

# 米国におけるPrivacy Policy 策定上の留意点

～CCPA / CPRAを踏まえた実務上のポイント～

2021年10月28日

SGR法律事務所 弁護士 小島 清顕

# 事務所紹介

Smith Gambrell & Russell, LLP (SGR)

スミス・ガンブレル&ラッセル法律事務所(SGR法律事務所)は、1893年に創設された創業約130年の米国ジョージア州アトランタ市発祥の総合法律事務所です。ニューヨーク、ロサンゼルス、ワシントンDC、フロリダ、テキサス、ロンドン、ミュンヘン等主要都市にオフィスを構え、約300人の弁護士が所属しています。

取扱分野は、法人設立、各種契約、M&A・合併・業務提携、雇用・労務、訴訟・紛争、企業誘致・助成金交渉、貿易・通商関連、環境、建設、不動産、知財、倒産、税務、遺産相続計画、年金・福利厚生、海事、サイバーセキュリティ・情報保護法、移民法・ビザ等、企業法務全般をカバーしています。全米法律事務所ランキング・トップ200(Am Law 200)にも継続して選出されています。日本チームは、上記の総合法律サービスを日本語により提供しています。詳しくは、SGR法律事務所の日本語ページをご参照ください。ご不明な点、ご質問等ございましたら、正式にご起用いただくまで費用は発生いたしませんので、お気軽にご相談ください。

日本語ページ <https://www.sgrlaw.com/practices/japan-practice-team/>

\* 弊所では、米国の法律に関わる最新情報・ウェビナーの案内等ニュースレターを配信しております。ご希望の方は、右記QRコード、またはジャパンデスク 柿内のメールアドレス [skakiuchi@sgrlaw.com](mailto:skakiuchi@sgrlaw.com) からお申し込み下さい。



# 講師紹介

Smith Gambrell & Russell, LLP (SGR)

いつでもお気軽にお問い合わせください。

小島 清顕  
Kiyooki (Kiyoo) Kojima  
Partner



Smith, Gambrell & Russell, LLP

Address Suite 1000

1105 W. Peachtree St. N.E.

Atlanta, GA 30309

Telephone 404-815-3893

E-mail [kkojima@sgrlaw.com](mailto:kkojima@sgrlaw.com)

## 【経歴】

日本出身(地元:神奈川県小田原市)、幼少期から米国在住。ロチェスター大学(NY州)で政治学・経済学を二重専攻し卒業。同時期にイーストマン音楽学校にてファゴットを学ぶ。学位取得後、インディアナ大学ロースクールと音楽校に同時進学。JD取得後、2003年からホームタウンのジョージア州アトランタ市を拠点に米国各地で弁護士業務を営む。専門業務として、法人設立やコンプライアンス・再編等に伴う相談、交渉・各種取引アドバイス、M&A・JV・共同開発・ライセンシング案件、雇用・労務案件、社内ポリシー作成や遂行、紛争防止・対応(特に調停と仲裁)、知的財産管理・保護・活用、企業誘致・土地選定・インセンティブ交渉と文書化、その他各種幅広い法務に対応。SGR 法律事務所にパートナー弁護士として在籍、Japan Practice を立ち上げる。

# 講師紹介

Smith Gambrell & Russell, LLP (SGR)

佐賀 洋之  
**Hiroyuki Saga**  
Exchange Attorney

Smith, Gambrell & Russell, LLP  
Address Suite 1000  
1105 W. Peachtree St. N.E.  
Atlanta, GA 30309  
E-mail [hsaga@sgrlaw.com](mailto:hsaga@sgrlaw.com)



**【経歴】**

2014年東京大学法科大学院修了。

2015年弁護士登録。同年よりアンダーソン・毛利・友常法律事務所外国法共同事業にて執務。コーポレート(株主総会対応・M&Aを含む業務提携・グローバル報酬プランの設計等)、国内外のベンチャー企業に対する投資案件、独占禁止法・下請法対応、国内外の訴訟対応等を主たる業務分野として活躍。

2021年米国コロンビア大学ロースクール(LL.M.)修了。  
2021年8月からSGR法律事務所にて交換弁護士として執務。

# 本ウェビナーの概要

|       |                                  |      |
|-------|----------------------------------|------|
| I.    | そもそも「プライバシー」とは？                  | P.2  |
| II.   | “Privacy Policy”とは？              | P.5  |
| III.  | CCPA・CPRAについて ① CCPA ② CPRA      | P.10 |
| IV.   | Privacy Policy に盛り込むべき内容         | P.19 |
| V.    | Privacy Policy に盛り込むべき内容～CCPA対応～ | P.29 |
| VI.   | Privacy Policy に盛り込むべき内容～GDPR対応～ | P.33 |
| VII.  | 社内規定としての Privacy Policy          | P.35 |
| VIII. | Privacy Policy をめぐる世界的動向         | P.37 |
| IX.   | おわりに                             | P.41 |

# はじめに ～ Privacy Policyとは？～

# I. そもそも「プライバシー」とは？

## □ プライバシーの辞書的意味

- ✓ 個人や家庭内の私事・私生活、個人の秘密
- ✓ 他人から干渉・侵害を受けない権利(大辞泉)

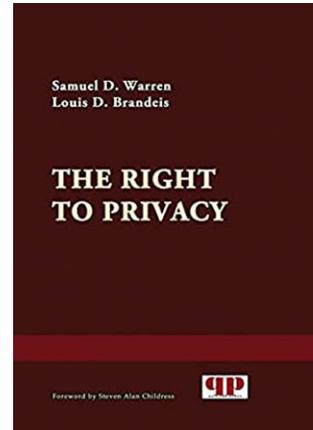


## □ 歴史を振り返ると...プライバシーはそもそも存在しなかった

- ✓ かつては「共同生活」が当然であったため、「プライベートな空間」という概念がそもそも存在しなかった
  - 古代ローマ: トイレや浴場は公共の場
  - 「寝室」がヨーロッパの富裕層の間に浸透したのは17世紀以降
  - イギリス: 18世紀半ばの産業革命の結果、仕事の間は家庭から工場や事務所へ移転。結果として家庭は純粋な私生活の場となる。

# I. そもそも「プライバシー」とは？

- 個人が享受する権利として確立したのは更に後世になって
  - ✓ 1890年、弁護士であったWarren及びBrandeisによる「The Right to Privacy」(ハーバード・ロー・レビュー)において提唱される
    - 過剰なイエロージャーナリズムへの対抗手段として醸成
    - 「一人で放っておいてもらう権利」として定義
  - ✓ Prosser教授によるプライバシーの権利の細分化(1960年)
    - プライバシーの侵害行為を体系化
  - ✓ 個人の権利として認められたのは1967年の最高裁判決(Katz v. United States (389 U.S. 347))



# I. そもそも「プライバシー」とは？

## □ 現代におけるプライバシーの「**複雑化**」

- ✓ 情報化社会におけるプライバシー概念の変化
  - ネット上で暗号化された個人のデータ自体がプライバシーを形成
  - **世界中のどこからでも、誰に対してもプライバシーの侵害が可能**な時代
  - 物理的な壁だけでは私生活を守れない時代
- ✓ 企業が抱える個人情報量の増加及び内容の複雑化
  - ✓ 顧客や取引先情報は企業にとっての「**資産**」
  - ✓ ハッキング等による情報漏えい＝企業にとって莫大な損失
  - ✓ 個人情報の第三者への開示をめぐるトラブルが多発



## II. “Privacy Policy”とは？

- 何を定めた文書か：企業活動における個人情報について、
  - 1) どのように取得し
  - 2) どのように使用し
  - 3) どのように管理するかについて定めたもの
- Privacy Policyの種類：大きく分けて以下の2パターンが存在
  - 1) サービスやウェブサイトの利用者等、外部向けのPrivacy Policy
  - 2) 従業員等内部者向けの社内規定としてのPrivacy Policy  
(関連する他の規定として、Information Management Policy等)
- 本日は主に外部向けのPrivacy Policyを念頭に解説

## II. “Privacy Policy”とは？

### □ なぜPrivacy Policyを策定するのか？米国では…

- ✓ 個人情報の利用目的について情報提供者に通知するため
- ✓ 個人情報の第三者提供について同意を得るため
- ✓ 個人情報の提供者による権利行使の手順等について定めるため

### □ California州におけるCCPA／CPRA対応

- ✓ 特にCalifornia州において事業活動を行う場合、CCPA(California Consumer Privacy Act)、CPRA(California Privacy Rights Act)を意識した個人情報保護体制の構築が必要であり、その一環としてPrivacy Policyの策定／運用が重要視される
- ✓ CCPA及びCPRAの詳細については後述

# II. “Privacy Policy”とは？

## □ 日本におけるPrivacy Policy

- ✓ 米国と同様の趣旨が当てはまるほか、**Pマーク**の取得といった対外的なアピールもPrivacy Policy策定の趣旨として含まれる
  - Pマーク(プライバシーマーク): 個人情報の保護体制に対する**第三者認証制度**。個人情報保護体制の基準への適合性を評価し、一般財団法人日本情報経済社会推進協会が使用を許諾
- ✓ 日本国外への意識
  - 米国をはじめ国外での情報運用を前提とする必要(詳細は後述)



# II. “Privacy Policy”とは？

## □ 日本におけるPrivacy Policyの例（各趣旨への対応例）

- ✓ 個人情報の利用目的についてユーザーに通知する
  - 「当社は、以下に示す利用目的のために、皆様から個人情報をご提供いただく場合があります。下記以外の目的で個人情報を収集・利用する際は、利用目的をお知らせしたうえで収集いたします。」
- ✓ 個人情報の第三者提供についての同意取得（多くの場合、Privacy Policyを確認し、了解した旨のユーザーのチェックを通じて）
  - 「当社は、以下の提供先に対して各項に従い、書面または電磁的な方法により個人情報を提供いたします。」
- ✓ 個人情報の提供者による権利行使の手順等について定める
  - 「ユーザー本人または代理人は、当社所定の手続きに従い、ユーザー本人が識別される個人情報の開示・内容の訂正、追加または削除・利用の停止または消去および利用目的の通知を求めることができます。具体的な請求方法については〇〇（問合せ先）にご連絡ください。」

# CCPA及びCPRAの概要

# III. CCPA・CPRAについて ①CCPA

## □ CCPA: カリフォルニア州消費者プライバシー法

- ✓ 2020年1月1日施行(州司法局による運用は同年7月1日開始)
- ✓ **Californians for Consumer Privacy**(プライバシー保護団体)が主導して住民提案した法令
- ✓ 適用対象: カリフォルニアで事業活動を行う事業者は、**拠点がカリフォルニア州内に存在するか否かにかかわらず**、以下の**いずれか**に該当する場合は適用対象
  - 年間総収入(全世界)が2,500万ドルを超えている
  - 5万人以上のカリフォルニア州の居住者、世帯又はデバイスの個人情報を購入、受信、又は販売している
  - カリフォルニア州の住民の個人情報を販売することによって、年間収益の50%以上を得ている

# III. CCPA・CPRAについて ①CCPA

## □ CCPAに違反した場合のリスク

- ✓ CCPAの執行機関はカリフォルニア州司法長官であり、違反が発覚した場合、以下の執行が可能  
(※不遵守の通知から30日間の**治療期間**あり)
  - **差し止め**
  - 違反ごとに**最大2,500米ドル**の民事制裁金
  - **意図的な違反**の場合は違反ごとに**最大7,500米ドル**の民事制裁金
- ✓ 上記執行以外にも、消費者による**私的訴訟権行使**も可能(事案ごとに一人最大750米ドル又は実損害のいずれか高い方を請求可能)



## □ 適用事例: (<https://oag.ca.gov/privacy/ccpa/enforcement>)

- ✓ 現時点では不遵守の通知に応じてPrivacy Policyをアップデートしたといった例が**最も多い**  
(**例示として公表された27件中14件**)ものの、制裁金が実際に課された事例はまだない
- ✓ **CCPAを引用する民事訴訟は増加傾向**にあり、今後も動向が注目される

# III. CCPA・CPRAについて ②CPRA

## □ CPRA: カリフォルニア州プライバシー権利法

- ✓ CCPA同様、Californians for Consumer Privacy が主導して住民提案、2020年11月3日の住民投票において可決
- ✓ 2023年1月1日適用開始、同年7月1日以降に執行開始となるが、CPRA上の事業者の義務(消費者による事業者に対する開示請求等権利行使)は2022年1月1日以降に収集した個人情報に関して適用
- ✓ 適用対象: B to B企業に対しても幅広く適用(以下は全て適用可能性あり)
  - カリフォルニア州内の米国子会社
  - カリフォルニア州外の米国子会社
  - カリフォルニア州内に事業所を持つ日本国内の日本企業
  - カリフォルニア州内に事業所を持たない日本国内の日本企業



# III. CCPA・CPRAについて ②CPRA

- CPRAとCCPAとの比較: CPRAはCCPAの強化版
  - ✓ 「**共有**」概念の新設(データ「売却」とは異なる概念として)
  - ✓ カテゴリーとしての「**センシティブ情報**」の新設
  - ✓ プライバシー保護法令の執行を**専門に扱う行政機関**(**カリフォルニア州プライバシー保護庁**(California Privacy Protection Agency))の新設
  - ✓ **私的訴訟権の拡大**、16歳未満の消費者の個人情報に関連するCCPA違反への制裁金の増額
  - ✓ CCPAに存在する「**治癒期間**」は必ずしも保証されない: **民事制裁金が賦課される事例が今後増加する可能性**
- 適用対象につき、次頁以降の4種類のテストのうち**いずれか**を充足する場合には、CPRAが適用される「**事業者**」に該当

# III. CCPA・CPRAについて ②CPRA

## □「事業者」該当性テスト(1)

### <テスト1(以下①②のいずれも充足する場合)>

- ✓ 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(第三者を介して取得する場合を含む)し、単独又は共同でその処理の目的・手段を決定し、利益又は金銭的便益を目的としてカリフォルニア州において事業活動を行っていること
- ✓ 要件②: 以下の3つの事由のいずれかを充足すること
  - 1月1日時点で、前年の(全世界での)年間総売上が2,500万米ドル超である
  - 年間ベースで10万件以上の消費者又は世帯の個人情報を単独若しくは組み合わせた形で購入若しくは販売又は共有している
  - 消費者の個人情報の販売又は共有によって年間収入の50%以上を得ている



# III. CCPA・CPRAについて ②CPRA

## □「事業者」該当性テスト(2)

### <テスト2>

- ✓ テスト1に該当する事業者を支配し又は当該事業者によって支配され、かつ、当該事業者と共通のブランドを有している、当該事業者が消費者の個人情報共有する主体
  - 例：日本企業のグループ会社の中にテスト1を充足する事業者が存在し、(商号に共通性がある等の理由で)共通のブランドを有している場合であって、当該事業者から個人情報の共有を受けているときは、当該日本企業にCPRAが適用される

# III. CCPA・CPRAについて ②CPRA

## □「事業者」該当性テスト(3)

### <テスト3>

- ✓ (いずれかのテストに適合する)各事業者が少なくとも40%の持分を有する、事業者によって構成されるジョイントベンチャー又はパートナーシップ
  - JV/Partnershipと、これらを構成する事業者はCPRA上は別の事業者

### <テスト4>

- ✓ カリフォルニア州で事業を行う者で、上記テスト1～3の対象とならないものの、CPRAに準拠/拘束されることに同意する旨をプライバシー保護当局へ自主的に宣明した者

# III. CCPA・CPRAについて まとめ

## □ CCPA・CPRAを踏まえた消費者の権利／事業者の義務

| 消費者の権利                 | 対応する事業者の義務(規制内容)   |
|------------------------|--|
| 知る権利                   | (A) 利用目的の通知:①通知事項(追加あり)、②通知態様、③目的外利用の禁止、④情報の保持期間の限定<br>(B) 消費者が請求を行う場合の対応事項:①開示事項、②行使方法の提供、③権利行使の受領確認<br>④事業者サイドの対応期限、⑤費用(要求があれば無償で情報提供)、⑥本人確認、⑦請求時の事項<br>(C) Privacy Policyの開示:①開示方法、②記載事項(少なくとも12ヶ月に1回はアップデート) |
| センシティブ情報の利用及び開示を制限する権利 | 制限請求の手續<br>(※「センシティブ情報」はCPRAで新設)   |
| 削除請求権                  | 削除請求への対応義務:<br>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   |
| 訂正請求権                  | 訂正請求への対応義務<br>(※「訂正請求権」はCPRAで新設)   |
| 個人情報の売却又は共有についてのオプトアウト | オプトアウト手續:<br>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 (※「共有」はCPRAで新設)   |
| 未成年者のオプトイン             | 未成年者についてのオプトイン手續(※CPRAで新設)   |
| 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<br>【その他事業者サイドで行うべき事項】<br>①売却／共有先となる第三者、個人情報の開示先となるサービス提供者や契約受託者との契約締結、②研修<br>③記録管理、④個人情報の性質に照らし合理的なセキュリティ手續／慣行の導入・実施、⑤データ保護影響評価                                       |

# III. CCPA・CPRAについて まとめ

## □ CPRAによって新たに対応が必要な事項

- ✓ 「共有」の概念、「センシティブ情報」という枠組みを始めとした追加のコンセプトや新たに追加された消費者の権利に対する理解を深める
  - ① 体制面: 「事業者」該当性の確認(14頁)、管理部門における研修実施、保有個人情報のカテゴリーのアップデート(センシティブ情報の追加)等
  - ② 運用面: 消費者からの問い合わせや請求に対するマニュアルの更新、現場担当者への研修実施等
- ✓ 個人情報の売却／共有先となる第三者との契約書を見直す  
例: 属性(サービスプロバイダ、契約受託先等)に応じて禁止事項を設定する
- ✓ プライバシー通知のアップデート(新規の権利やセンシティブ情報)
- ✓ Privacy Policyの見直し(次頁参照)

# III. CCPA・CPRAについて まとめ

## □ CPRAによってPrivacy Policyに追加すべき事項

- ✓ 個人情報「共有」の事実・可能性に関する言及
- ✓ 訂正請求権についての規定(27頁)
- ✓ センシティブ情報についての条項追加・手当て(22頁、23頁)

※CPRA規則は未公表であるため、追加で対応を強いられる可能性あり

## □ CPRAの全容が確定するCPRA規則の採択期限:2022年7月1日

(\*Privacy Policyのサンプルについても、CPRAのあらゆる規制に対応するものではない(アップデートを要する)点お含みおきください)



# 実践編

## ～Privacy Policyに盛り込むべき内容～

# IV. Privacy Policyに盛り込むべき内容

## □ ①適用対象となる情報

- ✓ 大前提として、どのような情報(どのようにして取得される情報)がPrivacy Policyの適用を受けるかについて明確に定める必要あり
- ✓ 個別のサービスやWebsiteの性質に応じて調整

SAMPLE

We collect several types of information from and about users of our Website, including information:

- By which you may be personally identified, such as name, postal address, e-mail address, telephone number any other identifier by which you may be contacted online or offline.
- About your internet connection, the equipment you use to access our Website, and usage details.

The information we collect on or through our Website may include:

- Information that you provide by filling in forms on our Website. This includes information provided at the time of registering to use our Website, subscribing to our services, posting material, or requesting further services. We may also ask you for information when you report a problem with our Website.
- Records and copies of your correspondence (including email addresses), if you contact us.

As you navigate through and interact with our Website, we may use automatic data collection technologies to collect certain information about your equipment, browsing actions, and patterns, including:

- Details of your visits to our Website, including usage details, logs and other communication data and the resources that you access and use on the Website.
- Information about your computer and internet connection, including your IP address, operating system, and browser type. (\* “Website”はPolicy上に定義)

# IV. Privacy Policyに盛り込むべき内容

## □ ①適用対象となる情報(続) – CCPA適用を見越した詳細例(1) –

※**赤線**はCPRAにおいてセンシティブ情報と認定されうるもの

SAMPLE

| Category   | Examples  |
|--|---|
| Identifiers.   | A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, <b>account name</b> , <b>Social Security number</b> , <b>driver's license number</b> , <b>passport number</b> , or other similar identifiers.  |
| Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)). | A name, signature, <b>Social Security number</b> , physical characteristics or description, address, telephone number, <b>passport number</b> , <b>driver's license or state identification card number</b> , insurance policy number, education, employment, employment history, <b>bank account number</b> , <b>credit card number</b> , <b>debit card number</b> , or any other financial information, medical information, or health insurance information.             |
| Protected classification characteristics under California or federal law.  | Age (40 years or older), <b>race</b> , <b>color</b> , <b>ancestry</b> , <b>national origin</b> , <b>citizenship</b> , <b>religion</b> or creed, marital status, <b>medical condition</b> , physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), <b>sexual orientation</b> , veteran or military status, <b>genetic information (including familial genetic information)</b> . |
| Commercial information.  | Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.  |
| Biometric information.   | <b>Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information</b> , such as, fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.   |

# IV. Privacy Policyに盛り込むべき内容

## □ ①適用対象となる情報(続) – CCPA適用を見越した詳細例(2) –

※**赤線**はCPRAにおいてセンシティブ情報と認定されうるもの

SAMPLE

| Category   | Examples   |
|--|--|
| Internet or other similar network activity.  | Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.   |
| Geolocation data.  | <b>Physical location or movements.</b>   |
| Sensory data.  | Audio, electronic, visual, thermal, olfactory, or similar information.   |
| Professional or employment-related information.  | Current or past job history or performance evaluations.  |
| Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)). | Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records. |
| Inferences drawn from other personal information.  | Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.  |

# IV. Privacy Policyに盛り込むべき内容

- ①適用対象となる情報(続) – CCPA対応: 除外される情報の列挙 –
  - ✓ 明確化の観点から、どのような情報は保護対象から外れるかについて明示する

SAMPLE

Personal information **does not include**:

- Publicly available** information from government records.
- De-identified or aggregated** consumer information.
- Information excluded from the CCPA's scope, like:
  - health or medical information covered by the Health Insurance Portability and Accountability Act of 1996 (**HIPAA**) and the California Confidentiality of Medical Information Act (**CMIA**) or clinical trial data;
  - personal information covered by certain sector-specific privacy laws, including the Fair Credit Reporting Act (**FCRA**), the Gramm-Leach-Bliley Act (**GLBA**) or California Financial Information Privacy Act (**FIPA**), and the Driver's Privacy Protection Act of 1994.



# IV. Privacy Policyに盛り込むべき内容

## □ ②個人情報の利用目的

- ✓ 利用目的を具体的かつ詳細に記載することは極めて重要
- ✓ 「サービス向上のため」・「今後の事業展開のため」といった曖昧な内容のみ記載する対応はもはや**NG!!**

SAMPLE

We use information that we collect about you or that you provide to us, including any personal information:

- To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to request a price quote or ask a question about our products or services, we will use that personal information to respond to your inquiry.
- To provide, support, personalize, and develop our Website, products, and services.**
- To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve our responses.
- To help maintain the safety, security, and integrity of our Website, products and services, databases and other technology assets, and business.**
- For testing, research, analysis, and product development, including to develop and improve our Website, products, and services.**
- To respond to law enforcement** requests and as required by applicable law, court order, or governmental regulations.
- To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by Company about our Website users is among the assets transferred.

(\* “Company”はPolicy上に定義)

# IV. Privacy Policyに盛り込むべき内容

## □ ③個人情報の開示対象

- ✓ 提供された個人情報をどのような場合に、どのような相手に開示する可能性があるか

SAMPLE

**We may disclose**, without restriction, aggregated information about our users, and information that does not identify any individual.

We may disclose personal information that we collect or you provide as described in this privacy policy:

- To our **subsidiaries** and **affiliates**.
- To a **buyer** or other **successor** in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Company assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by Company about our Website users is among the assets transferred.
- To fulfill the purpose for which you provide it.**
- For any other purpose disclosed by us** when you provide the information.
- With your consent.**

We may also disclose your personal information:

- To comply with any **court order, law, or legal process**, including to respond to any government or regulatory request.
- To enforce or apply our terms of use [**inset a link to the Terms of Use**] and other agreements, including for billing and collection purposes.

# IV. Privacy Policyに盛り込むべき内容

## □ ④個人情報主体の権利

- ✓ 情報提供主体がどのような権利を行使できるかを明記する

SAMPLE

You may have legal rights when it comes to how your personal information is handled.

These rights may vary depending on the applicable jurisdiction, but may include for example:

- A **right to know** what personal information the Company maintains about you and/or with whom the Company has shared the personal information.
- A **right to access** the personal information, including obtaining the specific pieces of information collected from you.
- A **right to delete** your personal information.
- A **right to opt-out** of personal information sales.
- A **right to opt-out** of using personal information for targeting advertising or marketing purposes.
- A **right to non-discriminatory treatment** for exercising any rights. (CCPA対応)
- A **right to initiate a private cause of action for data breaches**. (CCPA対応)

※CPRAにおいては、以下の権利を追加することが考えられる

- A **right to limit the use of sensitive personal information**. (CPRA対応)
- A **right to manage and request corrections to personal information**. (CPRA対応)



# IV. Privacy Policyに盛り込むべき内容

## □ ⑤個人情報主体の権利の行使方法

- ✓ ④の個人情報主体の権利の具体的な行使方法を定める

SAMPLE

**You can review and change** your personal information by logging onto the Website and visiting your account profile page.

You may also send us an email at [email address] **to request access to, correct or delete** any personal information that you have provided to us. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect.

Your access to and use of information provided on the Website is governed by our terms of use [inset a link to the Terms of Use].

California residents may have additional personal information rights and choices. Please see Your California Privacy Rights section below for more information. (CCPA 対応)

## □ ⑥個人情報主体の権利の行使方法

- ✓ 一般条項として、**Policyの変更及び当該変更に対する利用者の「みなし同意」**について言及

SAMPLE

If we make material changes to how we treat our users' personal information, **we will post the updated version of the privacy policy on the Website together with the policy's updated effective date.**

**Your continued use of our Website following the posting of changes constitutes your acceptance of such changes.**

The date this policy was last revised is identified at the top of the document. You are responsible for ensuring that we have an up-to-date, active and deliverable email address for you, and for periodically visiting our Website and this policy to check for any changes.

# V. Privacy Policyに盛り込むべき内容 ～CCPA対応～

## □ California州における特別な対応

- ✓ California 州において対消費者向けの事業が存在する場合、特にCCPA(及びCPRA)を意識した条項を容易する必要あり
  - California対応のPrivacy Policyを別途作成するのではなく、(例えば)一般的な(前頁までの基本項目を押さえた)条項の後ろに「Your California Privacy Rights (“California Notice”)」といった形で、カリフォルニア州の住民に特に適用される章を設けることで、1つの汎用的なPrivacy Policyを策定することが可能
- ✓ 既に言及しているもののほか、CCPA適応を意識した、より詳細なPrivacy Policyにおける規定例(あくまで一部)は次頁以降参照
- ✓ CPRAに関しては現状判明している情報からして確実な部分のみ反映

# V. Privacy Policyに盛り込むべき内容 ～CCPA対応～

## □ ①差別関連

- ✓ 情報提供者の権利行使を理由とした不利益な取扱いを行わないことを確認的に記載

### Non-Discrimination

**We will not discriminate against you for exercising any of your CCPA rights.** Unless permitted by the CCPA, we will not:

- Deny you** goods or services.
- Charge you** different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you** a different level or quality of goods or services.
- Suggest that you** may receive a different price or rate for goods or services or a different level or quality of goods or services.

SAMPLE

# V. Privacy Policyに盛り込むべき内容 ～CCPA対応～

## □ ②情報主体の権利

✓ 権利行使の条件を含め、仔細まで定める必要あり

SAMPLE

### Access to Specific Information and Data Portability Rights

You have the **right to request that Company disclose** certain information to you about our collection and use of your personal information over the **past twelve (12) months**. Once we receive and confirm your verifiable consumer request, we will disclose to you:

- i. The **categories of personal information** we collected about you.
- ii. The **categories of sources for the personal information** we collected about you.
- iii. **Our business or commercial purpose** for collecting that personal information.
- iv. The **categories of third parties** with whom we share that personal information.
- v. The **specific pieces of personal information** we collected about you (also called a data portability request).
- vi. If we disclosed your personal information for a business purpose, **a list identifying the personal information categories that each category of recipient obtained**.

### Limitation of Exercise of Rights

**You may only make** a verifiable consumer request for access or data portability **twice within a 12-month period**. The verifiable consumer request must:

- i. Provide **sufficient information that allows us to reasonably verify that you are the person about whom we collected personal information or an authorized representative**.
- ii. Describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it.
- iii. We cannot respond to your request or provide you with personal information if we cannot verify your identity, or authority to make the request, and confirm the personal information relates to you. Making a verifiable consumer request does not require you to create an account with us.
- iv. We will only use personal information provided in a verifiable consumer request to verify the requestor's identity or authority to make the request.

# V. Privacy Policyに盛り込むべき内容 ～CCPA対応～

## □ ③個人情報削除要請に対応しない場合

✓ 予測可能性を高める観点からも、どのような場合に要請に対応できないかを明記

SAMPLE

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- i. Complete the transaction for which we collected the personal information, provide a good or service that you requested, take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you.
- ii. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities.
- iii. Debug products to identify and repair errors that impair existing intended functionality.
- iv. Exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise other rights provided for by law.
- v. Comply with the California Electronic Communications Privacy Act (Cal. Penal Code § 1546 et. seq.).
- vi. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement, if you previously provided informed consent.
- vii. Enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us.
- viii. Comply with a legal obligation.
- ix. Make other internal and lawful uses of that information that are compatible with the context in which you provided it.

# VI. Privacy Policyに盛り込むべき内容 ～GDPR対応～



## □ GDPR (General Data Protection Regulation) の特徴

✓ 適用範囲の広さ: 以下の場合に広く域外適用される

### ▪ EU域内のデータ主体に対する物品又はサービスの提供

(例: EU域内の顧客がサービスサイトにアクセスし、問い合わせフォーム等に個人情報を登録する場合)

### ▪ EU域内のデータ主体のモニタリング

(例: EU域内に設定してある子会社が収集した顧客の個人情報に、日本の本社からアクセスして日本の端末に個人情報を表示する場合)

✓ CPRAと比較してより重い義務が課される(データ侵害の通知義務等)

## □ Privacy Policy上の対応: CCPAと同様に、単一のPrivacy Policyの中にGDPRに対応する章を設けることが可能

# VI. Privacy Policyに盛り込むべき内容 ～GDPR対応～

## □ GDPR対応条項の例(一部)は以下のとおり

SAMPLE

### Legal Bases for Processing Personal Information of European Union Citizens

When processing your personal information, Company may rely on one or more of the following **legal bases** (or other available legal grounds), depending on the circumstances:

- i. **Legitimate Interests**. We may process your personal information where Company has a legitimate interest in such processing for managing, operating or promoting our business, and that legitimate interest is not overridden by your interests, fundamental rights or freedoms.
- ii. **Consent**. We may process your personal information where Company has obtained your consent to the processing.
- iii. **Contractual Necessity**. We may process your personal information where such processing is necessary in connection with any contract that Company has with you.
- iv. **Legal Requirements**. We may process your personal information where such processing is required by applicable law.

### Your Rights as a European Union Citizen

You have a number of rights concerning your personal information that Company holds and uses, including the following:

- i. **Right of Access**. You have the right to be informed about what personal information Company holds about you and to a copy of this personal information.
- ii. **Right to Rectification**. You have the right to have any inaccurate personal information which Company holds about you updated or corrected.
- iii. **Right to Erasure**. In certain circumstances you may request that Company delete the personal information that Company holds about you.
- iv. **Right to Complain**. You have the right to lodge a complaint regarding the processing of your personal information to an applicable governmental or supervisory authority in your country.
- v. **Right to Withdraw Consent**. Where processing of personal information is based on your consent, you have the right to withdraw such consent at any time.
- vi. **Right to Object**. Where Company relies on its legitimate interests to process your personal information, you have the right to object to such use and Company is required to discontinue such processing unless Company can demonstrate an overriding legitimate interest in such processing.
- vii. **Right to Restriction**. You have the right to request that Company stop using your personal information in certain circumstances including if you believe that the personal information Company holds about you is inaccurate or that Company's use of your personal information is unlawful. If you validly exercise this right, Company will store your personal information and will not carry out any other processing until the issue is resolved.

# VII. 社内規定としてのPrivacy Policy

## □ 社内規定としてのPrivacy Policyの意義

- ✓ 概要：従業員や外部ベンダー等、社内で個人情報に触れる可能性のある人員に対して適用される、個人情報の取扱いに関する社内規定
- ✓ ポイント：企業活動の過程でどのような形で、どのような個人情報を取得するか、情報提供主体はどのような権利を有しているかを周知する
- ✓ 有事対応：Privacy Policy内にて、社内で個人情報の漏洩が発覚した場合の対応について規定する
  - 管掌部署・役職の指定
  - 他の有事対応に関する規定（Risk Management Policy等）との関係性



おわりに  
～Privacy Policyを巡る世界的動向  
今後の対応ポイントと共に～

# VIII. Privacy Policyをめぐると世界的動向

## □ アメリカ

- ✓ 個人情報保護法制については、EUのGDPRが先行
- ✓ 米国では、情報漏えい事件や「なりすまし犯罪」が増加する一方、ビッグデータやIoT等のデータを活用したビジネスが日常生活に浸透しつつある状況
  - 次世代の個人情報保護制度が喫緊の重要課題として認識されている
- ✓ 連邦法: **個人情報保護のための包括的な連邦法は未制定**
  - (FTC法 (Federal Trade Commission Act) Section 5 (a)(1)が抽象的に「**不公正若しくは欺瞞的な行為又は慣行**は、本法により違法と宣言する」と定めるのみ)
- ✓ 州法: CCPAやCPRAをはじめ、州法レベルでの対応が進んでおり(例: バージニア、コロラド)、**連邦法レベルでの個人情報保護法制の整備が今後予想**される(民主党の政権公約における項目化: 現状は民主党案である**COPRA (C**onsumer **O**nline **P**rivacy **R**ights **A**ct)をベースとした立法化が有力)



# VIII. Privacy Policyをめぐる世界的動向

## □ 中国

- ✓ **中国版個人情報保護法** (PIPL) が2021年11月1日に施行予定
  - 2017年6月1日施行の「**サイバーセキュリティ法**」、2021年9月1日施行の「**データセキュリティ法**」と並ぶ、中国における情報・データ管理法制度に関する基本法
- ✓ **適用範囲**: 中国国外において中国国内の自然人の個人情報を処理する場合であっても、以下の**いずれか**に該当する場合は適用されるため、注意が必要
  - 1) 中国国内の自然人に向けて商品またはサービスを提供することを目的としている場合
  - 2) 中国国内の自然人の行為を分析し、評価するためである場合
  - 3) 法律若しくは**行政法規の規定する**その他の状況に該当する場合

# VIII. Privacy Policyをめぐる世界的動向

## □ 中国版個人情報保護法の内容

- ✓ 越境規制: 中国(本土)外への個人情報の提供(持出し)を制限
  - 国家ネットワーク情報部門(CAC: **C**yberspace **A**dministration of **C**hina)の安全評価への合格や、CACの定める標準契約書に依拠する場合等に例外的に許容
  - 国外の個人情報取扱者が「ブラックリスト」に指定された場合、当該事業者に対する個人情報の提供自体が禁止される
- ✓ 個人の権利: 知る権利や訂正請求権、削除請求権等、GDPRに類似
- ✓ 個人情報取扱者の義務: 有事の際の通知義務や個人情報保護影響評価制度等、CCPA・CPRAやGDPRに近い内容
  - 大型インターネットプラットフォームサービス提供者には報告義務等特別義務が課されるといった特色も(具体的な該当基準は今後施行細則で定まる見込み)
- ✓ 違反時のリスク: 行政責任 / 民事責任 / 刑事責任

# VIII. Privacy Policyをめぐる世界的動向

## □ 中国版個人情報保護法の評価

- ✓ 欧州のGDPRと内容面では一部類似するものであるが、顧客や従業員の個人情報の国外(本土外)への持ち出しを制限する等、政府によるIT業界への締め付けの意図が伺える内容
- ✓ 中国という国家の特性上、実際の運用状況を見なければ評価が難しい状況
- ✓ そもそも中国の国家体制(共産主義)と「プライバシー」概念は相反関係?
- ✓ 今後制定される施行細則、米国との貿易摩擦を含め、今後の同法の運用動向に注視が必要

⇒ 今般予想されている「デジタル冷戦」の一貫としての活用?



# IX. おわりに

## □ 今後のPrivacy Policy・個人情報／データ保護法制対応

- ✓ 各国・地域の個人情報保護法の「域外適用」問題
  - グローバルな事業展開を行う限り、本国(日本)の個人情報保護法のみを意識したPrivacy Policyでは不十分
  - 自社の事業展開する国・地域でどのような個人情報保護法制が敷かれているかを常に最新の情報として把握し、当該法制度に適合するPrivacy Policyの策定・更新・運用が必要
  - 関連会社間での情報管理についても注意が必要(国・地域別の管理を徹底?)
- ✓ 企業活動におけるデータの重要性が加速度的に高まる中で、旧来の「個人情報」では捕捉できない情報についても保護の必要あり(例: Cookieの保護)

# IX. おわりに

## □ 今後のPrivacy Policy・個人情報／データ保護法制対応

- ✓ 今後、ビッグデータの利用増加を背景に世界中で取り扱われるデータ量は増加の一途を辿ると予想される
  - 各国において(自国の利益保護を志向した)個人情報／データ保護法制が整備されることが予想され、状況が更に複雑化する見込み
  - 米中対立が、両国のデータ保護関連法令／企業のPrivacy Policyをめぐって(両国のデータ関連大企業を巻き込んで)展開されるおそれ
- ✓ 行政機関による関連法令の執行、情報提供者からの訴訟提起といった有事の発生を、税務や労働関連と並ぶ企業のレピュテーション上の重大なリスクとして常に想定し、必要に応じて専門家とも協議のうえ、対応方針の策定や関連法令の遵守に務める必要がある

# IX. おわりに

- 最後に: 当局による摘発を避けるために・・・「**3本柱**」が必要
  - 1) 個人情報保護に関する**対内文書**の整備・運用  
社内規定としてのInformation Security PolicyやDocument Management Policy等の周知徹底
  - 2) 個人情報保護に関する**対外文書**の整備・運用  
対外的なPrivacy Policyの整備・関連法令の注視(本セミナーの主眼)
  - 3) 個人情報保護に関する関係者の「**啓蒙**」  
文書の整備以前に、**(役位を問わず)個人情報を取り扱う企業人それぞれが個人情報保護の肝を理解していることが必要**
    - そのための研修制度やセミナー参加等
- 本日主に取り扱った対外文書以外の2本の柱についても、(目立たないからといって)**怠ってはいけません**！

# ご清聴ありがとうございました

## Questions???



弊社では米国の法律に関わる**最新情報・ウェビナーの案内**等のニュースレターを配信しております。ご希望の方は、上記QRコードまたは柿内のメールアドレス [skakiuchi@sgrlaw.com](mailto:skakiuchi@sgrlaw.com) からお申し込み下さい。