Legal Wire

pillsbury

Japan Practice

Vol. 57 / June 2019

カリフォルニア州消費者プライバシー法施行へのカウントダウン（その2）：CCPA と GDPR のコンプライアンスは似て非なるもの

キャサリン・D・マイヤー、スティーブン・ファーマー、奈良房永、ラフィ・アジム・カーン

- CCPA はカリフォルニア州の「住民」に一定の権利を付与していますが、この「住民」とはカリフォルニア州所得税の賦課対象となる「住民」の定義によっています。
- CCPA のもとでプライバシーポリシー上開示が求められる事項の範囲は、GDPR よりも広いです。
- 一定の事項について消費者から請求があった場合、GDPR の開示対象外の請求でも CCPA のもとでは応じなければならない場合があります。

2018 年カリフォルニア州消費者プライバシー法（CCPA）は 2020 年 1 月 1 日に発効します。同法のもとでは、「消費者」に新たに以下の 5 つの権利が付与されることになります。「消費者」といっても、対象企業との関係で消費者であるとか何らかの関係にある必要はなく、あらゆるカリフォルニア州の住民を指します。[1]

1. 収集した個人情報のカテゴリー、情報源、情報の用途及び収集した情報の開示先等、企業のデータ収集の運用について知る権利
2. 消費者による請求から過去 12 ヶ月の間にその消費者について収集された具体的な個人情報のコピーを受け取る権利
3. かかる情報を削除してもらう権利（但し例外あり）
4. 企業のデータ売却の運用について知り、その消費者の個人情報を第三者に売却しないよう求める権利
5. 消費者らが CCPA により付与された新たな権利を行使したことに基づいて差別されない権利

これらの権利は、EU の一般データ保護規則（GDPR）のコンプライアンス対応に追われた企業にとってはお馴染みのもののように感じられるかもしれません。しかし、GDPR と今回の CCPA の間には似たところもある一方で、両者の間には重要な違いもあるので、GDPR を遵守していても CCPA コンプライアンスには不十分ということを認識しなければなりません。

とりわけ、CCPA 上の要請が GDPR 上の要請と異なる点としては、プライバシーポリシーでの開示事項及び個々の消費者から請求があった場合の開示事項について GDPR では求められていないものがあること、個々の消費者に係る具体的な情報の所在を把握しこれを提供することについても GDPR とは対象となる情報が異なっていること、「情報の売却」の定義が CCPA ではより広くなっていることから「情報の売却」として扱われる契約の見分け方も違ってくること、種々のポリシーや手続きを定めるに当たっても、CCPA では同法上の権利を行使した個々の消費者の差別を防止する対応も含まれることから、GDPR のもとで定めるとされているものとは相応に異なったものとなるはずであること、などがあります。

CCPA は GDPR よりも対象となる企業及び個人の範囲は狭いものの、個人に付与される権利はより幅広いものとなっています

EU 域内において自分のデータが処理されるか、又は一時的であっても自らが EU 域内にいる個人であれば権利が付与される GDPR と異なり、CCPA のもとでの権利が付与されるのは、カリフォルニア州の住民である個人に限られ、ここでいう住民とは所得税の賦課対象となる住民の定義によっています。CCPA は同州に一時的にいる者については適用されませんが、他の州の学校に通っている学生のような、一時的に州外にいるだけのカリフォルニア州の住民には適用されます。そのため、CCPA の対象となる個人の範囲は GDPR よりも狭いです。

GDPR においては、個人データとは識別された又は識別されうる個人に関するあらゆる情報をいうと定義されています。CCPA は、特定のカリフォルニア州の住民もしくは世帯と結び付けることができるか、又は直接若しくは間接的にこれらに繋がっているあらゆる情報をいうとして、その定義を広げているということができます。その結果、GDPR のもとでは、世帯に繋がる情報が常に個人データの定義にあたるとはいえないとの議論が可能ですが、CCPA のもとでは対象企業が対象情報の特定・所在の把握・開示の対応をしなければならない情報の範囲は GDPR よりも広くなります。

ある企業が CCPA の対象となるためには、その企業が営利企業（又は所有者の金銭的な利益を追求する企業）でなければならず、また財務上の要件もしくは一定のデータ処理を行っているとの要件を満たす必要があります。CCPA 上その企業がカリフォルニア州内に所在していることは求められていないものの、同州内でビジネスを行っていることは要件としています。加えてその企業は、年間の総収入が 2500 万米ドル超であるか、5 万人を超えるカリフォルニア州の住民の個人データを処理しているか、又は収入の 50%超をカリフォルニア州の住民のデータの売却から得ているかのいずれかの要件を満たしたものでなければなりません。対象となる企業を支配するか、又は同企業に支配されており、同一のブランドのもとにある関係会社も同法の対象となります。また、CCPA は非営利企業、政府系企業又は小規模企業には適用されません。他方 GDPR にはこのような要件はなく非営利企業にも同じように適用されるため、捕捉している会社の範囲としては CCPA よりも広くなっています。

CCPA では、データの売却にいう「売却」の定義がより広いこともあり、GDPR と比較してプライバシーポリシーで開示すべき事項が異なっています

CCPA も GDPR も、情報を収集した目的とそのあらゆる用途、個人の有する権利及びかかる権利を行使する方法をプライバシーポリシーに記載することを求めています。しかし、CCPA では更に進んで、その企業が個人データの売却を行っているか否か及び売却先となる第三者のカテゴリーについて記載することをも求めています。更に、CCPA では、プライバシーポリシー上の表示を常に最新の状態に保っていることが求められています。毎年記載をアップデートしなければならず、過去

12 ヶ月の間の活動を含めて開示しなければなりません。つまるところ、これによって、対象となる会社は CCPA 対応として 12 ヶ月ごとにプライバシーポリシーを見直さなければならないことになります。

従前、データの売却というと金銭を対価とするものが想定されてきました。CCPA では更に進んで、「売却」とはどのような形や様式により開示するかを問わず、金銭又はその他何らかの価値を有する対価と引き換えになされるおよそいかなる第三者に対する開示をも指すと定義されています。同法は各企業に対し、個々人によるかかる売却からオプトアウトしたいとの請求を行いやすくし、かつそのような請求があった場合にはきちんと言われた通りに対応するよう求めています。「その他何らかの価値を有する対価」という語は実質的に「売却」の定義を拡張しています。この定義だと、会社が個人データを業者に提供してデータ分析をしてもらっている場合も、会社の方から業者にデータ分析業務の料金を支払っているにもかかわらず、その会社が「データの売却をしている」とされる可能性があります。同法のもとでは、ある企業がデータを開示し、データへのアクセスを与える代わりにそのデータについての価値のある分析結果を得ることも、「売却」とされることがあるのです。このようなコンセプトは GDPR にはなく、したがって GDPR に沿ってデータの第三者への開示について正確に記載したとしても、CCPA の要求を完全に満たしたことにはならないものと考えられます。

CCPA は消費者による請求に基づく開示について GDPR に無い取扱いを求めています

GDPR も CCPA も、企業に対して自身についての個人情報を削除するよう請求する権利を個人に付与していますが、同時に、いずれも同じような要件のもと広く例外を認めています(ただし、CCPA のもとでの例外はより会社側に有利になっているということはいえそうです)。いずれの法も、個人は企業が保有する自身のデータのコピーを企業のデータベースから切り離して保有できる形で受け取ることができると定めていますが、CCPA はその対象となるデータを請求がなされる前 12 ヶ月以内に収集されたデータに限定している一方で、GDPR は(一定の例外はあるものの)保有する全てのデータの提供を求めています。CCPA のもとでは、企業は請求をしている個人の本人確認を行うこと、及び開示の請求に対して 45 日以内に応答することが求められています。カリフォルニア州の住民は 12 ヶ月の間に 2 回かかる請求を行うことができます。他方 GDPR のもとでの応答の期限はもっと短く(延長を必要とする正当な理由が無い限り)1 ヶ月であり、かかる請求をできる回数にも特に制限はありません。

データ収集の運用

企業のデータベースから切り離して保有できる形でデータの提供を受ける権利に関連して、CCPA のもとでは、企業は請求している個人の具体的な個人データの提供そのものと合わせて、データ収集の運用についても開示することが求められています。かかる開示においては、請求の前 12 ヶ月の間にその企業によって収集された個人情報のカテゴリー、情報源、データがビジネス上の目的で他に提供され又は売却されたか否か、及び情報の提供先となる第三者のカテゴリーについての記載をも含めなければなりません。他方 GDPR においては、請求への対応方法や、対象となる期間について 12 ヶ月の期間制限が無い点が CCPA と異なっています。

データ売却の運用とオプトアウト

CCPA はカリフォルニア州の住民に対し、請求の前 12 ヶ月間の企業の個人情報売却又は開示の運用に関する情報を請求する権利、及び 45 日以内に応答を受ける権利を認めています。

かかる応答においては、(1)売却されたデータのカテゴリー及び(2)ビジネス上の目的で開示されたデータのカテゴリーが、それぞれ当該データを受領する第三者のカテゴリーとともに明らかにされなければなりません。上記のデータ売却の定義の広さを踏まえると、CCPA 特有のかかる義務がきちんと履行されているかという観点から、会社が締結する様々な契約について再度見直す必要も出てきます。加えて、データを売却する対象企業は、消費者が個人データの売却からオプトアウトするために利用できる分かりやすくかつ無料の方法を提供し、かつ自社のホームページのウェブサイトにおいても、かかるオプトアウトの権利を行使できるページに繋がっている「私の個人情報を売らないで」というリンクを設置しなければなりません。CCPA のコンプライアンスでは、かかるオプトアウトの受領・管理のプロセスを伴うことが必然となるのです。このような開示やオプトアウトは GDPR のもとでは違った規定の仕方がなされており、したがって、企業としては全てのデータについて両方の法律で必要となる対応のいわば最大公約数を取って統一的に対応していくのか、それとも CCPA 対応と GDPR 対応で異なった対応をしていくのかの選択を迫られることとなりますが、こと後者の場合にはデータ管理の実務上かなり悩ましい問題を抱えることにもなりかねません。

差別の禁止及び執行

CCPA は権利行使をした個人を企業が差別することを禁止することによって、同法のもとで付与された権利を行使する個人を保護しようとしています。「差別をしない」とは具体的には、商品やサービスを拒否したり、人によって商品やサービスの値段や値引きの有無・金額、量や質が異なる、といった取扱いをしてはいけないということです。GDPR はこのような保護の仕組みを明確に定めていないため、CCPA の対象となる企業としては、コンプライアンス対応の中で、差別を禁止するポリシーや手続きを打ち出していくことで、この違いにも適応していく必要があります。

CCPA も GDPR とも、主な所管当局として、GDPR については各国のデータ保護機関、CCPA についてはカリフォルニア州司法長官があり、かかる当局によって法の執行が行われます。CCPA のもとでは、各消費者にはデータセキュリティの違反に関する執行として民事上の訴訟を提起する権利があり、また GDPR でも民事上のクラスアクションの制度があります。カリフォルニア州司法長官が自ら訴訟を提起する場合その 30 日前までに違反の事前通知を行わなければならず、違反 1 件あたり 2,500 米ドル(意図的な違反の場合は 7,500 米ドル)の罰金を科すことができます。各消費者は違反 1 件あたり 100 から 750 米ドルの賠償金を請求できます。他方 GDPR のもとでの違反に対する罰金は最高で 2000 万ユーロ又は全世界での収入の 4%(いずれか多い方)です。

本稿の原文(英文)につきましては、Countdown to CCPA #2: GDPR Compliance Does Not Equal CCPA Compliance をご参照ください。

[1] CCPA のもとでの要求はカリフォルニア医療情報秘匿法(CMIA)の対象となる「医療情報」又は HIPAA(医療保険の相互運用性と説明責任に関する法)のプライバシー、セキュリティ及び違反状態の通知に係る規則のもとで対象となる当事者や事業提携者によって収集された「保護対象健康情報」に対しては適用されません。更に、CMIA の対象となる医療事業者及び HIPAA の対象となる者は、それぞれ、CMIA の対象となる「医療情報」又は HIPAA の対象となる「保護対象健康情報」を保持するのと同じ方法で全ての患者の情報を保持している場合には、CCPA の対象外となります。CCPA は連邦のグラム・リーチ・ブライリー法又はカリフォルニア金融情報プライバシー法にしたがって収集、処理、売却又は開示された情報をも適用除外としています。これとは対照的に、GDPR には保健関連のデータについてのかかる適用除外は規定されていません。

本稿の内容に関する連絡先

奈良房永（日本語版監修）
31 West 52nd Street
New York, NY 10019
+1.212.858.1187
fusae.nara@pillsburylaw.com

池辺健太（日本語版作成協力）

Catherine D. Meyer
725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
+1.213.488.7362
catherine.meyer@pillsburylaw.com

Steven Farmer
Tower 42, Level 21, 25 Old Broad Street
London, EC2N 1HQ, England
+44.20.7847.9526
steven.farmer@pillsburylaw.com

Rafi Azim-Khan
Tower 42, Level 21, 25 Old Broad Street
London, EC2N 1HQ, England
+44.20.7847.9519
rafi@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com