシティブ個人情報の使用および開示を制限する消費者の権利

- CCPAは、対象事業者による個人情報の売却をオプトアウトする権利を消費者に与えている。2020年、司法長官は、CCPAに基づく消費者の個人情報売却のオプトアウトの権利を実施するための規則を採択した。CPPAは現在、個人情報の売却をオプトアウトする権利に関するCCPAの規則を更新し、センシティブ個人情報の使用を制限するための規則を作成し、その他の改正を考慮して、追加の規則作成を行う。
  - 消費者が事業者によるセンシティブ個人情報の使用を制限することを可能にするために、どのようなルールと手続きを確立すべきか。
  - どのような要件と技術仕様が、プラットフォーム、技術、またはメカニズムによって送信されるオプトアウト優先信号を定義すべきである。これは、消費者の個人情報の売却または共有をオプトアウトする、あるいは消費者のセンシティブ個人情報の使用または開示を制限するという消費者の意思を示すためのものである。
  - 消費者または消費者の親権者が、消費者が13歳未満であること、または13歳以上16歳未満であることを指定できるオプトアウト優先信号について、どのような技術仕様を確立すべきか。
  - オプトアウト・プリファレンス・シグナルによって表明された消費者の権利を、事業者はどのように処理すべきか。
  - 以前にオプトアウト希望信号を介してオプトアウト希望を表明した消費者に、個人情報の売却や共有、あるいはセンシティブ個人情報の使用と開示に同意する機会を提供するために、事業者がすべきこと。

S&K Brussels

© S&K Brussels LPC 2021

6. センシティブ個人情報の使用および開示を制限する消費者の権利

- CCPAは、消費者の個人情報に関連して、事業者には一定の責任を、消費者には一定の権利を与えている。CPRAはCCPAを改正し、新たな種類の情報について消費者に追加の権利を与えている。CPRAはCCPA を改正し、「センシティブ個人情報」という新たな種類の情報に対する追加の権利を消費者に与え、これらの権利を実施するために既存の規制の改正および／または新たな規制の発行を行うよう、CPPAに指示している。これらの権利には、上述のセンシティブ個人情報の使用と開示を制限する新しい権利が含まれる。
  - 消費者に関する特性を推論する目的ではなく収集または処理された」とみなされ、したがって使用および開示を制限する権利の対象とならない「センシティブ個人情報」とは何か。
  - 消費者のセンシティブ個人情報の使用または開示を制限するという消費者の指示にかかわらず、事業者による消費者のセンシティブ個人情報のどのような使用または開示が許容されるべきか。

S&K Brussels

© S&K Brussels LPC 2021

7. 消費者の知りたいことに応じて提供される情報（具体的な情報項目）

- 事業者が消費者に特定の情報を開示することが求められる場合、CPRA は一般的に、消費者が要求する前の12 ヶ月間を対象とした開示を要求している。しかし、2022年1月1日以降に処理されたすべての情報については、消費者は以下の例外を条件として、12ヶ月間を超える情報を要求し、事業者は開示しなければならない。
  - 12ヶ月間を超えて情報を提供することが「不可能」または「不釣り合いな努力を必要とする」と事業者が判断する場合、どのような基準を適用すべきか。

S&K Brussels

© S&K Brussels LPC 2021

8. 定義と種類

CCPAとCPRAは、重要な用語や、法令が対象とする情報や活動の種類の定義を作成または更新するために、様々な規制を定めている。

- 法律で規定されている「個人情報」の種類に対して行われるべき更新または追加
- 法律に示されている「センシティブ個人情報」の種類に対してなされるべき更新または追加
- 「非識別化」および／または「固有識別子」の定義に関する更新
- 事業者から情報を得るための「要求を提出するための指定された方法」の定義に加えるべき変更点
- 事業者、サービス提供者、契約受託者が、異なる情報源から入手した消費者の個人情報を組み合わせることができる事業目的の定義
- 消費者が「意図的に人と接する」場合をさらに定義するために行うべき変更
- 「正確な位置情報」をさらに定義するために行うべき変更
- CPPAが採用すべき「消費者から得た特定の情報」の定義
- 「法執行機関が承認した調査」をさらに定義するために採用されるべき規制
- 「ダークパターン」をさらに定義するために採用すべき規制

S&K Brussels

© S&K Brussels LPC 2021

V. 米国連邦データプライバシー法案の行方

© S&K Brussels LPC 2021

最も有力な米国連邦データプライバシー法案

- 米国連邦データプライバシー法案の立法化は現政権を握る米国民主党の2020 Democratic Party Platformという政権公約に掲げられた。COPRA（Consumer Online Privacy Rights Act）（消費者オンラインプライバシー法）（https://www.cantwell.senate.gov/imo/media/doc/COPRA%20Bill%20Text.pdf）という法案が現状最も有力であり、COPRA の枠組みが維持されて立法化される可能性は高い。共和党の法案として最も有力な SDA（SAFE DATA Act）（https://www.commerce.senate.gov/services/files/BD4D6CB6-AE64-4453-8299-BAC4328BDC56）も立法化の過程である程度の影響力を持つことが予想される。

116TH CONGRESS
1ST SESSION

S. _____

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE SENATE OF THE UNITED STATES

Ms. CANTWELL (for herself, Mr. SCHATZ, Ms. KLOBUCHAR, and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Consumer Online Privacy Rights Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Effective date.

Maria Cantwell 上院議員（民主党・ワシントン州選出）
米国連邦議会上院の商務・科学・運輸委員会の現委員長・前ランキングメンバー

Roger Wicker 上院議員（共和党・ミシシッピー州選出）
米国連邦議会上院商務・科学・運輸委員会の前委員長・現ランキングメンバー

注：上記いずれの写真は、米国連邦議会上院商務・科学・運輸委員会のウェブサイトおよびWicker上院議員のウェブサイトから引用。

117TH CONGRESS
1ST SESSION

S. _____

To establish data privacy and data security protections for consumers in the United States.

IN THE SENATE OF THE UNITED STATES

Mr. WICKER introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish data privacy and data security protections for consumers in the United States.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or the "SAFE DATA Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Definitions.
Sec. 3. Effective date.

© S&K Brussels LPC 2021

最も有力な米国連邦データプライバシー法案の検討の行方

- 2021年7月16日、Roger Wicker上院議員をはじめとする共和党の有力議員は、米バイデン大統領に対し、米国における包括的なデータプライバシー法の立法を優先的に進めることを促す書簡を送った（https://www.commerce.senate.gov/2021/7/committee-leaders-urge-president-to-prioritize-data-privacy-legislation ）。2021年7月29日、Roger Wicker上院議員他は、SAFE DATA Actを今会期に再提出した。
- 2021年9月29日、米国連邦議会上院商務・科学・運輸委員会の委員長であるMaria Cantwell上院議員は、「Protecting Consumer Privacy」と題した公聴会を開催した。この公聴会では、プライバシー局の設立により連邦取引委員会が消費者のプライバシー保護に必要なリソースを備えることや、包括的な連邦プライバシー法の必要性など、消費者のプライバシー権をよりよく保護する方法の検討を行った。

July 16, 2021

The Honorable Joseph R. Biden, Jr.
President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, DC 20500

Dear President Biden:

We write to urge you to work with Congress to enact a nationwide consumer data privacy law. For the past year, millions of Americans have shifted their normal activities online in response to the COVID-19 pandemic. To facilitate this transition to virtual and remote living, Congress has accelerated its efforts to close the digital divide and expand broadband access to unserved and underserved communities throughout the country. Although this has helped increase access to connectivity, e-commerce products, and essential services, it has also resulted in more consumer data and personal information flowing across state lines and throughout the economy than ever before.

Consumer data has long been a target for cybercriminals and other bad actors seeking to exploit Americans' personal information for nefarious purposes. Unfortunately, the pandemic has only worsened this situation. According to the Federal Trade Commission, identity theft increased by almost 3,000 percent over the past year.[1] This problem is exacerbated by the failure of some companies to properly safeguard consumer data from misuse and unwanted collection and processing.

In light of the recent increase of cyberattacks on United States critical infrastructure, as well as businesses and localities, and ongoing efforts to expand internet services to every American, we urge you to prioritize comprehensive data privacy legislation as part of your Administration's agenda. Such legislation should:

- Establish one national data protection standard, rather than a patchwork of state laws, to provide consumers across the country with the same strong protections over their personal information no matter where they live;
- Increase transparency and accountability to ensure consumers have a better understanding of how their information is collected, used, and shared, and to ensure companies who misuse consumer information are held sufficiently accountable;
- Promote innovation by setting clear and workable rules that enable startups and small businesses to grow and compete; and
- Enhance data security protections to ensure companies have reasonable practices in place to safeguard consumer information.

Absent much-needed federal data privacy legislation, we risk losing consumers' trust and confidence in the internet marketplace and undermining our national security and technological leadership abroad. In particular, the passage of federal data privacy legislation would bolster America's position in the ongoing negotiations with the European Union to create a new framework governing transatlantic data flows. It would also solidify the United States' status as a global leader on consumer privacy, by ensuring innovation and competition remain a foundational principle to our economic advancements, especially at a time when China, Russia, and others seek to do the same.

Americans deserve to have their data protected and secured. We thank you for your attention to this urgent matter and look forward to working with you to develop a national bipartisan data privacy law that protects consumers, provides accountability, and promotes continued investment, innovation, and competitiveness in the digital economy.

Sincerely,

Senator Roger F. Wicker
Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation

Representative Cathy McMorris Rodgers
Ranking Member
U.S. House Committee on Energy and Commerce

Senator Marsha Blackburn
Ranking Member
U.S. Senate Subcommittee on Consumer Protection, Product Safety, and Data Security

Representative Gus Bilirakis
Ranking Member
U.S. House Subcommittee on Consumer Protection and Commerce

© S&K Brussels LPC 2021

COPRA（Consumer Online Privacy Rights Act）（消費者オンラインプライバシー法）（民主党案）

①対象事業者（（i）FTC 法（15 U.S.C. 41 et seq.）の適用対象（米国商取引に従事している、または商取引に影響を与える個人、組合または企業）であり、かつ（ii）対象データを処理または転送する事業者または個人）の義務

1. 対象データの処理と転送に関する義務

適法性の義務、透明性の義務、公平性の義務、目的の限定の義務、データ最小化の義務、データセキュリティ慣行の確立・実装・維持義務、自動的意思決定に関する義務、権利放棄の禁止、忠実義務

2. 社内態勢に関する義務

プライバシー責任者・データセキュリティ責任者の選任義務、包括的データプライバシープログラムおよびデータセキュリティプログラム、**サービス提供者の選択や第三者への対象データの転送の決定にあたっての合理的なデューデリジェンスの実施義務**、内部告発者の保護

3. 個人の権利の尊重

アクセス権、削除権、訂正権、データポータビリティ権、転送のオプトアウト権、センシティブ対象データ（**センシティブ対象データには、電子メールアドレスや電話番号が含まれており、BtoBの文脈での取引先の担当者のコンタクト情報もこれに該当する**）のオプトイン権

②大規模データ保有者（対象事業者であって、直近の暦年に（A）500 万人を超える個人、個人または世帯が利用する機器、もしくは世帯の対象データの処理または転送、あるいは（B）10 万人を超える個人、個人または世帯が利用する機器、もしくは世帯のセンシティブ対象データの処理または転送する法的主体）の義務

- **経営陣の責任：対象事業者の大規模データ保有者の最高経営責任者（または、最高経営責任者がいない場合は事業者の最高ランクのオフィサー）および当該事業者の各プライバシー責任者およびデータセキュリティ責任者は、FTC が指定する方法で、COPRA を遵守するための適切な内部統制、および当該認証責任者（最高経営責任者または最高ランクのオフィサー、プライバシー責任者およびデータセキュリティ責任者）が企業の COPRA の遵守に影響を与える決定に関与し、責任を負うことを保証するための報告構造を維持することを毎年 FTC に認証する義務**

③サービス提供者の義務

④第三者の義務

⑥NISTの報告

✓ デジタルコンテンツの偽造が個人および競争相手に与える影響に関する報告書

⑦連邦法と州法の関係

✓ COPRA または COPRA に基づいて制定された規制と直接矛盾する場合に限り、かつ当該直接的な対立の範囲内においてのみ COPRA は州法に優先する。州の法律、規則または規制は、COPRA で保護されているよりも高いレベルの保護を個人に対して提供する場合、直接の対立とは見なされず、無効化されない。

⑤COPRAの執行

1. FTC「不公正または欺瞞的行為または慣行」に関するFTCによる執行

✓ 初回の違反に民事制裁金なし

✓ 恒久的差止命令およびその他衡平法上の救済手段

2. 州司法長官による執行

✓ 上限金額のない民事制裁金制度

3. 個人による民事訴訟

✓ **懲罰的損害賠償制度**

✓ **クラスアクション制度の活用の可能性**

S&K Brussels

© S&K Brussels LPC 2021

SDA（SAFE DATA Act）（セーフデータ法）（共和党案）

①対象事業者（米国または外国の、営利または非営利の団体で、**対象データ**（**個人**（米国に居住する自然人）または個人にリンクする若しくは合理的にリンク可能なデバイスを、識別またはリンクしている、若しくは合理的にリンク可能な情報）を**取得、処理**または**転送**する者）の義務

* 一般的例外（取得、処理または転送が合理的に必要かつ相当で、かつその目的が限定されている場合、SDAが定める12項目のいずれかの目的のためであれば、下記1、3、4、8および9の義務を負うことなく、取得、処理または転送が可能）

1. 消費者ロイヤルティ（製品またはサービスの拒否の禁止、個人のコントロール権の不放棄）
2. 透明性（対象データの取得前または取得時のプライバシーポリシーの公開義務）
3. 同意の権利（センシティブ対象データの処理および転送について個人の事前の明確かつ明示的な同意の取得、対象データの取得、処理または移転のオプトアウト権）
4. **サービス提供者選択/第三者への転送に関し合理的なデューディリジェンス実行義務**
5. 対象データの保護（データセキュリティポリシーと慣行の確立、遂行および維持義務）
6. **内部統制および上級経営陣への報告構造の実行義務**
7. 内部通報者への報復はFTCによる執行においてSDA違反の罰則を決める際に考慮

以下も対象事業者の義務だが、小規模事業者（small business）には適用なし

8. 個人のコントロール（対象データへのコントロール権行使への対応義務）
9. 対象データの取得、処理および保持を最小限に抑える
10. **データプライバシー責任者およびデータセキュリティ責任者の選任義務**

⑧SDAの執行

1.「不公正または欺瞞的行為または慣行」に関するFTCによる執行
- ✓ 初回の違反に民事制裁金なし
- ✓ 恒久的差止命令およびその他衡平法上の救済手段

2. 州司法長官による執行
- ✓ 上限金額のない民事制裁金制度

⑨FTCによる認定資格プログラム

②大規模データ保持者のプライバシー影響評価の実行義務

③サービス提供者の義務

④第三者の義務

⑩FTCの報告
- ✓ 連邦差別禁止法違反に関するFTCの執行援助、年次報告書の議会への提出）
- ✓ アルゴリズムの透明性に関する報告
- ✓ デジタルコンテンツの偽造が個人および競争相手に与える影響に関する報告書

⑤大規模オンラインオペレータの義務
- ■ ユーザーインターフェースの操作に関する欺瞞的および欺瞞的行為と慣行の禁止

⑥データブローカーのFTCへの登録義務

⑪連邦法と州法の関係：州または州の行政小区域が対象事業者のデータプライバシーまたはデータセキュリティおよび関連活動に関する法律、規則、ルール、要件または基準を採択し、維持し、執行し、またはその効力を維持することができないとしており、広範に連邦法による州法の先占（pre-emption）による無効化を認める

⑦対象インターネットプラットフォーム運営者のフィルターバブルの透明性

S&K Brussels

© S&K Brussels LPC 2021

FTC（Federal Trade Commission：連邦取引委員会）：最も有力な米国連邦データプライバシー法案における執行機関

- FTC（Federal Trade Commission：連邦取引委員会）は、米国連邦データプライバシー法案であるCOPRAとSDAのいずれにおいても、執行機関として位置付けられている。したがって、将来の連邦データプライバシー法の立法化後もFTCが執行機関となる可能性は高い状況にある。本セミナー資料執筆時点ではRohit Chopra氏（民主党）が依然としてFTC委員であるが、近くCFPB（Consumer Financial Protection Bureau）長官に就任するとともに、FTC委員を辞任することが確定している。

Rebecca Kelly Slaughter
2018年-2022年
民主党
以前は、上院院内総務（Chuck Schumer）のチーフ・カウンセル。Khan委員長の就任前は委員長代行を務める。

Alvaro Bedoya
2021年-?
民主党
2021年9月13日バイデン大統領によって指名され、連邦上院の承認待ち。ジョージタウン・ロースクール教授・上院司法プライバシー・技術・法小委員会の前チーフカウンセル。

Lina Khan委員長
2021年-2028年
民主党
FTCの委員長に史上最年少の32歳で就任。反トラスト法分野の常識を覆す論陣で巨大IT企業の規制強化を訴える新進気鋭の法学者。Khan委員長は、2018年にChopra前委員のLegal Fellowを務めた。

Noah J. Phillips
2018年-2023年
共和党
以前は上院司法委員会における上院議員（John Cornyn）のチーフ・カウンセルおよび大手法律事務所（訴訟部門）勤務

Christine S. Wilson
2018年-2025年
共和党
以前はデルタ航空の法務、規制および国際部門のSVPおよび大手法律事務所（反トラスト部門）勤務

S&K Brussels

© S&K Brussels LPC 2021

参考資料①：カリフォルニア州司法長官によるCCPA執行事例（前記Iで緑字で言及した事例1-27のリストと詳細）

© S&K Brussels LPC 2021

カリフォルニア州司法長官によるCCPA執行事例

- 2021年7月、カリフォルニア州司法長官Rob Bonta氏は、CCPA不遵守の通知を送信しそれに対して各企業が講じた措置の実例を公表した（https://oag.ca.gov/privacy/ccpa/enforcement ）
- 当該通知の受領者は、2023年1月1日まで、30日間の治癒期間がある。2023年1月1日以降、違反ごとに最大2500ドルの民事制裁金または違反が意図的な場合（または16歳未満の消費者の個人情報が関わる違反の場合）、最大7500ドルの民事制裁金が科される。
- CCPA上の以下の事項へのコンプライアンス対応が適切になされているかを今一度確認することが望ましい。・下の表は、上記27の実例の内容に基づき、各違反類型への言及の回数をカウントしたもの

	CCPA違反が指摘された論点	言及の回数
1	プライバシーポリシーのコンプライアンス違反	14回
2	消費者の権利の請求方法なし/着信課金用電話番号なし	8回
3	違法な個人情報の売却	5回
4	「Do Not Sell My Personal Information」のリンクなし	4回
4	消費者への通知義務の違反	4回
6	オプトアウトプロセスのコンプライアンス違反	3回
7	認定代理人	2回
8	CCPA上の消費者請求に対する恐れ	1回
8	CCPA上の消費者請求に料金徴収	1回
8	本人確認、本人確認のためのアカウント作成	1回

Rob Bonta
カリフォルニア州司法長官
（注：写真は同司法長官オフィスのウェブサイトから引用）

S&K Brussels

© S&K Brussels LPC 2021

カリフォルニア州司法長官によるCCPA執行事例

- 受領者は、2023年1月1日まで、30日間の治癒期間
- 2023年1月1日以降、違反ごとに最大2500ドルの民事制裁金、または違反が意図的な場合（または16歳未満の消費者の個人情報が関わる違反の場合）、最大7500ドルの民事制裁金が科される。

→2023年1月1日以降、治癒期間が保証されないこととなった。すなわち、公表された27の執行事例はいずれも民事制裁金の賦課には至っていないものの、同日以降は民事制裁金の賦課につながりうる事例であるということを意味する。

S&K Brussels

© S&K Brussels LPC 2021

カリフォルニア州司法長官によるCCPA執行事例一覧①

事例	論点	概要
1	消費者への通知	マーケティング会社がサービス提供者としてのステータスを明確化した
2	サービス提供者契約のコンプライアンス違反	ソーシャルメディアネットワーク会社がサービス提供者契約を更新した
3	(1)プライバシーポリシーのコンプライアンス違反 (2)請求方法なし	オンラインイベント販売会社がプライバシーポリシーを更新し、請求方法を追加した
4	(1)「Do Not Sell My Personal Information」のリンクなし (2)プライバシーポリシーのコンプライアンス違反	オンライン・デイティングプラットフォームが「Do Not Sell My Personal Information」のリンクおよび売却情報の開示を追加した
5	(1)プライバシーポリシーのコンプライアンス違反 (2)サービス提供者契約のコンプライアンス違反	オンラインアドテックサービス提供者／事業者がプライバシーポリシーとCCPA上の消費者請求方法を是正した
6	CCPA上の消費者請求に対する対応の遅れ	オンラインソーシャルメディアアプリ会社がCCPA上の消費者請求に適時に対応するために新しいシステムを導入した
7	(1)プライバシーポリシーのコンプライアンス違反 (2)請求方法なし (3)CCPA上の消費者請求に料金徴収	子供向け玩具販売会社がプライバシーポリシーを更新した
8	金銭的インセンティブの未通知	食料品チェーンのロイヤルティプログラムで、金銭的インセンティブ通知の提供を必須化した
9	プライバシーポリシーのコンプライアンス違反	オンラインの求人広告会社がプライバシーポリシーを更新した

© S&K Brussels LPC 2021

カリフォルニア州司法長官によるCCPA執行事例一覧②

事例	論点	概要
10	(1)オプトアウトプロセスのコンプライアンス違反 (2)消費者への通知	メディア複合会社がオプトアウトプロセスおよび通知を更新した
11	オプトアウトプロセスのコンプライアンス違反	データブローカーがオプトアウト方法を更新した
12	(1)消費者への通知 (2)プライバシーポリシーのコンプライアンス違反 (3)着信課金用電話番号なし (4)請求提出方法の欠陥	自動車メーカーが収集時に対面で通知を実施し、プライバシーポリシーと欠陥のあった請求方法を更新した
13	(1)認定代理人 (2)個人情報の売却	ペット産業のウェブサイトで消費者が個人情報のあらゆる売却をオプトアウトするためのオプトアウトウェブフォームを更新した
14	(1)認定代理人 (2)プライバシーポリシーのコンプライアンス違反	食料品店チェーンが、消費者が認定代理人を通じて請求を提出する方法を説明するための開示を更新した
15	(1)個人情報の売却 (2)未成年者の個人情報の売却	モバイルアプリゲーム会社が個人情報の売却を停止し、未成年者に対する保護を更新した
16	(1)消費者への通知 (2)個人情報の売却	ソーシャルメディア会社が個人情報の売却を停止し、プライバシーポリシーを更新した
17	個人情報の売却	メーカーと小売店が個人情報の売却を停止した
18	(1)オプトアウトプロセスのコンプライアンス違反 (2)請求方法なし	メディア複合会社がオプトアウト方式を更新し、「Do Not Sell My Personal Information」のリンクを追加した

© S&K Brussels LPC 2021

カリフォルニア州司法長官によるCCPA執行事例一覧③

事例	論点	概要
19	プライバシーポリシーのコンプライアンス違反	国内食料品店チェーンがプライバシーポリシーを更新し、請求方法を追加した
20	プライバシーポリシーのコンプライアンス違反	メールニュースレタープラットフォームがプライバシーポリシーを更新し請求方法を追加した
21	(1)プライバシーポリシーのコンプライアンス違反 (2)請求方法なし	オンラインイベント売却会社がプライバシーポリシーを更新し、請求方法を追加した
22	(1)プライバシーポリシーのコンプライアンス違反 (2)消費者への通知 (3)「Do Not Sell My Personal Information」のリンクなし	デジタルパートナーが自社の義務を明確にした
23	(1)「Do Not Sell My Personal Information」のリンクなし (2)本人確認、本人確認のためのアカウント作成	データブローカーが、「Do Not Sell My Personal Information」のリンクを更新し、オプトアウト請求時の本人確認とアカウント作成の要求を停止した
24	プライバシーポリシーのコンプライアンス違反	テレビゲーム配信会社がプライバシーポリシーを更新した
25	(1)プライバシーポリシーのコンプライアンス違反 (2)請求方法なし (3)「Do Not Sell My Personal Information」のリンクなし	教育技術会社がプライバシーポリシーを更新し、「Do Not Sell My Personal Information」のリンクを追加した
26	プライバシーポリシーのコンプライアンス違反	衣料品販売店がプライバシーポリシーを更新し、請求方法を追加した
27	請求方法なし	データブローカーが「Do Not Sell My Personal Information」のリンクを追加した

© S&K Brussels LPC 2021

事例1：マーケティング会社がサービス提供者としてのステータスを明確化した

業種：オンラインマーケティングサービス
論点：消費者への通知
事案：

- メールマーケティング会社が消費者の代理で送信したメールを通じて消費者の個人情報を収集していた。
- 同社は消費者に必要な通知を行わず、消費者が請求を提出する方法も提供していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社は、消費者の個人情報を処理したときに、消費者の代理でサービス提供者としての役割を果たしたという証拠を提出した。
- 同社は、ある消費者について取得および処理した個人情報を、別の消費者にサービスを提供する際には使用されていないことを立証した。
- また、利用規約を更新し、CCPAにおけるサービス提供者としての義務を明確にした。

→CPRA適用開始前に、CPRAに準拠したサービス提供者との契約を締結していることを確認することも重要であるといえる。

S&K Brussels

© S&K Brussels LPC 2021

事例2：ソーシャルメディアネットワーク会社がサービス提供者契約を更新した

業種：ソーシャルメディアネットワーク
論点：サービス提供者契約のコンプライアンス違反
事案：

- ソーシャルメディアネットワークを運営していた会社が、契約に定められたサービス以外の目的で得た個人情報を、そのサービス提供者が保持・使用・開示することを契約上禁止していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はCCPAのAddendumを追加することによりサービス提供者契約を変更した。

S&K Brussels

© S&K Brussels LPC 2021

事例3:オンラインイベント販売会社がプライバシーポリシーを更新し、請求方法を追加した

業種:オンラインイベント販売
論点:(1)プライバシーポリシーのコンプライアンス違反、(2)請求方法なし
事案:

- 子供向けの授業や活動参加の販売を行う会社が、必要なCCPA上の消費者の権利(知る権利、削除請求権、差別されない権利)の通知を行うことをプライバシーポリシーで明記しておらず、消費者が CCPA上の権利を行使するために確立されている請求方法も公開していなかった。
- また、同社は過去12カ月間に個人情報を売却したか、または事業目的で個人情報を転送したかどうかについても明言していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新して必要なCCPA上の権利を追加し、2つの請求方法を実装し、事業目的のために転送した個人情報を記載し、個人情報を売却しなかった旨を明言した。

S&K Brussels

© S&K Brussels LPC 2021

事例4:オンライン・デイティングプラットフォームが「Do Not Sell My Personal Information」のリンクおよび売却情報の開示を追加した

業種:オンライン・デイティングプラットフォーム
論点: (1)「Do Not Sell My Personal Information」のリンクなし、(2)プライバシーポリシーのコンプライアンス違反
事案:

- オンライン・デイティングプラットフォームを提供し個人情報を売却していた企業が、そのホームページに「Do Not Sell My Personal Information」のリンクがなく、プライバシーポリシーにおいて売却する個人情報の種類に関して十分な情報を開示していなかった。
- また同社は、ユーザーが新しいアカウントを作成する際に「共有を承諾」ボタンをクリックするだけで、個人情報の売却に関する包括的な同意を得ていたことも明らかにした。
- コンプライアンス違反の疑いの通知を受けた後、同社は明確かつ目立つ「Do Not Sell My Personal Information」のリンクを追加し、プライバシーポリシーを更新してコンプライアンスに則った売却開示について追記した。

S&K Brussels

© S&K Brussels LPC 2021

事例5:オンラインアドテックサービス提供者／事業者がプライバシーポリシーとCCPA上の消費者請求方法を是正した

業種:オンライン広告
論点:(1)プライバシーポリシーのコンプライアンス違反、(2)サービス提供者契約のコンプライアンス違反
事案:

- ある会社がストリーミングサービスや様々なケーブルチャンネルと、そういった場所でターゲット広告スペースを売却したい広告主を仲介している。
- 同社は主としてサービス提供者であるが、一部状況では事業者であるとも言えるため、同社のプライバシーポリシーはCCPAに違反していた。
- さらに、同社のサービス提供者契約では、処理する個人情報の使用に関する必要な制限が含まれていなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社は個人情報を売却していないことを明記し、利用者がCCPA上の消費者請求を行うための手段を提供するなど、プライバシーポリシーを変更した。
- 同社はまた、CCPA上の消費者請求の方法の手順を改良し、CCPAに準拠するようにサービス提供者契約を更新した。

・特に注意したいのは、CCPA上の「サービス提供者」に該当する前提で事業を行っている場合であっても、一定の個人情報の収集等については「事業者」に該当すると評価される場合もあり、「事業者」か「サービス提供者」かの評価は、個人情報の収集等の行為毎に行う必要があるということである。

S&K Brussels

© S&K Brussels LPC 2021

事例6:オンライン・ソーシャルメディアアプリ企業がCCPA上の消費者請求に適時に対応するために新しいシステムを導入した

業種:オンライン・ソーシャルメディアアプリ企業
論点:CCPA上の消費者請求に対する対応の遅れ
事案:

- オンライン・ソーシャルメディアアプリを運営している企業が、個人情報に関する知る権利・個人情報の削除請求権といったCCPA上の消費者請求に適時に対応しておらず、ユーザーが、CCPA上の消費者請求が受信されたか、または実施されたかの通知を受け取っていないという苦情を申し立てた。
- コンプライアンス違反の疑いの通知を受けた後、同社は未処理の請求に応じた。また、同社はCCPA対応システムを更新し、今後は請求を適時に承認・対応できるようにした。

S&K Brussels

© S&K Brussels LPC 2021

事例7：子供向け玩具販売会社がプライバシーポリシーを更新した

業種：子供向け玩具の販売
論点：(1)プライバシーポリシーのコンプライアンス違反、(2)請求方法なし、(3)CCPA上の消費者請求に料金徴収
事例：

- 子供向け玩具販売会社が、必要なCCPA上の消費者の権利の通知を提供しておらず、消費者がCCPA上の知る権利・削除請求権を行使する方法を提供しておらず、開示した個人情報の種類を表示しておらず、過去12カ月間に個人情報を売却したかどうかを明記していなかった。
- 同社のプライバシーポリシーにおいて、消費者からの知る請求を処理するために手数料を請求する可能性があると主張している。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新して、これらの問題に対処した。

S&K Brussels

© S&K Brussels LPC 2021

事例8：食料品店チェーンのロイヤルティプログラムで、金銭的インセンティブ通知の提供を必須化した

業種：食料品店
論点：金銭的インセンティブの未通知
事案：

- 食料品店チェーンを運営する事業者において、消費者が会社のロイヤルティプログラムに参加するために、個人情報を提供する必要があった。
- 同社は、これらのロイヤリティプログラムに参加している消費者に、金銭的インセンティブの通知を提供していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを修正し、金銭的インセンティブ通知を追加した。

S&K Brussels

© S&K Brussels LPC 2021

事例9:オンラインの求人広告会社がプライバシーポリシーを更新した

業種:オンラインプラットフォーム
論点:プライバシーポリシーのコンプライアンス違反
事案:

- オンライン求人広告プラットフォームを運営する事業者が、必要なCCPA上の消費者の権利(知る権利、削除請求権、差別されない権利など)を通知しなかった。
- また、同社は過去12カ月間に個人情報を売却したか、または事業目的で個人情報を転送したかどうかについても明言していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新し、CCPAにおいて必要とされる権利を含め、事業目的で他者に転送する個人情報の種類を明記し、個人情報を売却しなかった旨を明言した。
- しかし、更新されたプライバシーポリシーは不必要に法律専門用語が用いられているなど、一般的な消費者にとって読みにくく理解しにくいものであった。
- 同社は、更新されたプライバシーポリシーがCCPA規制に準拠していない旨の2回目の通知を受領した。
- 同社はこの指摘に対処するためにプライバシーポリシーを大幅に改訂した。

S&K Brussels

© S&K Brussels LPC 2021

事例10：メディア複合会社がオプトアウトプロセスおよび通知を更新した

業種：マスメディア・エンターテイメント
論点：(1)オプトアウトプロセスのコンプライアンス違反、(2)消費者への通知
事案：

- マスメディア・エンターテインメントの事業者が、個人情報売却のオプトアウトの方法を消費者に提供していなかった。
- 同社は、オンライン広告を管理するための第三者業界団体のツールに消費者を誘導しただけであった。
- また、同社のプライバシーポリシーやオプトアウト権の通知には、消費者や代理人がオプトアウト権を行使する方法についての必須情報が含まれていなかった。
- 同社は収集時に通知を行っておらず、デジタル資産の一部に「Do Not Sell My Personal Information」のリンクがなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はオプトアウトプロセス、プライバシーポリシー、および通知を更新してこれらの問題に対処し、「Do Not Sell My Personal Information」のリンクをすべてのデジタル資産に追加した。

S&K Brussels

© S&K Brussels LPC 2021

事例11：データブローカーがオプトアウト方法を更新した

業種：位置データ
論点：オプトアウトプロセスのコンプライアンス違反
事案：

- 位置データブローカーのオプトアウトプロセスは、オプトアウト選択を実施するためにモバイルデバイスの設定を変更するよう消費者を誘導するものであった。
- 同社はまた、消費者が同社のデータ収集をオプトアウトできるようにするためのウェブフォームを提供していたが、このウェブフォームで消費者の個人情報の売却をオプトアウトできるかは明らかにしていなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はオプトアウトページを更新し、ウェブフォームにおいて、消費者がCCPAにおけるオプトアウト権を完全に実施にできる旨を目立つ形で掲載した。
- また、モバイルデバイスの設定を変更することで将来のトラッキングが制限されるが、CCPA上のオプトアウト請求は実施されない旨を明記した。

S&K Brussels

© S&K Brussels LPC 2021

事例12：自動車メーカーが収集時に対面で通知を実施し、プライバシーポリシーと欠陥のあった請求方法を更新した

業種：自動車
論点：(1)消費者への通知、(2)プライバシーポリシーのコンプライアンス違反、(3)着信課金用電話番号なし、(4)請求提出方法の欠陥
事案：

- 自動車メーカーは、試乗した消費者から情報を収集したが、収集時に通知をしていなかった。
- 同社のプライバシーポリシーには、CCPA上の権利の説明や、認定代理人が請求を提出する方法が含まれていなかった。
- また、CCPA上の消費者請求を行った消費者に着信課金用電話番号を提供しておらず、知る請求・削除請求を提出する方法としてオンラインでの方法を提供していたが、機能していなかった。
- コンプライアンス違反の疑いの通知を受けた後、オンラインで収集するかまたは対面で収集するかにかかわらず、試乗に関連する個人情報の収集時に通知を実施した。
- 同社はプライバシーポリシーを更新して消費者のCCPA上の消費者の権利に関する必要な開示を追加、着信課金用電話番号を記載、機能していなかったCCPA上の消費者請求をオンラインで提出する方法を修正した。

・本事例におけるCCPA違反の類型は多岐にわたっており、CPRA適用開始以降に同様の事例が調査された場合には、民事制裁金の賦課に至る可能性が特に高い事例と考えられる。

S&K Brussels

© S&K Brussels LPC 2021

事例13：ペット産業のウェブサイトで消費者が個人情報のあらゆる売却をオプトアウトするためのオプトアウトウェブフォームを更新した

業種：ペット産業
論点：(1)認定代理人、(2)個人情報の売却
事案：

- オンラインでペット引き取りプラットフォーム運営している事業者が、消費者がCCPA上の権利を発動する際に、消費者の認定代理人に公的な証明書を提出するよう求めていた。
- 同社のデータの売却に関する開示は分かりにくく、消費者が個人情報の売却をオプトアウトする仕組みを提供していないように思われた。
- また、オンライン広告を管理するための第三者業界団体のツールに消費者を誘導させ、さらなる手順を消費者に行わせた。
- コンプライアンス違反の疑いの通知を受けた後、同社は代理人の公的な証明書の要求を削除し、「Do Not Sell My Personal Information」のリンクを追加し、消費者が個人情報（ターゲティング広告のために提供した個人情報を含む）の売却から完全にオプトアウトできるようオプトアウトウェブフォームを更新した。

S&K Brussels

© S&K Brussels LPC 2021

事例14：食料品チェーンが、消費者が認定代理人を通じて請求を提出する方法を説明するための開示を更新した

業種：食料品店
論点：(1)認定代理人、(2)プライバシーポリシーのコンプライアンス違反
事案：

- 食料品店チェーンを運営している企業が、認定代理人がCCPA上の消費者請求を顧客の代理として提出する方法に関する情報を提供しておらず、プライバシーポリシーにおいてもその他事項の欠落があった。
- この明らかな違反について民間およびカリフォルニア州司法長官オフィスから通知を受けた後、同社はプライバシーポリシーを更新して、認定代理人が消費者の代理人としてCCPA上の消費者請求を提出する方法、および請求を確認するための同社の要件を記載した。

S&K Brussels

© S&K Brussels LPC 2021

事例15：モバイルアプリゲーム会社が個人情報の売却を停止し、未成年者に対する保護を更新した

業種：オンラインゲーム
論点：(1)個人情報の売却、(2)未成年者の個人情報の売却
事案：

- モバイルアプリゲームを運営する事業者が、サードパーティ製のモバイル広告プラットフォームから、13歳から15歳までの未成年者を含むプレーヤーの個人情報を取得するためのソフトウェアをインストールした。
- 同社は成人にオプトアウトの仕組みを提供しておらず、未成年者のためのオプトインを得ていなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社は当該広告ソフトウェアを削除し、年齢制限や保護者による検証機能など、若年ユーザー向けのその他プライバシー保護を導入した。

・未成年者の個人情報の収集等におけるオプトイン同意の取得等の問題に関して執行リスクが比較的高いことは、データ保護の分野で一般的であるが、特に、サードパーティ製のソフトウェアが関連する場合は注意が必要であるといえる。

S&K Brussels

© S&K Brussels LPC 2021

事例16：ソーシャルメディア会社が個人情報の売却を停止し、プライバシーポリシーを更新した

業種：ソーシャルメディアプラットフォーム
論点：(1)消費者への通知、(2)個人情報の売却
事案：

- ソーシャルメディアプラットフォームを立ち上げプライバシーを保護しているとして宣伝していた企業が、CCPA上の権利について消費者に通知しなかった。
- また、ユーザーのオンライン活動に関する個人情報をさまざまなサードパーティの分析会社に提供したが、必要な通知を行わず、消費者が個人情報の売却をオプトアウトする方法を提供していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新し、アプリとウェブサイトからすべてのサードパーティ製トラッカーを削除した。

・開示された事実から詳細は明らかではないものの、サードパーティの分析会社に対するユーザーのオンライン活動に関する個人情報の提供を、被疑会社のアプリとウェブサイトから全てのサードパーティ製トラッカーを削除することによってカリフォルニア州司法長官からの不遵守通知への対応を行ったものと考えられる。

・ウェブサイトについてはCCPAに準拠したクッキー同意管理ツールを使用することで、ウェブサイトへの訪問者である消費者に対して個人情報の売却に関するオプトアウト権を提供することが可能であったはずであり、アプリに関しても同様に同意管理ツールを使用することによるCCPA対応が可能であったと考えられる。

S&K Brussels

© S&K Brussels LPC 2021

事例17：メーカーと小売店が個人情報の売却を停止した

業種：家電
論点：個人情報の売却
事案：

- 電子機器を販売している事業者が、消費者のオンラインショッピングに関するデータを広告主と共有している小売サイト上で、サードパーティ製のオンライントラッカーを使用していた。
- 同社はこのサードパーティとサービス提供者契約を締結しておらず、また、ユーザーが使用できるグローバルプライバシー制御（グローバルプライバシー制御の信号を送るブラウザ拡張機能など）により提出されたオプトアウトに対する消費者の請求も処理していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーベンダーと協力して、消費者のオプトアウト請求を実施し、CCPAに違反した売却条件の下でサードパーティと個人情報を共有しないようにした。

・カリフォルニア州司法長官オフィスは、グローバルプライバシー制御の信号を送るブラウザ拡張機能等によって提出されたオプトアウトに対する消費者の請求に関しては、CCPA上のオプトアウト権の行使として取り扱う必要があるという立場を取っているものと考えられる。

S&K Brussels

© S&K Brussels LPC 2021

事例18：メディア複合会社がオプトアウト方式を更新し、「Do Not Sell My Personal Information」のリンクを追加した

業種：デジタルメディア
論点：(1)オプトアウトプロセスのコンプライアンス違反、(2)請求方法なし
事案：

- メディア複合会社である事業者が、ポートフォリオ内の各ウェブサイトで、消費者が個人情報の売却をオプトアウトする際に、消費者に複数の個別の請求を提出することを請求していた。また、デジタル資産の一部には「Do Not Sell My Personal Information」のリンクがなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はオプトアウトプロセスを更新してオプトアウト請求を単純化し、「Do Not Sell My Personal Information」のリンクをすべてのデジタル資産に追加した。

S&K Brussels

© S&K Brussels LPC 2021

事例19：国内食料品店チェーンがプライバシーポリシーを更新し、請求方法を追加した

業種：食料品店
論点：プライバシーポリシーのコンプライアンス違反
事案：

- 食料品店チェーンを運営している企業が、個人情報の収集と使用に関する情報をプライバシーポリシーで開示しておらず、消費者のCCPA上の消費者の権利（知る権利、削除請求権、差別されない権利など）の通知を行っておらず、知る請求、削除請求、個人情報の売却をオプトアウトする請求の提出方法について消費者に通知していなかった。
- コンプライアンス違反の疑いの通知を受けた後、CCPAにおいて求められる情報をプライバシーポリシーに追加し、消費者がCCPA上の消費者請求を提出できるプロセスを実装し、個人情報を売却していない旨を明言した。

S&K Brussels

© S&K Brussels LPC 2021

事例20：メールニュースレタープラットフォームがプライバシーポリシーを更新し請求方法を追加した

業種：メール購読プラットフォーム
論点：プライバシーポリシーのコンプライアンス違反
事案：

- 購読ベースのメールニュースレターのプラットフォームのプライバシーポリシーにおいて、必要なCCPA上の消費者の権利（知る権利、削除請求権、差別されない権利など）の通知が行われておらず、知る請求・削除請求の提出方法が消費者に十分に通知されていなかったため、コンプライアンス違反状態であった。
- また、同社は過去12カ月間に個人情報を売却したか、または事業目的で個人情報を転送したかどうかについても明言していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新して必要なCCPA上の消費者の権利を追加し、事業目的で転送した個人情報を列挙し、CCPA上の消費者請求の提出方法を指定し、個人情報を売却しなかった旨を明言した。

S&K Brussels

© S&K Brussels LPC 2021

事例21：オンラインイベント販売会社がプライバシーポリシーを更新し、請求方法を追加した

業種：オンラインイベント販売
論点：(1)プライバシーポリシーのコンプライアンス違反、(2)請求方法なし
事案：

- イベントのチケットを販売するオンライン事業者が、プライバシーポリシーにおいて必要なCCPA上の消費者の権利（知る権利、削除請求権、差別されない権利など）の通知を行っておらず、コンプライアンス違反状態であった。
- 同社はプライバシーポリシーにおいてCCPA上の消費者の権利を行使する方法を消費者に説明しておらず、過去12カ月間に個人情報を売却または開示したかどうかを明記していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新し、必要な情報を追加した。また、個人情報を売却していない旨を明言した。

S&K Brussels

© S&K Brussels LPC 2021

事例22：デジタルパートナーが自社の義務を明確にした

業種：デジタル体験提携
論点:(1)プライバシーポリシーのコンプライアンス違反、(2)消費者への通知、(3)「Do Not Sell My Personal Information」のリンクなし
事案：

- 大手企業と提携してデジタル戦略を展開する企業が、CCPAにおける自社の義務を果たしていなかった。同社のプライバシーポリシーにおいてCCPA上の権利について消費者に通知しておらず、個人情報の収集・使用・売却方法についても十分な通知を行っていなかった。
- また、消費者が会社のウェブサイトや電話で請求を行う方法も説明していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新し、CCPA上の権利および通知に関して明記した。
- また、「Do Not Sell My Personal Information」のリンクを追加し、消費者が請求を提出するためのメールアドレスと電話番号を記載した。

S&K Brussels

© S&K Brussels LPC 2021

事例23：データブローカーが、「Do Not Sell My Personal Information」のリンクを更新し、オプトアウト請求時の検証とアカウント作成の要求を停止した

業種：データブローカー
論点：(1)「Do Not Sell My Personal Information」のリンクなし、(2)本人確認、本人確認のためのアカウント作成
事案：

- データブローカーが「Do Not Sell My Personal Information」のリンクを掲示していたが、機能していなかった。
- また、個人情報の売却をオプトアウト請求する際、政府発行の身分証明書のコピーと消費者の住所が記載されている申告書を用いた本人確認を必須としていた。
- 消費者が請求を実施するにあたり消費者にアカウントを作成することを要求していた。
- コンプライアンス違反の疑いの通知を受けた後、同社は「Do Not Sell My Personal Information」のリンクを更新し、消費者が個人情報の売却をオプトアウトする際の本人確認を無くし、消費者がCCPA上の消費者請求を行うためにアカウントを作成しなくてもよいこととした。

S&K Brussels

© S&K Brussels LPC 2021

事例24:テレビゲーム配信会社がプライバシーポリシーを更新した

業種:テレビゲーム配信
論点:プライバシーポリシーのコンプライアンス違反
事案:

- テレビゲーム配信会社のプライバシーポリシーにおいて、必要なCCPA上の消費者の権利が通知されておらず、開示した個人情報の種類を記載しておらず、過去12カ月間に個人情報を売却したかどうかを記載していなかったため、コンプライアンス違反状態であった。
- 同プライバシーポリシーにおいて、消費者がCCPA上の知る権利・削除請求権を行使する方法について、誤った指示を出していた。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新して、これらの問題に対処した。

S&K Brussels

© S&K Brussels LPC 2021

事例25：教育技術会社がプライバシーポリシーを更新し、「Do Not Sell My Personal Information」のリンクを追加した

業種：教育技術
論点：(1)プライバシーポリシーのコンプライアンス違反、(2)請求方法なし、(3)「Do Not Sell My Personal Information」のリンクなし
事案：

- 学校・高等教育機関・事業者へオンライン学習プラットフォームを提供している教育技術企業が、そのプライバシーポリシーにおいて、(1)知る権利・削除請求権・差別されない権利などのCCPAにおける消費者権利の通知を行っておらず、(2)消費者がCCPAの権利を行使して知り削除する請求を行う方法を記述しておらず、(3)過去12カ月間に開示または売却した個人情報の種類を記述していなかったため、コンプライアンス違反状態であった。
- また、同社のホームページには「Do Not Sell My Personal Information」のリンクがなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新してこれらの問題に対応し、ホームページに「Do Not Sell My Personal Information」のリンクを追加した。

S&K Brussels

© S&K Brussels LPC 2021

事例26：衣料品販売店がプライバシーポリシーを更新し、請求方法を追加した

業種：オンライン衣料品販売店
論点：プライバシーポリシーのコンプライアンス違反
事案:

- オンライン衣料品販売店のプライバシーポリシーにおいて、必要なCCPA上の消費者の権利（知る権利、削除請求権、差別されない権利など）の通知が行われておらず、知る請求・削除する請求の提出方法が消費者に通知されていなかったため、コンプライアンス違反状態であった。
- また、同社は過去12カ月間に個人情報を売却したか、または事業目的で個人情報を転送したかどうかについても明言していなかった。
- コンプライアンス違反の疑いの通知を受けた後、同社はプライバシーポリシーを更新して必要なCCPA上の消費者の権利を追加し、事業目的で転送した個人情報を列挙し、CCPA上の消費者請求の提出方法を指定し、個人情報を売却しなかった旨を明言した。

S&K Brussels

© S&K Brussels LPC 2021

事例27：データブローカーが「Do Not Sell My Personal Information」のリンクを追加した

業種：データベース・ディレクトリ販売
論点：請求方法なし
事案：

- 消費者の個人情報を含む専門的な連絡先ディレクトリを販売するデータブローカーが、そのホームページに「Do Not Sell My Personal Information」のリンクを掲載していないことを発見したというレポートが消費者擁護団体により公開された。
- 当該レポートおよび司法長官オフィスからの通知により、CCPAの違反が同社の知るところとなった。
- 同社は「Do Not Sell My Personal Information」のリンクをホームページに加えることで対応した。

S&K Brussels

© S&K Brussels LPC 2021

参考資料②：BtoB企業が収集している個人情報とCPRAの適用関係

S&K Brussels

© S&K Brussels LPC 2021

BtoB企業が収集している個人情報とCPRA

- BtoB企業が収集している個人情報は、CPRAとの関係では、以下の類型に整理することができる。

A) CPRA一部規定の適用猶予の対象となる以下の個人情報

1. 役職員等の雇用関連個人情報
2. 取引先の従業員の個人情報
   - ✓ 従業員/契約受託先のプライバシーの利益も保護されるべきであるが、従業員/契約受託先と事業者の関係は、消費者と事業者の関係とは異なるため、当該保護においても相違点が考慮されるべきである。また、CPRAはNational Labor Relations Actの下での組合加入権や団体交渉に干渉することを意図したものではない。それがCCPA上の従業員およびBtoBコミュニケーションのための適用除外を2023年1月1日まで延長することとした目的および意図である（SEC. 3. Purpose and Intent, A. Consumer Rights, para 8）。

B) CPRA一部規定の適用猶予の対象とならない以下の個人情報

3. ウェブサイトへの訪問者の個人情報（クッキーを通じた取得）
4. それ以外の個人情報、例えば
   - ✓ 自社ウェブサイトの問い合わせフォームからの連絡
   - ✓ マーケティングを通じて収集する個人情報のうち上記2の適用猶予対象となる文脈以外で取得したもの

S&K Brussels

© S&K Brussels LPC 2021

A) CPRA一部規定の適用猶予の対象
1. 役職員等の雇用関連個人情報

■ 以下の役職員等の雇用関連個人情報について、以下の範囲に限りCPRAの一部の規定の適用が2023年1月1日まで猶予される。

適用猶予となる個人情報	適用猶予となる利用目的の範囲
事業者の求職者、従業員、所有者、役員、オフィサー、医療スタッフメンバーまたは契約受託先（「**役職員等**」）として行動する過程において、当該事業者が当該自然人について収集する個人情報	当該自然人の個人情報が、役職員等としての当該自然人の役割または以前の役割の文脈内でのみ収集および使用されるもの
事業者が収集する、役職員等として行動する自然人の緊急連絡先である個人情報	当該個人情報が専ら緊急連絡先をファイルに入れる文脈内で収集および使用されるもの
役職員等として行動する自然人に関連する他の自然人の特典を管理するために保有が必要な個人情報	当該特典を管理する文脈内でのみ収集および使用されるもの

- ✓ 役職員等の雇用関連個人情報の収集の一部には適用猶予とならないものがある。
  - ✓ 適用猶予となる範囲から外れる可能性があるもの→外れると全てのCPRAの規定の適用を受ける
    - ✓ 日本本社が、①米国子会社での幹部候補者の採用を承認するためにCVを受け取る（「事業者」の「求職者」ではない）、②米国子会社所属の駐在員の個人情報を収集する（「事業者」の「従業員」ではない場合）、③日本本社のグローバル内部通報制度によって米国子会社の従業員からの通報を受け取る（「事業者」の「従業員」ではない）等
    - ✓ 役職員の家族の個人情報を収集・使用する
    - ✓ 事業所の防犯カメラに撮影された従業員の映像に含まれる個人情報を防犯目的以外で使用する
    - ✓ 従業員の人事評価に関する情報を担当者以外の他の従業員と共有する
  - ✓ 役職員等の個人情報についてもCPRA対応のためのデータマッピングを行うことが必要
- ✓ 2023年1月1日より前に適用猶予の期限を延期または恒久化する法改正がなされなければ、役職員等の個人情報について適用猶予されているCPRAの他の規定も全て適用されることになる。

S&K Brussels

© S&K Brussels LPC 2021

A) CPRA一部規定の適用猶予の対象
1. 役職員等の雇用関連個人情報

- 役職員等の雇用関連個人情報についてCPRAの適用が猶予される場合であっても、以下については適用が猶予されず、（CPRAによる改正前の）CCPAが適用されている。
  - ① 収集する個人情報の種類とその利用目的についての、収集時または収集前の、消費者への通知義務
    - ✓ CPRAによって当該通知義務は以下の通り拡張されるため、2023年1月1日以降は、以下の内容を通知に含められるように事前に準備が必要である。
      1. 当該個人情報が共有されるか。
      2. 収集されるセンシティブ個人情報の類型および当該センシティブ個人情報の類型が収集または使用される目的および当該情報が売却または共有されるか。
      3. センシティブ個人情報を含む個人情報の各類型の保持を意図する期間、または、それが可能でない場合、当該期間を定めるために使用される基準
  - ② 通知未提供での新たな個人情報の類型の収集禁止および目的外利用の禁止
    - CPRAによって当該禁止の対象に、通知未提供での新たなセンシティブ個人情報の類型の収集禁止および目的外利用の禁止が追加された
  - ③ 個人情報が漏洩した場合に消費者に付与される損害賠償請求権
    - CPRAによって、「パスワードまたはセキュリティ上の質問との組み合わせの電子メール・アドレスおよびそのアカウントへのアクセスが許可される回答が、無権限アクセス、流出、窃取または開示の対象となった場合」についても、これが個人情報を保護するため情報の性質に適切な合理的なセキュリティ手続きとプラクティスを実施し維持する義務に事業者が違反した結果として起こった場合には、消費者に付与される損害賠償請求権に含まれることとなった。
- CPRAによって以下の事業者の義務が適用猶予されないものとして追加された。
  - ④ 開示された利用目的に合理的に必要とされる期間を超える消費者の個人情報・センシティブ個人情報の保持の禁止（保持期間の制限）

S&K Brussels

© S&K Brussels LPC 2021

A) CPRA一部規定の適用猶予の対象
2. 取引先の担当者の個人情報

- BtoBの文脈での取引先の担当者の個人情報についても、CPRAの一部の規定の適用が2023年1月1日まで猶予される。

適用猶予となる個人情報	適用猶予となる範囲
消費者が、会社、パートナーシップ、個人事業主、非営利または政府機関（「会社等」）に対して従業員、所有者、役員、オフィサーまたは契約受託先として活動する自然人である場合（消費者が会社等の役職員等である場合）に、事業者と消費者との間の書面または口頭による連絡または取引を反映した個人情報	事業者との連絡または取引が、以下の文脈に限って生じる場合 ①消費者が所属している会社等に関して事業者がデューディリジェンスを実施する、 ②当該会社等に対する商品やサービスの提供、または ③当該会社等からの商品やサービスの受領

- 上記適用猶予規定は、あらゆるBtoBの文脈での取引先の担当者の個人情報の収集、利用、移転に適用されるものではない。
  - ✓ BtoBの文脈で収集した取引先の担当者の個人情報を商品やサービスの提供や受領の文脈とは異なる文脈でマーケティングに用いた場合
    - ✓ 取引先の担当者の名刺を、当該担当者の所属先の会社等への商品やサービスの提供とは無関係に、当該担当者個人に対する連絡に用いた場合
      - ✓ 例えば、一般的な市況に関するものをはじめとする商品やサービスの提供と無関係な情報交換への誘い、ヘッドハンティングの声掛け、個人的な会食への誘い等
- ✓ BtoBの取引先の担当者の個人情報についてもCPRA対応のデータマッピングが必要
- ✓ 2023年1月1日より前に適用猶予の期限を延期または恒久化する法改正がなされなければ、BtoBの取引先の担当者の個人情報について適用猶予されているCPRAの他の規定も全て適用されることになる。

S&K Brussels

© S&K Brussels LPC 2021

A) CPRA一部規定の適用猶予の対象
2. 取引先の担当者の個人情報

- BtoBの文脈での取引先の担当者の個人情報についてCPRAの適用が猶予される場合であっても、以下については適用が猶予されず、（CPRAによる改正前の）CCPAが適用されている。
  - ① オプトアウトの権利に伴う義務
    - ✓ オプトアウトの権利を認める必要のある「売却」または「共有」に該当する個人情報の移転がないかを確認する必要がある。
      - ✓ 例えば、米国子会社が、取引先の担当者の名刺に記載された個人情報を、日本企業（日本本社）へ移転している場合がこれに該当する可能性がある。
  - ② 消費者を差別的に取り扱わない権利に伴う義務
  - ③ 個人情報が漏洩した場合に消費者に付与される損害賠償請求権
    - CPRAによって、「パスワードまたはセキュリティ上の質問との組み合わせの電子メール・アドレスおよびそのアカウントへのアクセスが許可される回答が、無権限アクセス、流出、窃取または開示の対象となった場合」についても、これが個人情報を保護するため情報の性質に適切な合理的なセキュリティ手続きとプラクティスを実施し維持する義務に事業者が違反した結果として起こった場合には、消費者に付与される損害賠償請求権に含まれることとなった。
    - ✓ 個人情報が漏洩した場合には、取引先の担当者等から損害賠償請求がなされる可能性がある。
    - ✓ 個人情報の性質に照らして合理的なセキュリティの手続と慣行が実装されているかを確認する必要がある。

S&K Brussels

© S&K Brussels LPC 2021

A) CPRA一部規定の適用猶予の対象

個人情報が漏洩した場合に消費者に付与される損害賠償請求権の行使を防ぐため、BtoB事業者も守らなければならないこと

1. **個人情報を保護するため、情報の性質に応じた合理的なセキュリティ手続きとプラクティスを実施し、**
   - ✓ 業務ごとに処理する個人情報の性質からプライバシーリスクを評価し、これに相応する管理策を定め、社内ルールとして実施すること
   - ✓ 処理する個人情報の性質に見合ったセキュリティ対策が必要
     - ✓ カリフォルニア州司法長官（カマラ・ハリス米副大統領）が2016年に2月に出したCalifornia Data Breach Report での推奨策としてはCenter for Internet Security（CIS）のCritical Security Controls（CSC）の20の管理策を最低限の実装として推奨している。
       - ✓ CIS Control® V8（英語版）
         - ✓ https://learn.cisecurity.org/cis-controls-download
2. **1798.81.5 条(d)(1)(A)に定める個人情報または「パスワードまたはセキュリティ上の質問との組み合わせの電子メール・アドレスおよびそのアカウントへのアクセスが許可される回答」が、**
   - ✓ 前者（1798.81.5 条(d)(1)(A)に定める個人情報）はカリフォルニア州民法典の「顧客記録」に定められる以下の定義となり、CCPAが定義する個人情報よりも狭くなっている。
     - ■ 個人のファーストネーム、もしくはファーストイニシャル＋ラストネームと、以下の情報の組み合わせ
       - ■ ソーシャルセキュリティ番号、運転免許証番号、カリフォルニア州IDカード番号、納税者番号、パスポート番号、軍用ID番号、特定の個人を確認する政府文書に、付与された固有の識別番号、銀行口座番号、クレジットカード・デビットカード番号とそれらのセキュリティコード、アクセスコード、パスワードの組み合わせ、医療情報、健康保険情報、特定の個人を認証するために使われる指紋等の生体情報
3. **暗号化や編集がされていない状態で、**
4. **無権限アクセス、流出、窃取または開示の影響下に置かれることを防ぐこと**

S&K Brussels

© S&K Brussels LPC 2021

B)CPRA一部規定の適用猶予の対象とならない個人情報
3. ウェブサイトへの訪問者の個人情報（クッキーを通じた取得）

- CPRAは、プロファイリングを、個人データの自動処理によって職場での成績、経済状況、健康状況、趣味嗜好、興味、扶養関係、行動、位置・移動などを予想することと定義。CPRAは、このようなプロファイリングを行う場合、情報提供およびオプトアウト権の付与を義務づける規則を今後制定する旨規定。
  - ✓ ターゲティング広告のように、閲覧履歴の分析により、閲覧者の趣味嗜好・購買傾向に関するプロファイリングを行う場合、情報提供およびオプトアウトが求められる。
- CCPAは、個人データを売却（おおむね、経済的なメリットのために委託先以外の者に開示する行為）に対するオプトアウト権を認めているが、CPRAはこれを一歩進め、個人データの共有（share）についても消費者のオプトアウト権を認める。「共有」は、事業者の利益のために、ウェブやアプリをまたがる消費者のネット上の行動履歴を共有、開示、移転することを含むこととされている。
  - ✓ CCPAでは、ターゲティング広告の効果を上げるという経済的利益のために第三者クッキーによる閲覧履歴を広告エージェンシーに共有することについて、これが「売却（sell）」に該当するかどうかについて議論があったが、CPRAでは共有がある時点でオプトアウトが求められる。

S&K Brussels

© S&K Brussels LPC 2021

B)CPRA一部規定の適用猶予の対象とならない個人情報
3. ウェブサイトへの訪問者の個人情報（クッキーを通じた取得）

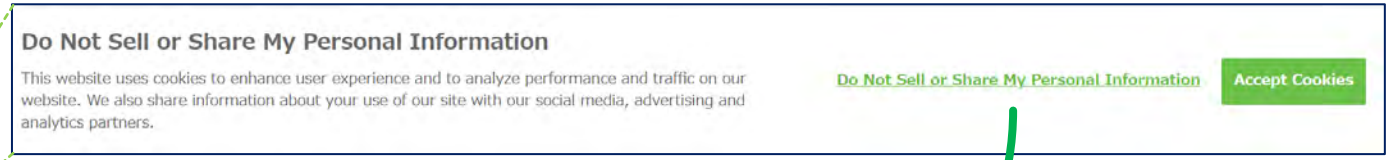
- ✓ 実装のポイント
  - ✓ クッキーバナーを利用してウェブサイト閲覧者のプロファイリング、ターゲティング広告を行う場合における情報提供
  - ✓ オプトアウト機会提供については、従来にも増して的確な対応が必要
  - ✓ 情報提供およびオプトアウト機会提供のために適切なクッキーバナーツールを実装すること
  - ✓ タグマネジャーの適切な設定により、ウェブサイト閲覧者の選択がクッキー設定に正確に反映されるように実装すること。
    - ✓ 実装が不適切な場合、法違反のリスク

S&K Brussels

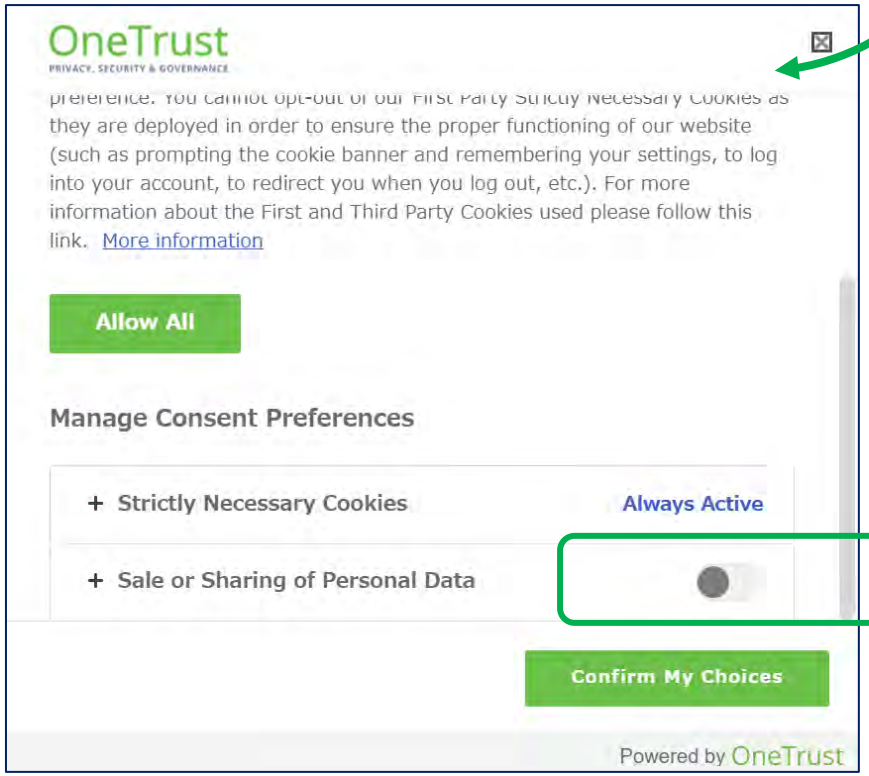
© S&K Brussels LPC 2021

B)CPRA一部規定の適用猶予の対象とならない個人情報
3. ウェブサイトへの訪問者の個人情報（クッキーを通じた取得）実装例

バナー第1層（概括的な情報提供）



“Do Not Sell or Share My Personal Information”のリンク



バナー第2層
（より詳細な情報提供と
オプトアウト機会提供）

オプトアウト

S&K Brussels

© S&K Brussels LPC 2021

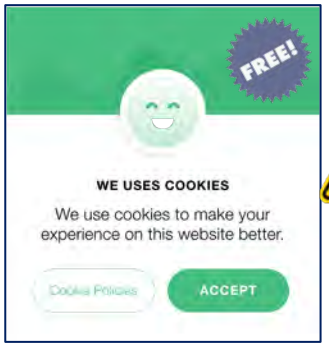
B)CPRA一部規定の適用猶予の対象とならない個人情報
3. ウェブサイトへの訪問者の個人情報（クッキーを通じた取得）
現実的な対応策

自社開発

デメリット

- ✓ システム開発以外に専門的な法律知識が必要
- ✓ ユーザがクッキー取扱にオプトアウトした際の記録管理が難しい
- ✓ 法改正にあわせシステム更新が必要
- ✓ 開発コストが膨大
- ✓ 開発のためのリソースの確保が困難

フリーツール



デメリット

- ✓ 法律の要件にあったクッキーバナーを表示できない
- ✓ ユーザーのアクセス元の判定による法域ごとのバナー出し分けができない
- ✓ 細かいカスタマイズができない
- ✓ オプトアウトの実装が難しい、もしくは対応できない

- ■ 多くの利用実績のあるクッキーバナーツールの利用が現実的
- ■ クッキーツール導入サービスの利用も費用対効果が比較的高い
- ■ 日本語対応サポートサービスもある方が楽（CPRAのみならず、日本、ブラジル、タイ、中国、インド等の法規制のクッキー対応が必要）

S&K Brussels

© S&K Brussels LPC 2021

B)CPRA一部規定の適用猶予の対象とならない個人情報
4. それ以外の個人情報

- ✓ BtoB企業であっても、役職員の雇用関連個人情報や取引先の従業員の個人情報を、適用猶予規定が定めるのと異なる文脈で収集・使用したり、それら以外の個人情報を収集する場合には、以下に代表される一連のCPRA対応を全て実行しなければならなくなる。そのような場合に該当するか否かは、CPRAに準拠したデータマッピングの質問票によって、詳細にデータマッピングを行わなければ、正確に判断することは難しい。
  - ✓ CPRAにおいて要求される開示事項をプライバシー通知に入れ込むために改訂する
  - ✓ CPRA上の新しいプライバシー権の行使を受け取り、回答しおよび有効化するために、ポリシーならびに消費者に面したメカニズムをアップデートする
  - ✓ 事業目的で個人情報を売却し、共有しまたは開示するサービス提供者、契約受託先および第三者を特定し、テンプレートの契約文言を作成する
  - ✓ 必要性および比例性の原則を遵守するため、個人情報の収集、使用、保持および共有を管理するポリシーおよび手続を準備する
  - ✓ センシティブ個人情報の処理、自動化された意思決定技術（プロファイリングを含む）の使用およびクロスコンテクスト行動広告の使用に関するCPRA上の義務を分析し運用する
  - ✓ サイバーセキュリティ監査およびリスク評価枠組を発展させる
  - ✓ センシティブ個人情報用のものを含む、データ保持ポリシーを準備する
  - ✓ トレーニング文書のアップデートおよびトレーニングセッションの実行
  - ✓ 今後公表されるCPRA規則の解釈

S&K Brussels

© S&K Brussels LPC 2021

参考資料③:カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool

© S&K Brussels LPC 2021

カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool

- カリフォルニア州司法長官オフィスは、2021年7月に、消費者が、CCPAに違反した可能性のある事業者に対して送付するための不遵守の通知をドラフトすることを助けるツールを公表した（https://oag.ca.gov/consumer-privacy-tool）。
- このツールは、現状では、容易に発見可能な”Do Not Sell My Personal Information”リンクを自社のウェブサイトに備えていない事業者に対する通知のドラフティングに限られているものの、今後、他の潜在的なCCPA違反を含む可能性がある。このツールを通じて司法長官オフィスが収集した情報は調査および執行に使用されることに注意が必要である。

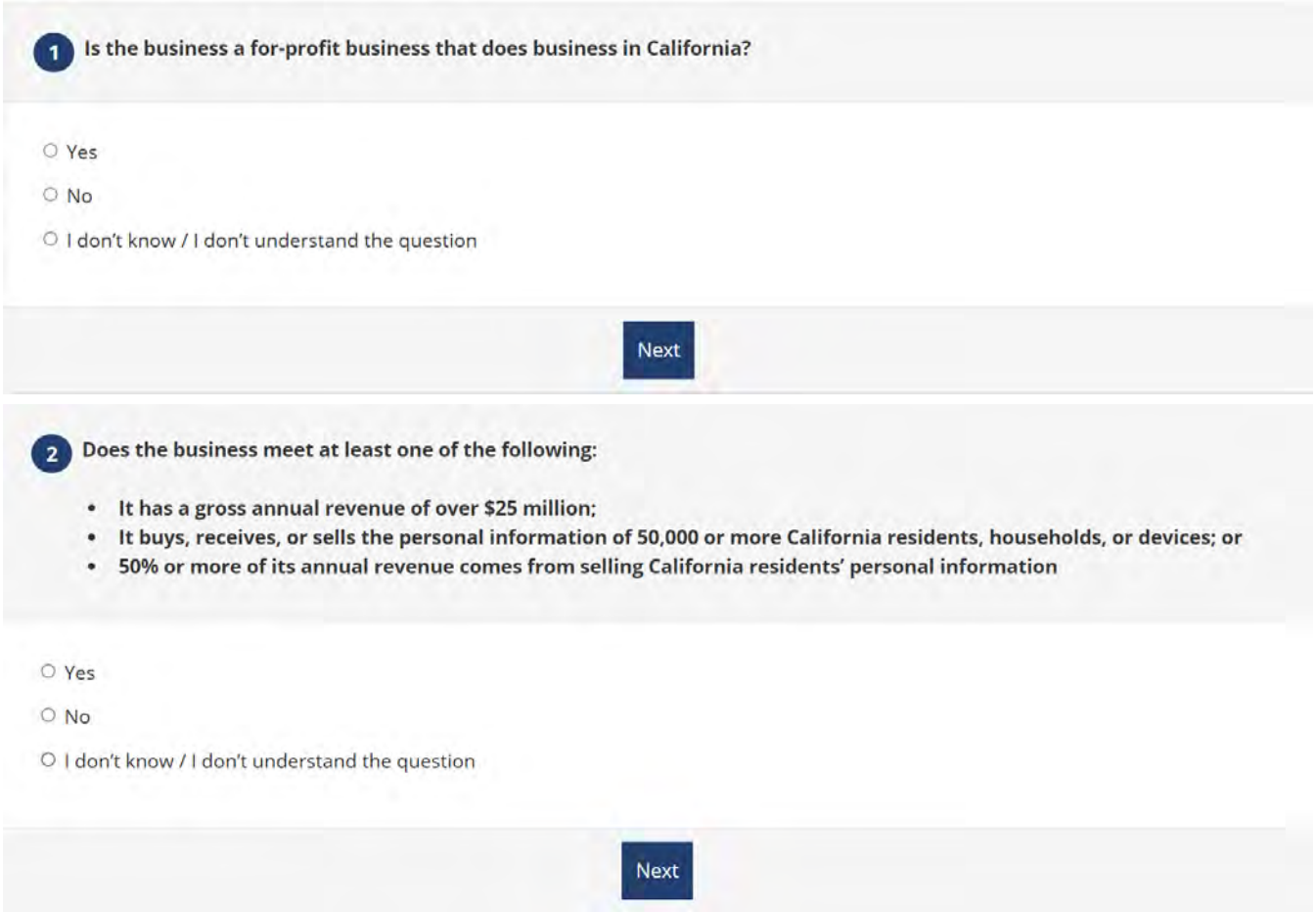
  “This tool is not legal advice. The Office of the Attorney General provides this tool as a resource but takes no position on the truthfulness of the information submitted or on whether a business has violated the CCPA. Please note that the ***OAG collects the information you provide in the tool to assist us in investigating and enforcing the law.*** *This information may be also be subject to a public records act request.”*
- カリフォルニア州司法長官オフィスは、30日間の治癒期間が、このツールを使って作成された不遵守の通知を含む電子メールの事業者への送付によって開始され得るという立場を取っている（https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-first-year-enforcement-update-california）ため、今後、執行はより容易になる可能性が高い。

  “The tool, available here, asks guided questions to walk consumers through the basic elements of the CCPA before generating a notification that the user can then email to the business. ***This email may trigger the 30-day period for the business to cure their violation of the law****, which is a prerequisite to the Attorney General bringing an enforcement action. The tool does not constitute legal advice.“*

© S&K Brussels LPC 2021

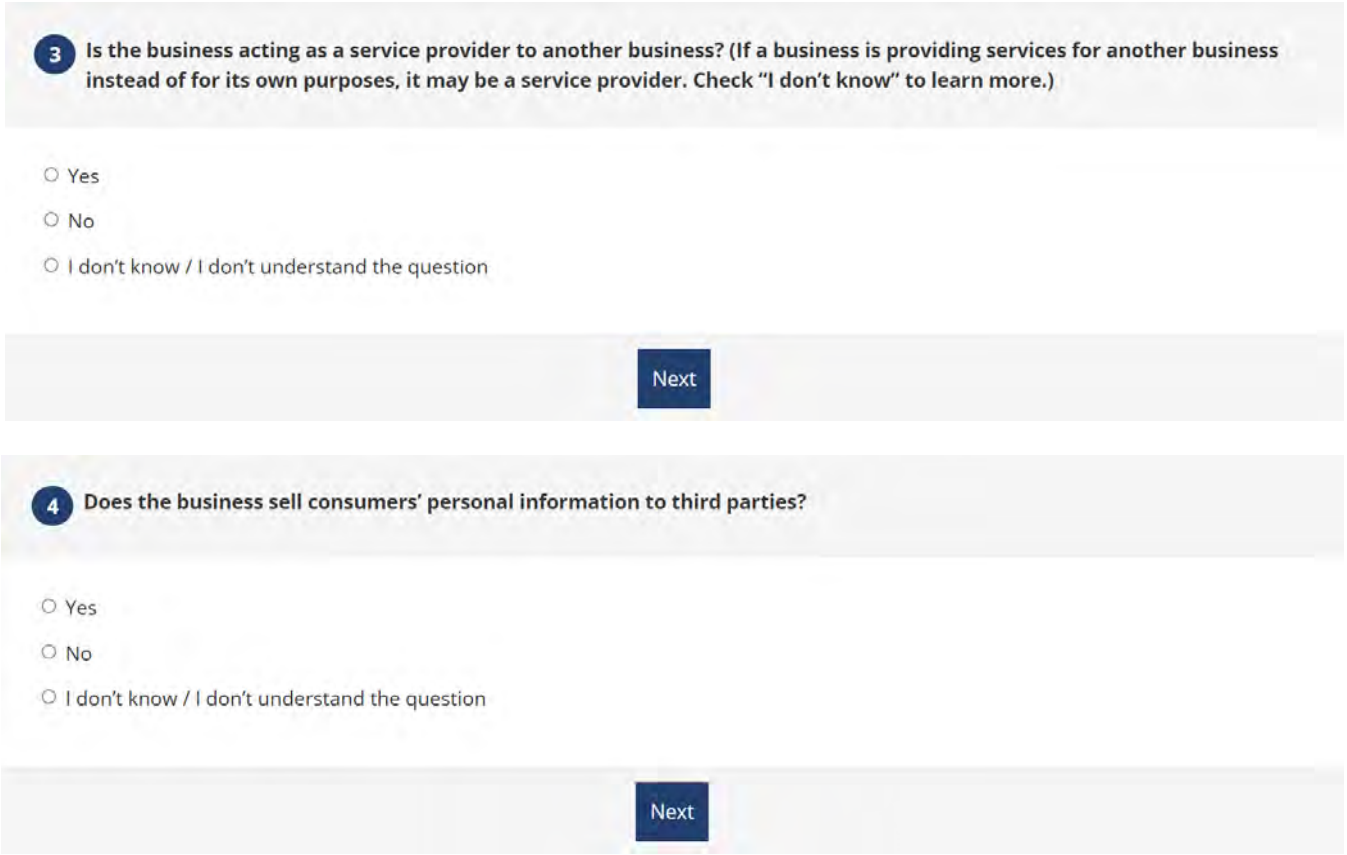
カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool

■このToolは設問1から5まであり、CCPAの適用がある事業者が個人情報を販売していて、かつ”Do Not Sell My Personal Information”のリンクをウェブサイトに掲示していない場合にDraft Noticeを作成する情報を入力するフォームが現れるように設計されたウェブフォームである。



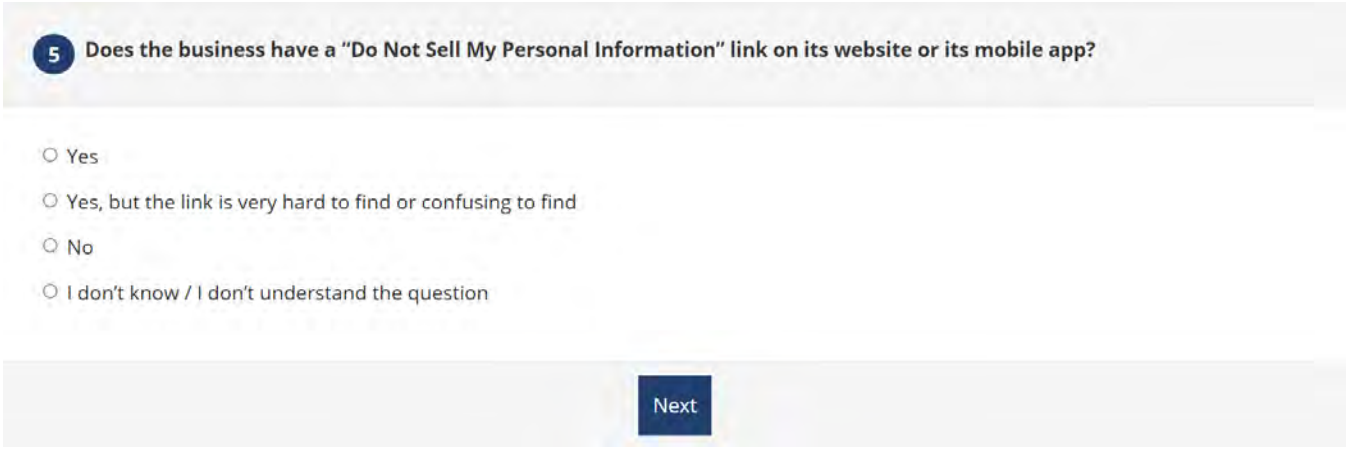
© S&K Brussels LPC 2021

カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool

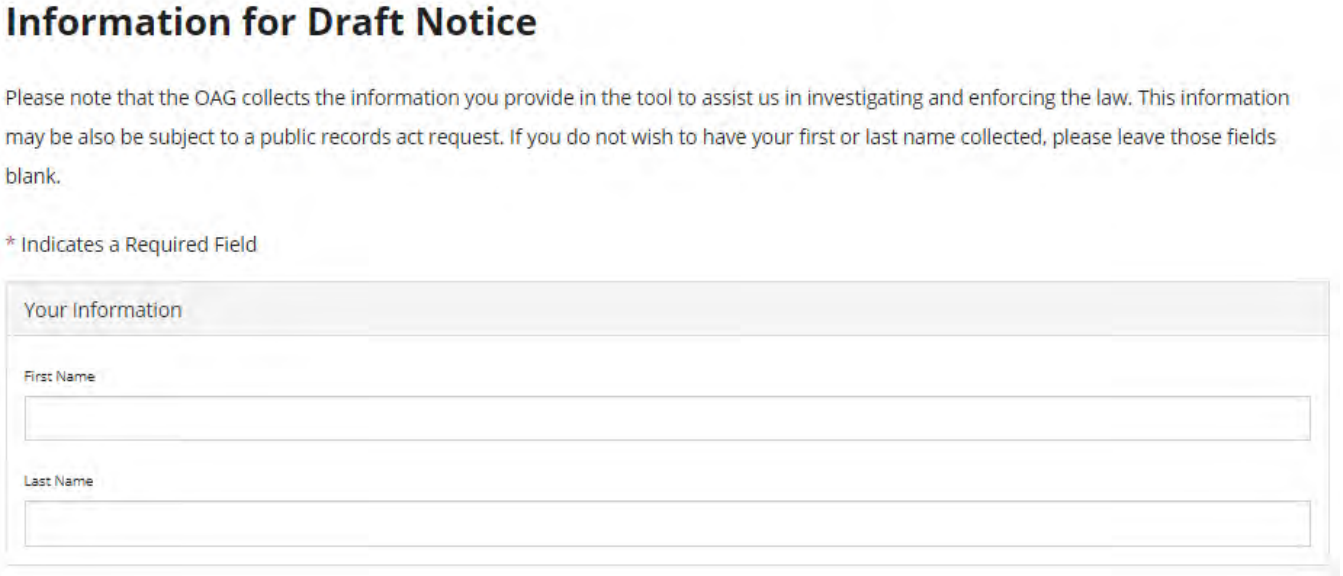


© S&K Brussels LPC 2021

カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool



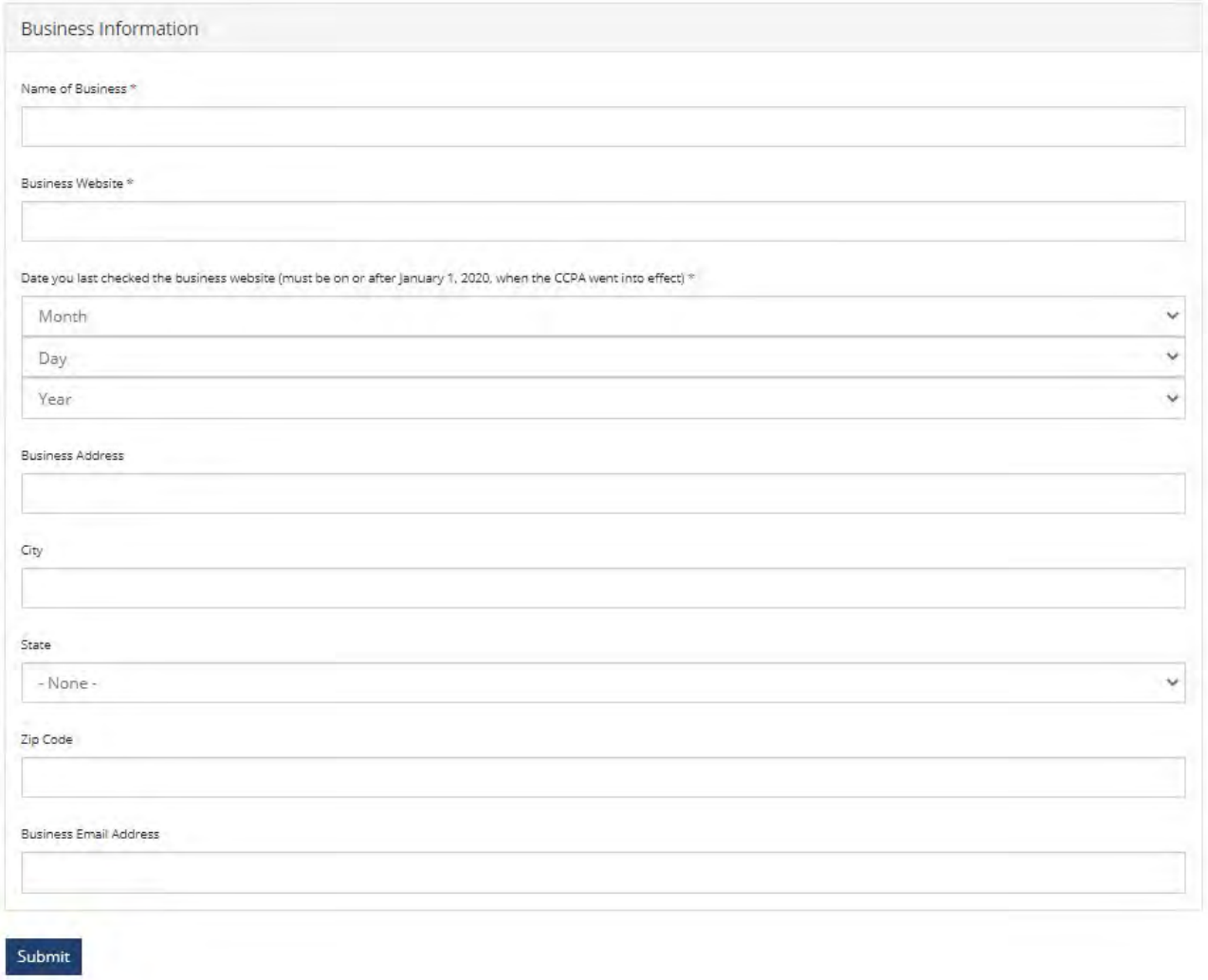
■Draft Noticeを作成する情報を入力するフォームの上半分（次スライドに続く）



© S&K Brussels LPC 2021

カリフォルニア州司法長官オフィスのConsumer Privacy Interactive Tool

■Draft Noticeを作成する情報を入力するフォームの下半分（前スライドからの続き）



© S&K Brussels LPC 2021

参考資料④：CCPA訴訟の動向

© S&K Brussels LPC 2021

CCPA訴訟の動向

・CCPA訴訟は、CCPA上の私的訴訟権によって認められるものである1の類型のみならず、CCPA上の私的訴訟権の範囲に含まれない消費者のプライバシー権の侵害に基づく2の類型のものもみられる。また、3のようにCCPAの違反が他の類型の訴訟において理由として主張されるものもみられる。

- CCPAを引用した訴訟事例は、2021年7月時点で150以上確認されている。
  - 訴えの種類
    1. データ侵害：CCPAの私的訴訟権の範囲が限られていることを前提として、これまでのCCPA訴訟事例の多くはデータ侵害につながる合理的なセキュリティ保護手段の実装に失敗したという主張となっている。2020年にはデータセキュリティ違反を含むCCPAの私的訴訟権の下で約50件の訴訟が提起された。
    2. 消費者のプライバシー権：CCPAは、法令に基づくプライバシー権の侵害に対する私的訴訟権（知る権利、削除請求権、オプトアウト権など）を認めていない。しかし、消費者がCCPA上のプライバシー権が侵害され、被告がCCPAに基づく要件を満たさなかったとして提訴すること自体は妨げられるものではない。
    3. CCPAへの言及：その他の場合、原告は直接CCPA上の請求または違反を主張するのではなく、代わりにたとえばカリフォルニア州の不公正競争法（UCL）の違反など、他の訴訟原因の理由としてCCPAに言及することがある。
- 多くのCCPA訴訟の内訳：
  - 金融24件、ソフトウェアを中心とするクラウド23件、フィンテック12件、ヘルスケア12件、サーチエンジン9件、ソーシャルメディア6件、保険6件
  - 2-5件：自動車、バイオテック、衣料、サイバーセキュリティ、電子商取引、健康フィットネス、ホスピタリティ、レストラン、小売、廃棄物管理
  - 1件：事業者サービス、コンピュータ、エンタメ、眼鏡類、食品、家庭警備、マーケティング、医療機器、医用画像、携帯装置アクセサリ、音楽、オンラインデイティングサイト、オンライン音楽レッスン、写真共有、旅行、等

・CCPA訴訟は、金融、クラウド、ヘルスケアなどの分野において多くみられるが、他の産業分野においても広くみられる。

S&K Brussels

© S&K Brussels LPC 2021

CCPA訴訟の動向
1798.150(a) – CCPA「私的訴訟権」

制裁
- 違反一件毎、消費者一人毎に100-750米ドル（又は実損害の方が大きい場合には、実損害額）
- 差止命令、等

要件:

①「事業者」による不合理なセキュリティ慣行 → ②データ侵害を引き起こす → ③狭義の個人情報に影響 ＋ ④事業者が30日以内に違反状態の治癒ができない

かつ

法定損害賠償に関してのみ

注意点1:「CCPA上の事業者の義務に違反したからといって、CCPA以外の他の法律を根拠として訴訟を提起することは、CCPA上、認められない。」

注意点2:カリフォルニア州の居住者のみが利用可能（「消費者」）
- カリフォルニア州の居住者の個人情報が影響を受け、かつ
- カリフォルニア州の居住者のみがCCPA上で訴訟を提起する権利を持つ

注意点3:「事業者」（「サービス提供者」ではなく）に対してのみ
- B2B及びB2C企業いずれも含む。消費者（原告）と事業者（被告）間の契約関係は不要

注意点4: 2020年1月1日 (CCPAの適用開始日)以降に生じた行為に関して
- 2020年1月1日以前に生じた、及び同日に進行中でない、データ侵害は提訴できない

注意点5:私的訴訟権の対象となる「個人情報」は、通常の「個人情報」よりも限定された狭義の「個人情報」のみ

■ 次スライド以降で、最近のCCPA訴訟の実例のうち、注目に値する幾つかの事例（事例1: Anurag Gupta et al v. Aeries Software, Inc.、事例2: Benjamin Karter v. Epiq Systems, Inc.、事例3: Harbour v. California Health）について解説する。

・CCPA上の私的訴訟権の要件は、①から③。法定損害賠償が認められるための要件として④がある。

・注意点1から5は、CCPA上の私的訴訟権に基づく請求を否定するための被告側の主張のポイントになるものである

・注意点5の私的訴訟権の対象は、CPRAにより拡張され「自身の暗号化されておらず、かつ修正されていない個人情報、もしくはパスワードまたはセキュリティ上の質問との組み合わせの電子メールアドレスおよびそのアカウントへのアクセスが許可される返答が、無権限アクセス、流出、窃取または開示の対象となった消費者」が提起できることとなった。

S&K Brussels

© S&K Brussels LPC 2021

事例1: Anurag Gupta et al v. Aeries Software, Inc.
2021年6月、$175万 ＋ 12カ月のクレジット／ID保護で和解

・この「データ侵害」は2019年11月から2020年1月まで、あるいは同年3月まで継続しているという主張（注意点4）
・裁判所は、本事件がtrialの段階に進むことを確保するため、原告側に有利な極端な解釈を行うことに前向きである。

概要：・Aeries SIAとは、Aeries Student Information System（Aeries学生情報システム）の略。

- カリフォルニア州の公立学区システムに**データホスティング及び管理サービス**を提供（Aeries SISを使用）する**Aeries Software, Inc.**に対する集団訴訟。
- **2019年11月に発生したデータ侵害**により、Aeries社のサーバーにホストされている166のデータベースが影響を受けた。
- 侵害を受けた個人情報には、保護者や学生の**名前**、**社会保障番号**、**固有の政府ID番号**、電子メールなどが含まれる。

・具体的には、本事件ではAeries Software社が、教育機関にかわって各教育機関自体の個別の目的のために、個人情報の収集を行っており、CCPA上の「サービス提供者」であって「事業者」ではないことは否定しがたいように見えたのにもかかわらず、裁判所は本裁判の初期の段階では同意しなかった。

S&K Brussels

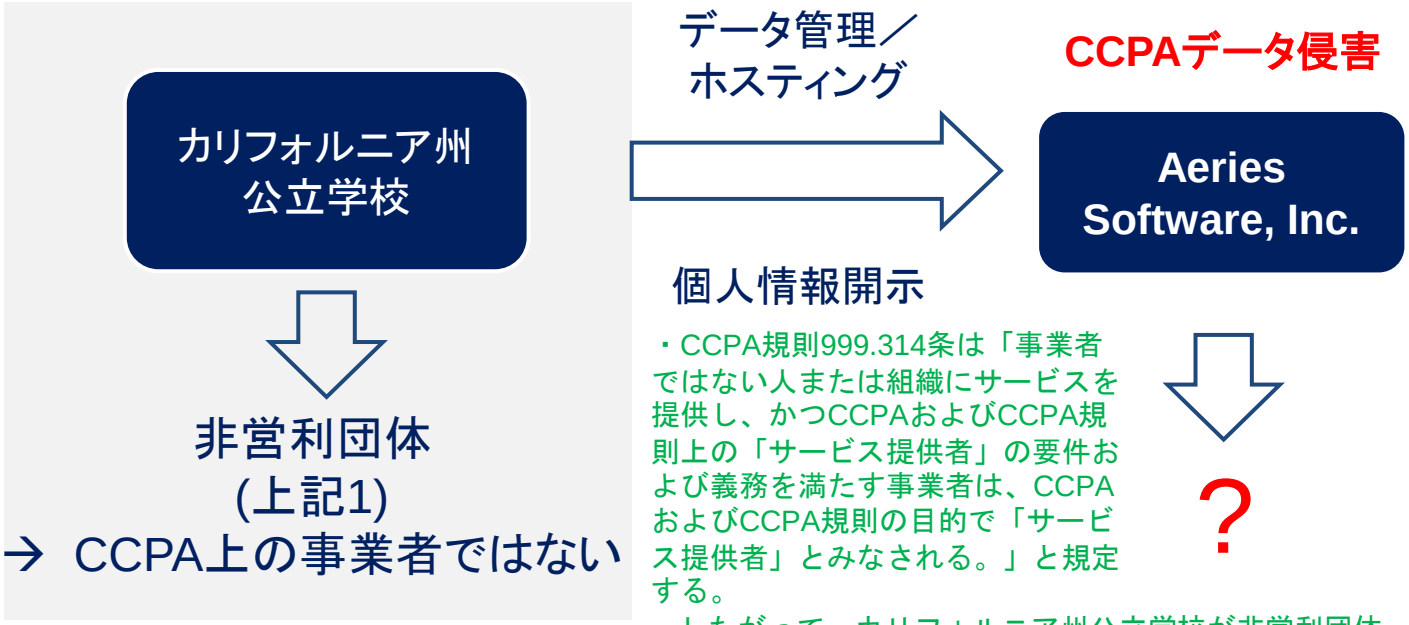
© S&K Brussels LPC 2021

事例1: Anurag Gupta et al v. Aeries Software, Inc.
2021年6月、$175万 ＋ 12カ月のクレジット／ID保護で和解

CCPA私的訴訟権は、「事業者」に対してしか行使できない

CCPAの事業者とは *§1798.140(c)(1)*

1. カリフォルニア州で事業を展開している**「営利」企業**
2. 消費者の個人情報を収集し、処理している
3. 当該処理の**目的と手段を決定している**
4. 特定の追加しきい値を満たしている



© S&K Brussels LPC 2021

事例1: Anurag Gupta et al v. Aeries Software, Inc.
2021年6月、$175万 ＋ 12カ月のクレジット／ID保護で和解

Aeries Software：CCPAの事業者か、CCPAのサービス提供者か？

CCPAのサービス提供者とは *§1798.140(v)*

1. **事業者に代わって情報を処理する**主体
2. **事業目的**で消費者の個人情報を事業者から開示される
3. 上記は書面の契約によるものである
4. これにより、**契約で指定されたサービスを実施するという特定の目的以外で、**個人情報を処理することを禁止されている

・自社が「サービス提供者」に該当することを確保するため、CCPA上の「サービス提供者」の要件を踏まえたAddendumの締結が重要であるとともに、合理的なセキュリティ対策の確保も肝要。

Aeriesは「消費者の個人情報を処理及び保管するシステムを設計している」
＝ 処理の目的と方法を決定している？

Aeriesは「学区のクライアントに代わって、学生、親、保護者の情報を学区の特定の目的のために［契約に基づき］処理している」
＝ 契約に基づく特定の目的のために、事業者に代わって処理している？

- 和解前に、Aeries Softwareは、**自身がCCPAにおけるサービス提供者であり、事業者ではないという考え方に基づいて棄却の申立てを2件**行ったが、**却下された**。

・注意点3（「事業者」（「サービス提供者」ではなく）に対してのみ）との関係では、CCPA上の「サービス提供者」であるとの主張が認められそうであるAeries Software社であっても、CCPA上の訴訟を提起され、また当該主張が裁判所に認められないことによって、長期の訴訟対応を強いられる事態が継続し、最終的に、Aeries Software社が一定の金銭の支払いと措置を取ることを内容とする和解にまで持ち込まれた。

S&K Brussels

© S&K Brussels LPC 2021

事例2: Benjamin Karter v. Epiq Systems, Inc.
2020年7月22日に提起。2022年11月に陪審裁判が予定

概要:

- Epiq Systems, Inc.とその完全子会社であるEpic Class Action & Claims Solutions, Inc.に対する集団訴訟
  - ***Epiq Systemsは法律事務サービスを提供しており、****クライアントによる集団訴訟、裁判報告、eディスカバリー、コンプライアンス、再編、破産等における事務手続きを支援している。*
  - ***Epiq Class Actionは、集団訴訟／集団不法行為の和解と判決を管理している***
- 2020年2月に発生した**データ侵害**により、消費者の**名前**や**社会保障番号**など、Epiqのネットワーク上の個人情報が影響を受けた。

・注意点3（「事業者」（「サービス提供者」ではなく）に対してのみ）が争点であり、Epiq Systems社およびEpiq Class Action社が「サービス提供者」に該当するかが争われている。

© S&K Brussels LPC 2021

事例2: Benjamin Karter v. Epiq Systems, Inc.
2020年7月22日に提起。2022年11月に陪審裁判が予定

EpiqはCCPA上の事業者か、CCPA上のサービス提供者か？

裁判所の判断（被告の棄却申し立てを却下）:

1. Epiqは、他の主体との契約に基づいてサービスを提供するため、消費者の個人情報を収集している。**これは、事業者の活動であり、事業者から個人情報を受領するサービス提供者の活動ではない。**

2. Epiqは、クライアントと共に、消費者の個人情報を使用して通知を行い、請求やオプトアウトを管理する方法を決定している。したがって原告は、**Epiqが「単独又は他の者と共同して、**消費者の個人情報の**処理の目的と方法を決定している」**と主張している。

・上記の裁判所の判断は、「サービス提供者」への該当性を否定し、広範に「事業者」への該当性を認めるもの。この判断が一般的となった場合、今後も多くのサービス提供者に該当すると考えられる企業がデータ侵害の場合に、CCPA訴訟への対応を強いられることとなり、和解にもちこまれるケースは増えるものと考えられる。

・自社が「サービス提供者」であることを前提として、CCPA対応を限定的なものに止める方針を取ることには慎重な検討が必要といえる。

・また、「サービス提供者」への該当性を基礎づけるためのCCPA上の契約は、益々重要性が高いものと認識されるようになると考えられる。特に、「サービス提供者」への該当性を基礎づけるための契約の要件はCPRAによって修正されているため、注意が必要。

S&K Brussels

© S&K Brussels LPC 2021

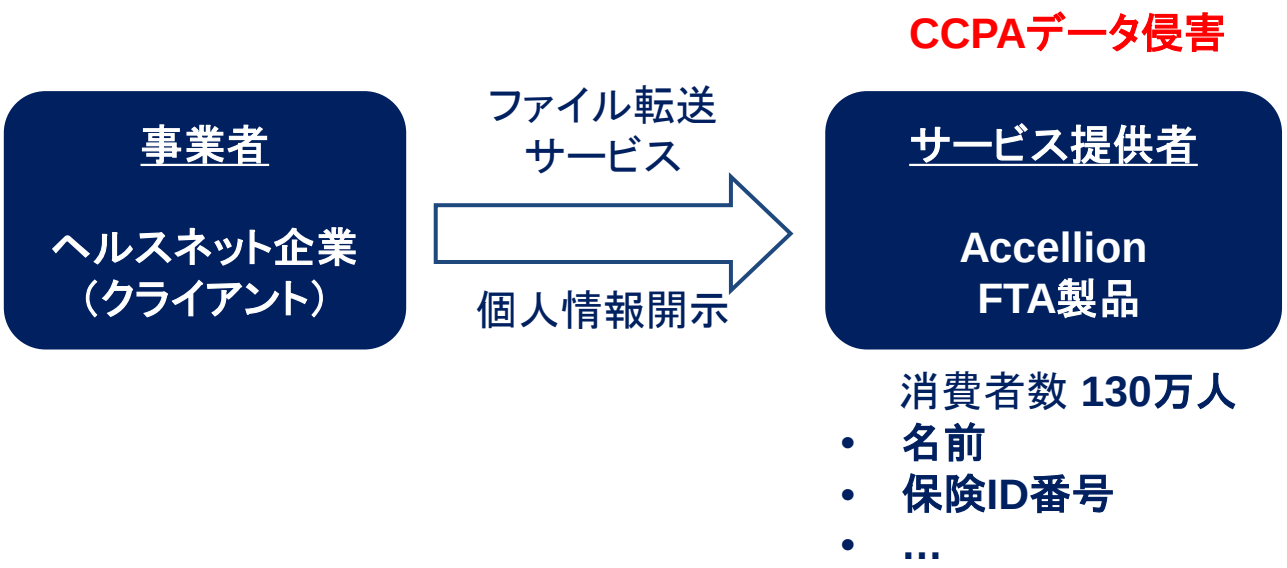
事例3: Harbour v. California Health
2021年5月に提訴

概要:

・Accellion社は、自社がセキュアかつ信頼されるサービス提供者であったという主張を繰り広げている。

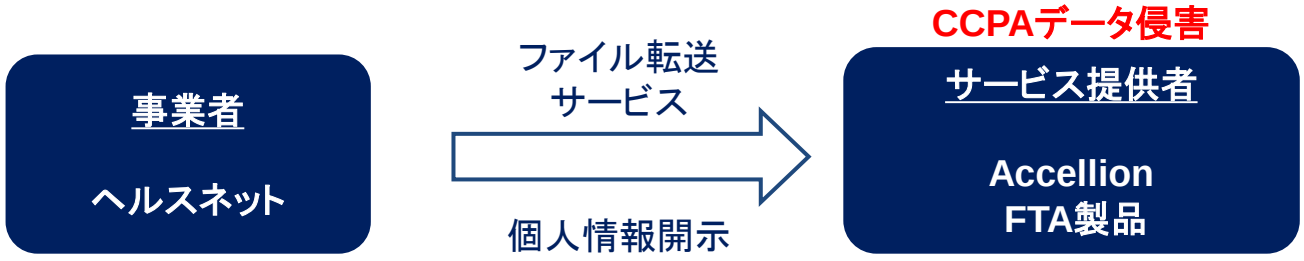
- **2**の被告に対する集団訴訟:
  1. 「ヘルスネット」企業(事業者):全国の医療ケアコングロマリット(HMO及びPPO保険プランの提供とケアの調整)
  2. Accellion(サービス提供者):ファイル転送アプライアンス(FTA: File Transfer Appliance)を含むサードパーティのファイル転送サービスを提供するソフトウェア企業
- **2021年1月に発生したデータ侵害**で、AccellionのFTA製品が影響を受けた。

- 侵害を受けたヘルスネットの顧客130万人の個人情報には、**氏名や保険ID番号**、(住所、生年月日、センシティブな医療データ)が含まれる。



© S&K Brussels LPC 2021

事例3: Harbour v. California Health
2021年5月に提訴



- **名前**
- **保険ID番号**

サービス提供者は、CCPAの「私的請求権」の対象とはならない（Section 1798.150）
→ *AccellionがCCPAでの「サービス提供者」の場合、Accellionに対するCCPAの主張は成り立たない。*
CCPAの「サービス提供者」であるためには、Accellionは以下を満たす必要がある。

- （1）特定の「事業目的」のサービスを提供する
- （2）ヘルスネットの代わりとして、及びその指示で動く
- （3）ヘルスネットと「サービス提供者」契約を締結した

CCPAに基づく事業者は、CCPAの「サービス提供者」による過失行為に対して責任を問われることはない。ただし、事業者にもデータ侵害の責任がある場合を除く。
*「ヘルスネットの被告は、FTAソフトウェアが安全ではなく、これ以上データ転送に関して使用すべきではないことを知っていた。実際、「複数のサイバーセキュリティ専門家は...Accellion FTAは20年前のアプリケーションで、企業が大規模なファイルを安全に転送できるように設計されているが、間もなく寿命となると強調しており」、**「Accellionは昨年、kiteworksという新しい製品に切り替えるよう顧客に求めていた。」 … 被告全員が、kiteworksへの切り替えを怠り、故意にFTAを使用し続け、原告集団の個人識別情報と健康情報を窃取、ID窃取、及び不正行為のリスクに晒した。」*

・CCPA1798.145条(j)は、本巻に準拠して、サービス提供者に対して個人情報を開示する事業者は、当該個人情報を受け取る当該サービス提供者が、本巻に定める制限に違反して当該情報を使用している場合、当該個人情報を開示するときに当該サービス提供者が違反を行う意図であったことについて実際に知らずまたはそう信じるべき理由を持たないとき、本巻のもとに責任を問われないと規定する。

S&K Brussels

© S&K Brussels LPC 2021

事例3: Harbour v. California Health 2021年5月に提訴

Accellion FTAの侵害の影響を受けたその他の法的主体は以下のとおりである。したがって、これらの法的主体は、*「情報の性質に適した合理的なセキュリティ手順と慣行を実施し維持する」*というCCPA上の義務に違反したとされるヘルスネット企業と同様の違反をしていると主張されている。

- Allens
- American Bureau of Shipping (“ABS”)
- Arizona Complete Health
- The Australia Securities and Investments Commission
- Bombardier
- CSX
- Danaher
- Flagstar Bank
- Fugro
- Goodwin Proctor
- Harvard Business School
- Jones Day
- The Kroger Co.
- The Office of the Washington State Auditor
- QIMR Berghofer Medical Research Institute
- Qualys
- The Reserve Bank of New Zealand
- Shell
- Singtel
- Southern Illinois University School of Medicine
- Stanford University
- Steris
- Transport for New South Wales
- Trillium Community Health Plan
- University of California
- University of Colorado
- University of Maryland, Baltimore
- University of Miami (Florida)
- Yeshiva University

・適切なCCPA上のサービス提供者との契約を締結していない場合、本スライド記載の事業者も、Accellionによるデータ侵害に関してCCPA上の責任を問われるおそれがある。

S&K Brussels

© S&K Brussels LPC 2021

今後のCCPA/CPRA訴訟に対する未然防止策
1. CPRAによる私的訴訟権の拡大を念頭に置く

- CPRAによる私的訴訟権への修正
  - CCPA上の私的訴訟権を拡大し、パスワード又はセキュリティ上の質問との組み合わせの電子メール・アドレス及びそのアカウントへのアクセスが許可される回答が、無権限アクセス、流出、窃取又は開示の対象となるデータ侵害をカバーする
  - データ侵害後の合理的セキュリティ手続・慣行の実施及び維持が当該データ侵害に関して「治癒」を構成しないことを明確化

→今までよりも多くのデータセキュリティ違反に基づくCCPA/CPRA訴訟が提起される可能性が高い。

・注意点5の私的訴訟権の対象は、CPRAにより拡張され「自身の暗号化されておらず、かつ修正されていない個人情報、もしくはパスワードまたはセキュリティ上の質問との組み合わせの電子メールアドレスおよびそのアカウントへのアクセスが許可される返答が、無権限アクセス、流出、窃取または開示の対象となった消費者」が提起できることとなった。

・私的訴訟権の要件④との関係では、法定損害の賠償請求が行われた場合にも、CCPAの下では、データ侵害後に合理的セキュリティ手続・慣行の実施および維持の対応を取ることによっても、治癒期間の恩恵を受けることができたが、CPRA適用開始（2023年1月1日）以降はできなくなる。平時のセキュリティ対応がより重要性を増すことになる。

S&K Brussels

© S&K Brussels LPC 2021

今後のCCPA/CPRA訴訟に対する未然防止策
2. CCPA/CPRA上の法的責任を回避するための備え

- CCPA上のデータ侵害の発生を防ぐことが最良の防御。データ侵害が発生した場合にも「不合理な」セキュリティ手続き及び慣行が原因ではないことを確保することが重要
- 2016年2月に公表された”California Data Breach Report 2012-2015”（https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ）30頁においてカリフォルニア州の当時の司法長官（現・米副大統領Kamala D. Harris氏）は20の「CISコントロール」を「合理的なセキュリティ」の最低限の基準と述べている。

Kamala D. Harris
元カリフォルニア州司法長官（現・米副大統領）
（注：写真は上記California Data Breach Report 2012-2015から引用）

Recommendation 1:
The 20 controls in the Center for Internet Security's Critical Security Controls define a 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.

Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.[22] The Controls were originally developed by federal agencies in 2008 and since then have been the product of a public-private partnership that includes cyber security experts from government and the private sector in the U.S., as well as around the world.

© S&K Brussels LPC 2021

今後のCCPA訴訟に対する未然防止策

3. CCPA/CPRA上のセキュリティ対策を実行することを検討する。

- 事例1（Anurag Gupta et al v. Aeries Software, Inc.）の原告による差止命令申立てはCISコントロール（https://learn.cisecurity.org/cis-controls-download）でほぼカバーされる。

原告が求める差止命令	Anurag Gupta et al Aeries Software, Inc.	CISコントロールとの重複(もしあれば)
暗号化	protect, including through adequate encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local law	CIS Control 13: Data Protection CIS Control 14: Controlled Access Based on the Need to Know
包括的な情報セキュリティプログラム	implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of [PII]	CIS Control 13: Data Protection
第三者としてのセキュリティ監査人及び社内の自動化されたセキュリティモニタリング	engage independent third-party security auditors and internal personnel to run automated security monitoring	CIS Control 3: Continuous Vulnerability Management CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
新しい/修正された手続に関する監査、テスト、及び従業員の訓練	audit, test, and train its [security] personnel regarding any new or modified procedures	CIS Control 17: Implement a Security Awareness and Training Program
ファイアウォール及びアクセス管理を含むデータセグメンテーション	segment data by, among other things, creating firewalls and access controls so that if one area of [Defendant's] network is compromised, hackers cannot gain access to other portions of [Defendant's] Systems	CIS Control 8: Malware Defenses CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches CIS Control 14: Controlled Access Based on the Need to Know
データベーススキャニング/チェック	conduct regular [database/computer system] scanning and security checks	CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services
全従業員向けの年次トレーニング＋特別トレーニングを含む、ITセキュリティトレーニングプログラム	establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII	CIS Control 17: Implement a Security Awareness and Training Program
侵害の特定、封じ込め対応に関する反復の社内トレーニング	routinely and continually conduct internal training and education [at least annually], to inform security personnel how to identify and contain a breach when it occurs and what to do in response to a breach	CIS Control 17: Implement a Security Awareness and Training Program CIS Control 19: Incident Response and Management
模擬攻撃を含む脅威マネジメントプログラム	implement, maintain, regularly review, and revise as necessary, a threat management program designed to appropriately monitor Aeries' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated	CIS Control 19: Incident Response and Management CIS Control 20: Penetration Tests and Red Team Exercises
サーバートラフィックを追跡するためのログ作成及びモニタリング	implement logging and monitoring programs sufficient to track traffic to and from its servers	CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs
不要な情報の除去/破壊	delete, destroy, and purge the PII . . . unless Aeries can provide the Court a reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs .	---
該当なし	**N/A**	CIS Control 1: Inventory and Control of Hardware Assets CIS Control 2: Inventory and Control of Software Assets **CIS Control 7**: Email and Web Browser Protections CIS Control 10: Data Recovery Capabilities CIS Control 15: Wireless Access Control **CIS Control 18:** Application Software Security

参考資料⑤：CPRAデータマッピング質問票－人材採用の例での回答）

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
A. 部署および記録

Q1. 部門、事業部または下位グループ

各行で特定される事業記録または処理活動を主に担当するグループを特定して下さい。

（回答）

- [グループ]
- 例：人事部門

Q2. 事業記録または処理活動

CPRAの対象となる個人情報を含む事業記録または処理活動を特定して下さい。

（回答）

- [事業記録または処理活動]例: 電子メールマーケティング、人事採用、顧客記録、人事記録、マーケティングリスト
- 例：人事採用

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
A. 部署および記録

Q3. 記録または処理活動の状況
記述された事業記録または処理活動がまだ元の形式で使用されているか(「アクティブ」)、まったく使用されなくなったか([日付]時点で使用されていない)、または元の形式から特定の変更を加えて使用されている(すなわち、[日付]から[変更内容]に変更された)を特定して下さい。
(回答)

- [活動ステータス]
  - 例:アクティブ

Q4. 個人の数の記録
個人情報が取得された消費者の数の推定を記載して下さい(過去12か月の合計数の推定を括弧内に記載して下さい)。個人情報を取得したカリフォルニア州の住民数について、第二の推定を記載して下さい(過去12ヶ月間の合計数を括弧内に記載してください)。
(回答)

- [合計 # (過去12か月)]
- [カリフォルニア州 # (過去12か月)]
  - 例:全米合計:180(90)
    - [注:全米でデータ保護コンプライアンス対応を行うことを想定]
  - カリフォルニア州: 35(18)

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
B. 消費者のカテゴリ：誰

Q5. 消費者のカテゴリ

誰に関する個人情報であるかを特定して下さい。

（回答）

- [消費者のカテゴリ]カテゴリの例: 顧客、顧客候補、現在の従業員、ウェブサイト訪問者
  - 例：採用候補者

Q6. 子供の個人情報

子供の情報が取得されるかどうかを特定して下さい（"はい"または"いいえ"）。
→ もし取得される場合、子供の年齢範囲を特定して下さい。

（回答）

- "[はい/いいえ][年齢範囲]"
  - 例：いいえ

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
C. 個人情報の収集：何を、なぜ、どこで

Q7. 取得された個人情報のカテゴリ

事業記録または処理活動に関して過去12ヶ月間に取得された個人情報のカテゴリ以外の数字を消去して下さい。

*一部の個人情報は複数のカテゴリに該当する場合があります。該当するカテゴリは全て残して下さい。

（回答）

- 1. 識別子
- 2. その他の識別子
- 3. 保護された分類上の特性
- 4. 商業情報
- 5. 生体情報
- 6. インターネット・ネットワーク情報
- 7. 位置データ
- 8. 知覚情報
- 9. 職業/雇用に関する情報
- 10. 教育情報
- 11. プロフィールに関するデータおよび推測
- 12 従業員情報
- 13. センシティブな個人情報（CPRA）
- 14. カリフォルニア消費者記録カテゴリ
- 15. 子供の情報

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
C. 個人情報の収集：何を、なぜ、どこで

Q7. 取得された個人情報のカテゴリ

事業記録または処理活動に関して過去12ヶ月間に取得された個人情報のカテゴリ以外の数字を消去して下さい。

*一部の個人情報は複数のカテゴリに該当する場合があります。該当するカテゴリは全て残して下さい。

（回答）

例：

- 1. 識別子
- 2. その他の識別子
- 9. 職業/雇用に関する情報
- 10. 教育情報
- 11. プロフィールに関するデータおよび推測

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
C. 個人情報の収集：何を、なぜ、どこで

Q8. 取得された個人情報の具体的内容

チェックした個人情報のカテゴリごとに、→ 過去12ヶ月間に取得された個人情報の具体的内容を特定して下さい。

（回答）

例：

- 1→氏名、電話番号、メールアドレス 、住所、IPアドレス、申請者ポータルクッキー
- 2.→氏名、住所、電話、職歴
- 9.→プロフェッショナル/雇用:以前の仕事と期間、雇用主のリファレンス
- 10.→教育:学校、成績、学業区分
- 11.→推論:知性

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
C. 個人情報の収集：何を、なぜ、どこで

Q9. 個人情報の取得・使用の目的
チェックした個人情報の各カテゴリについて、そのカテゴリ内の個人情報を収集/処理する目的を特定・説明し、目的ごとに→「事業目的」または「商業目的」かの特定を括弧内にお願いします。
注:「プロファイリング」（自動的処理の形態）を実施する場合は、個人情報の「プロファイル（profiled）」のカテゴリを特定してください。*個人情報の一部のカテゴリは、取得/処理に関する複数の異なる目的を伴う場合があります。関係するすべての目的と、その事業および/または商業の性質を特定してください。
（回答）例：
1、2→
- 特定の個人を内部で追跡し、重複するアプリケーションの提出を防止するため→（事業）
- 役職に関して特定の個人とコミュニケーションを取る→（事業）
- 名前ではなく識別子を使用して個人情報を保護する→（事業）

9、10、11 →
- 内部で特定の個人を追跡する （個人の記録）→（事業）
- 社内の役職に適した候補者を特定し、配置する→（事業）

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
C. 個人情報の収集：何を、なぜ、どこで

Q10. 個人情報の情報源
消費者（該当する場合）を含む、個人情報が取得された情報源のカテゴリ（消費者から直接、自動的に、または第三者）を特定して下さい
→各カテゴリの情報源に関して、括弧内に特定の情報源および各情報源から収集した個人情報のカテゴリ（数字で）を特定して下さい。
（回答）
例：

- 消費者から直接取得→（オンライン求人アプリケーション）→1、2、9、10、11
- 自動的なデータ取得→（会社ウェブサイト上のオンラインアプリケーションポータルは、応募者のIPアドレスを取得し、デバイス上にクッキーを配置する）→1、2
- 第三者から取得→（LinkedInが提供する候補者）→1、2、9、10、11

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
D. 受領団体

Q11．受領団体
過去12ヶ月間に個人情報を開示した、全ての受領団体/会社を列挙してください。→当該受領者が(1)関連している*、(2)外部/非関連、または(3)不明確、のいずれかを括弧内で特定してください。
*(1)各関連団体について→関連性または関係性、および共通のブランドを共有しているか否かを、括弧内に記載してください。
注:この目的で、関連団体は、子会社、親団体および兄弟団体、ならびに共通の所有またはブランドを共有する団体(商標または名称の共有等)を含みます。
(回答)例:

- Google Drive→(外部)
- Microsoft Exchange→(外部)
- HostGator→(外部)
- NY HQ → (関連) → 親会社(100%支配)であるが、異なる名称/ブランド
- テキサスに拠点を置く関連会社 → (関連) → 異なる名称/ブランドを有する兄弟会社

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
D. 受領団体

Q12.　外部受領者に移転された個人情報のカテゴリ
Q11において列挙された各受領者について（共通のブランドを共有する親団体または子団体を除く。）—受領者を列挙してください。→過去12ヶ月間に当該受領者に開示された個人情報のカテゴリを、括弧内で番号により特定してください。→開示された各カテゴリについて、当該開示の目的を記載してください。
（回答）例：

- Google Drive→（1、2、9、1、11）→ クラウド・インフラストラクチャーおよびストレージ・データベースの目的
- Microsoft Exchange→（2、9、10、11）→ 従業員のインボックスならびに内部および外部のEメール通信
- HostGator→（1、2、9、10、11）→ HRのNetworked H Driveのための外部サービス
- NY HQ→（2、9、10、11）→ HQレベルでの採用および面接のための候補者情報の提供
- 日本HQ→（2、9、10、11）→日本HQレベルでの候補者採用の承認
- テキサスに拠点を置く関連会社 →（2、9、10、11）→ 採用および面接のための候補者情報の提供

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
E. 過去12ヶ月間の個人情報の売却、共有および事業目的開示

Q13. 売却
Q12において列挙された、金銭またはその他の価値ある対価のための「売却」と記載された全ての個人情報の開示について—受領団体を特定してください。
→括弧内で、「売却」された個人情報のカテゴリを番号で列挙してください。→当該各カテゴリについて、売却の商業目的を説明してください。
（回答）
例：

- テキサスに拠点を置く関連会社 →（2、9、10、11）→ 候補者情報の提供、および採用が成功した場合、報酬の受領

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
E. 過去12ヶ月間の個人情報の売却、共有および事業目的開示

Q14. 共有
Q12において列挙された、クロスコンテキスト行動広告のための「共有」と記載された全ての個人情報の開示について—受領団体を特定してください。
→括弧内で、「共有」された個人情報のカテゴリを番号で列挙してください。→当該各カテゴリについて、共有の商業目的を説明してください。
（回答）
例：
- 適用なし

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
E. 過去12ヶ月間の個人情報の売却、共有および事業目的開示

Q15.　事業目的の開示
Q12において列挙された、「事業目的」の開示と記載された全ての個人情報の開示について―受領団体を特定してください。
→括弧内で、事業目的をアルファベットで列挙してください。
→当該各事業目的について、開示された個人情報のカテゴリを番号で列挙してください。
（回答）
例：

- Google Drive→（E）→1、2、9、10、11
- Microsoft Exchange→（E、I-通信）→2、9、10、11
- HostGator→（E）→1、2、9、10、11
- NY HQ → （E） → 2、9、10、11

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
E. 過去12ヶ月間の個人情報の売却、共有および事業目的開示

Q16.　第三者受領者による商業使用
Q15において特定された全ての開示について→ 開示された個人情報を第三者に対して再売却し、共有し、もしくはさらなる開示を行う、または契約上再売却（もしくは共有もしくはさらなる開示）を行う能力を有する受領者を列挙してください。
注：開示された個人情報のさらなる売却/共有/使用について契約に定めがない場合、ここに記載してください。
（回答）
例：

- HostGator（契約において禁止されていない）

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
F. 経済的インセンティブ・プログラム

Q17. 経済的インセンティブ
事業記録のためまたは事業者の処理活動に関連して、個人情報の取得、売却/共有または削除の対価として提供される金銭的インセンティブ（または罰則）を特定し、記載して下さい。
（回答）
例：
- なし

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
G. 保存、保持およびセキュリティ実務

Q18. 保存場所
貴社が個人情報を保存する場所（関連する場合、第三者の名前を含む）を特定して下さい→ （保存場所が物理的または電子的であるかを含む）
（回答）
例：

- 外部クラウド → （Googleドライブ）
- 従業員の受信トレイ → （マイクロソフトエクスチェンジ）
- HR のネットワーク化されたHドライブ → （X 社が提供する外部サーバー）
- 物理的な紙ファイル → （オンサイト）

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
G. 保存、保持およびセキュリティ実務

Q19. 保存された情報に関する組織化および再識別の能力
特定の個人、場所、および消費者のカテゴリに属するすべての保存された内容および/または個人情報のカテゴリの識別を可能にする、組織および検索機能について記載して下さい。
（回答）
例：

- 取得された任意のタイプの個人情報で検索/分類できる（IPアドレスとクッキーを除く）
- （カリフォルニア州を含む）郵送先住所で検索することができる。

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
G. 保存、保持およびセキュリティ実務

Q20. 保存期間
消費者の個人情報が保存される時間の長さ（個人情報のカテゴリによって時間の長さが異なる場合は、そのようなバリエーションとそれらが適用される個人情報カテゴリを括弧内に記載して下さい）を記載して下さい。
（回答）
例：
- 10年

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
G. 保存、保持およびセキュリティ実務

Q21. セキュリティ・コントロール
不正な開示/データ漏洩を防止するために、内部および外部のセキュリティに関する手続/実務のカテゴリ（技術的、管理的、および/または物理的）を特定し、その後に→各カテゴリの特定の種類のセキュリティ管理を括弧内に記載して下さい。
（回答）
例：
- 技術面　→（暗号、ファイアウォール、ウイルス対策プログラム）

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
H. 消費者通知/連絡

Q22. 消費者への通知・連絡
個人情報の取得、処理、売却/共有、および当該情報に関する権利、ならびに消費者が当該個人情報に関する問い合わせおよび要求を行う方法について、消費者に通知するための仕組を特定し、記載して下さい。
（回答）
例：
- クッキーの取得に関する通知
- 人事の連絡先メールアドレスおよび電話番号はオンラインで公開されている

S&K Brussels

© S&K Brussels LPC 2021

CPRAデータマッピング質問票
人材採用の例
I. 法的分析 - 受領者のカテゴリ

Q23. サービス提供者
サービス提供者の定義に該当する、貴社が個人情報を共有するQ12の受領者を特定し→共有される個人情報のカテゴリを括弧内に列挙し（数字で）→該当する契約が必要な条件が含まれていることを確認したか否かについて特定して下さい。
（回答）
例：

- Google ドライブ → （1、2、9、10、11）→契約が必要な条件を満たしていることを確認した。
- マイクロソフトエクスチェンジ → （2、9、10、11）→契約が必要な条件を満たしていることを確認した。

S&K Brussels

© S&K Brussels LPC 2021

S&K Brussels法律事務所
事務所代表・マネージングパートナー　弁護士　杉本　武重

杉本 武重
Takeshige Sugimoto
takeshige.sugimoto@sandkbrussels.com
www.sandkbrussels.com
直通 +81-3-6429-8040; 携帯 +81-80-8051-4848; +32 494 67 33 51; +1 347 259 2661
S&K Brussels法律事務所
Tokyo Office (HQ): 〒143-0023 東京都大田区山王2-5-6山王ブリッジB1F
New York Office: 1330 Avenue of the Americas, Suite 23, New York, NY 10019 US
Brussels Office: Bastion Tower Level 20, box 14, Place du Champ de Mars 5, 1050 Brussels, Belgium

2006年	弁護士登録（59期）
同年	第一東京弁護士会所属
2013年	ニューヨーク州弁護士登録
同年	ニューヨーク州弁護士会所属
同年	ブリュッセル弁護士会登録（B-List）
同年	同会所属

経歴

2000年　駒場東邦高等学校卒業
2004年　慶應義塾大学法学部法律学科卒業
2006年-2013年　長島・大野・常松法律事務所アソシエイト
2012年　シカゴ大学ロースクール法学修士課程卒業(LL.M)
2013年　オックスフォード大学法学部法学修士課程卒業(Magister Juris)
2013年-2014年　WilmerHale法律事務所ブリュッセルオフィスアソシエイト、2015年-2017年同オフィスシニアアソシエイト
2015年-2021年　デュッセルドルフ日本商工会議所法務委員会専門委員
2016年-2017年　公正取引欧州委員会競争政策研究センター客員研究員
2017年-2018年　Gibson Dunn & Crutcher法律事務所ブリュッセルオフィス・オブカウンセル
2018年-2019年　Bird & Bird法律事務所ブリュッセルオフィス・パートナー
2018年-現在　一般財団法人情報法制研究所上席研究員
2019年-現在　当事務所開設・事務所代表、ニューヨークオフィス・マネージングパートナー、ブリュッセルオフィス・パートナー
2019年-現在　一般社団法人日本DPO協会理事
2020年-現在　当事務所東京オフィス・マネージングパートナー
2020年-現在　（一社）次世代基盤政策研究所上席研究員

主要な取扱分野

- カリフォルニア州消費者プライバシー法（CCPA）、カリフォルニアプライバシー権利法（CPRA），米国連邦データプライバシー法案、EUの一般データ保護規則（GDPR）、電子プライバシー規制、中国の個人情報保護法、日本の個人情報保護法、ブラジル・タイのデータ保護法をはじめとするグローバルデータ保護コンプライアンス
- EUのデジタル関連法案（AI規則案、デジタル市場法案、デジタルサービス法案、データ法案、データガバナンス法案）

最近の主要著作

- 「米国連邦データプライバシー法案の概要（2021年6月）」（2021年6月、ジェトロ・サンフランシスコ事務所）https://www.jetro.go.jp/world/reports/2021/01/7f744522a1ddc8eb.html
- 「カリフォルニア州消費者プライバシー法(CCPA)実務ハンドブック」（2019年12月、ジェトロ・サンフランシスコ事務所・イノベーション・知的財産部　スタートアップ支援課）https://www.jetro.go.jp/world/reports/2019/02/c74bb9695c95edf9.html

最近の主要講演

- 「GDPR実務アップデートウェビナー」（2021年7月、在蘭日本商工会議所、ジェトロ・アムステルダム事務所、当事務所共催）
- 「EUのデータ保護とデジタル分野の規則の最新動向と日本企業の対応」（デュッセルドルフ日本商工会議所主催）（2021年3月、デュッセルドルフ）
- CPRA解説オンラインセミナー～ BtoB企業が求められる実務対応を分かりやすく解説～（2021年1月13日、主催：ジェトロ・サンフランシスコ/ロサンゼルス様、協力：北加日本商工会議所様、南カリフォルニア日系企業協会様）
- CCPA最新動向解説ウェビナー（2020年7月31日、Keidanren USA）

最近の受賞実績

- 2019年12月16日付日本経済新聞朝刊11面（法務）の「企業が選ぶ弁護士ランキング」の「データ関連」の部門で第4位に、同月15日付日本経済新聞電子版「2019年第15回企業法務・弁護士調査」で「ライジングスター」部門に、それぞれ選出
- EUデータ保護法：Legal 500 EMEA 2019 & 2020: Belgium: EU Regulatory: Privacy and Data Protection
- EU競争法：Legal 500 EMEA 2018 & 2019: Belgium: Competition: EU and global

オンライン名刺交換は下のQRコードを御利用下さい

© S&K Brussels LPC 2021

S&K Brusselsは2019年にベルギーのブリュッセルで開業したEUと米国のデータ関連法を主な取扱分野とする弁護士・外国弁護士によって構成される日本の法律事務所です。EU・米国の立法機関におけるデータ関連法の立法動向を踏まえたFuture proofと規制監督当局との交渉の経験に裏打ちされたEU法・米国法の法的サービスを、世界で活躍する日本企業・組織の皆様に日本語と英語で御提供します。

S&K Brussels Website: https://www.sandkbrussels.com/

本書には、弁護士法人S&K Brussels法律事務所に権利の帰属する秘密情報が含まれています。本書の著作権は、本書において引用であることを明示したまたは引用であることが明らかな著作物等を除き、当事務所に帰属し、日本の著作権法および国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。本書に掲載されているサービス名、会社名等は各会社の商号、商標、または登録商標です。サービスの仕様および本書に記載されている事柄は、将来予告なしに変更することがあります。また、本書に記載された情報は、当事務所の依頼者への情報提供の目的で提供されるものであり、当事務所による法的助言を構成するものではないことに御留意下さい。

© S&K Brussels LPC 2021