

▶ About us



渥美坂井法律事務所・外国法共同事業は、国内系法律事務所として初めて、完全に独立した形で外国法共同事業を立ち上げた総合法律事務所です。ロンドン、ニューヨーク及びフランクフルトに拠点を有し、国際業務経験豊富な弁護士等が、欧米から中東・アフリカまで約120か国におよぶ広範な海外ネットワークを活用し、国際案件にも適時に対応可能な体制を整えております。提携グループを中心とした様々な内外のプロフェッショナルと協力し、時代とともに複雑化・国際化するニーズに柔軟に対応してシナジーを発揮し、真のワンストップリーガルソリューションを提供いたします。

改正個人情報保護法ニューズレター（2021年9月版）

| Page 1/9 |

2021年9月 A&S_015

はじめに

ご質問（位置情報や体重等のアメリカへの移転について）



私は、スポーツ用品メーカーの法務部員です。現在、お客さまに弊社のアプリと体重計を設定していただき、位置情報、走行距離、消費カロリー、体重など情報を取得して、お客さまにランニングやダイエットのアドバイスをして、弊社の新商品を勧めること、及び新商品を開発することを企画しています。また、弊社は、米国の製菓・食品企業から、一般のランナー向けサプリを開発・販売するための協力要請を受けており、上記の情報を提供するように求められており、情報を提供しようと考えています。

基本的なビジネスプランは以上の通りであり、さらに以下のような点について議論していますので、アドバイスをお願いします。

プランA：データ漏えいの可能性などを考慮し、できるだけ個人情報保護法などの規制の適用を受けたくないので、お客さまから氏名や個人を特定できる情報は取得しない。

プランB：お客さまから、氏名、メールアドレス、怪我の有無・内容、使用中の薬などの情報を得て、商品のPR、新商品開発を強力に進める。ただ、プランBの場合でも、お客さまのプライバシーを考慮して、お客さまの氏名など、個人を特定できる情報については、米国企業に提供しない予定である。

回答項目

1. プランA：個人情報を取得しない場合
 - (1) 熊澤春陽元個人情報保護委員会委員のコメント
 - (2) 個人関連情報の新設（改正法26条の2）
 - (3) 個人関連情報の越境移転に係る規制内容（改正法26条の2第2項・3項）
 - (4) 改正法による域外適用の拡大（改正法75条）
2. プランB：個人情報を取得する場合
 - (1) 第三者提供規制適用の有無（個人情報該当性に関する提供元基準説）
 - (2) 安全管理措置（改正法20条、27条）
 - (3) 要配慮個人情報
 - (4) コメント
3. フィットネスデータの利用について、GDPRの観点からフランクフルト提携オフィスのコメント
4. 改正個人情報保護法の公布から施行までのスケジュール
5. 今後の連載予定

1. プラン A：米国企業と位置情報等を共有する場合の改正個人情報保護法の規制

(1) 令和2年改正による個人関連情報の導入と企業の対応について、熊澤春陽元個人情報保護委員会委員のコメント

ア 個人関連情報に関する考察

「個人情報」という概念をどのように定義し保護するかは、その国のプライバシー風土に深い関わりがあります。宗教的倫理感や国の歴史によって形成された国民性が、個人情報の定義を決定してきたとも言えます。

EUのGDPRは、ナチスやソ連の支配下における人権侵害の歴史が大きな影響を与えており、IPアドレスや行動履歴など幅広い情報を personal data として保護対象に含めています。

一方、米国では、国民の自由な経済活動を優先することを前提としており、行政や業界ごとに保護対象である個人情報が定義され、問題のある個人情報の取り扱いをFTCが監督し、高額な制裁金を課すことにより、事業者の自主的な個人情報保護を促してきました。ただ、近年は、州法等で法規制を強める方向となっています。

我が国の場合、米国と同様に行政や業界単位の規制が中心であり、他方、政府の介入を嫌う国民性もあって高額な制裁金を課する仕組みを導入することはできませんでした。個人情報の定義については、個人情報保護法の成立を契機として、定義を明確化するための整理が進められてきました。今回の改正では、新たに「個人関連情報」を定義することにより、これまで課題となってきたインターネット上の情報等に対して、より情報主体の関与を必要とするようになりました。

イ 法改正の経緯

インターネット上の行動履歴などの取り扱いに関しては、2015年の法改正に際しても重要な論点とされ議論されてきたところ、最終的には個人情報保護と活用の両立が日本経済の活性化に資するという法の目的に沿う考え方によって抑制的な形となりました。

すなわち、cookie等の端末IDの情報に関して単体では個人情報とせず、何らかの方法によって個人と特定されうる場合に「個人情報」として取扱うと整理されました。

今回の2020年の法改正においても、消費者と事業者双方のヒヤリングを通じて、基本的な定義に関しては変更しない方向となりましたが、cookie情報の第三者提供先での個人情報との紐付け等については明確な法の規定が必要となり、その点については規制が盛り込まれることとなりました。同時に、個人情報関連を定義づけることによって、取扱事業者の注意喚起と自主的な規制を促す方向となりました。

ウ 今後企業に望まれる対応

DX等データドリブンでの企業経営改革が課題となっている中、個人情報の保護と活用は企業の経営課題の大きな要素の一つとなっています。既にAppleやMicrosoftなど多くの先進的企業が幅広いプライバシー保護を単なる規制対応ではなく、むしろ成長戦略と位置付けています。

上述した諸外国を含む法改正の経緯及びデータドリブンが重要とされる経営環境の下では、個人に関する情報の取扱いが適法かどうかというだけでなく、個人に関する情報の保護は、顧客や社会に対する義務として事業者がとらえる必要があります。

すなわち、パーソナルデータを事業資産として活用し、自社のサービス・製品開発の源泉として企業価値の向上を目指す一方、個人関連情報も含めた個人に関する情報全体の取り扱いについて透明性と説明責任を持ってあたることがコーポレートガバナンス上の重要な課題といえます。そして、日本企業にもそれが成長戦略に繋がると捉えていただきたいと考えております。

(2) 個人関連情報の新設（改正法26条の2）^[1]

改正法26条の2第1項は、個人関連情報について、以下の通り規定しています。

法第26条の2（第1項）

- 1 個人関連情報取扱事業者・・・は、第三者が個人関連情報を個人データとして取得することが想定されるときは、第23条第1項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ個人情報保護委員会規則で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。
- 一・・・本人の同意・・・
 - 二（略）

[1] このニューズレターは、令和2年改正による条文番号を前提としており、令和3年改正による条文番号を前提としていません。令和3年改正による条文番号につきましては、以下のウェブサイトをご参照ください。

https://www.ppc.go.jp/files/pdf/hogohou_50joukaisei.pdf
(デジタル社会形成整備法第50条による個人情報保護法の改正)
https://www.ppc.go.jp/files/pdf/hogohou_51joukaisei.pdf
(デジタル社会形成整備法第51条による個人情報保護法の改正)

ア 個人関連情報の意義^[2]

「個人関連情報」とは、生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいいます。

「個人に関する情報」とは、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報です。「個人に関する情報」のうち、氏名、生年月日その他の記述等により特定の個人を識別することができるものは、個人情報に該当するため、個人関連情報には該当しません。例えば、一般的に、ある個人の位置情報それ自体のみでは個人情報には該当しませんが、個人に関する位置情報が連続的に蓄積される等して特定の個人を識別することができる場合には、個人情報に該当し、個人関連情報には該当しないこととなります。また、統計情報は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当するものではないため、個人関連情報にも該当しません。

個人関連情報に該当する情報として、例えば、以下の情報が挙げられます。

- Cookie等の端末識別子を通じて収集された、ある個人のウェブサイト閲覧履歴
- メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等
- ある個人の商品購買履歴・サービス利用履歴
- ある個人の位置情報
- ある個人の興味・関心を示す情報

プランAにおいて、貴社が取得・利用を予定している位置情報などは、お客さまに関する情報ですが、その情報からは特定のお客さまを識別できませんので、貴社が提供する情報は個人情報には該当せず、個人関連情報に該当します。

イ 個人関連情報を第三者へ提供する場合の同意の要否

改正法26条の2の規定により、ある企業が、個人を識別できない情報を、別の企業に提供し、その別の企業が、個人を識別できる形で利用することが想定される場合（「第三者が個人関連情報を個人データとして取得することが想定される時」）、本人の同意を得る必要があります。

この点、提供元の個人関連情報取扱事業者と提供先の第三者との間の契約において「提供先の第三者は、提供を受けた個人関連情報を個人データとして利用しない」と規定されている場合、通常、「個人データとして取得することが想定され」ず、法第26条の2は適用されません。^[3]

プランAの趣旨は、個人情報保護法などの規制をできるだけ受けたくないというものですので、プランAを選択する場合、

貴社としては、可能な限り改正法26条の2が適用されないことを希望していると思われます。そのための方法として、貴社と米国企業との間の契約書により、「米国企業が、貴社から提供される情報を個人データとして利用しないこと」を義務づけ、米国企業が「個人データとして取得することが想定され」ないとする方法が考えられます。

ウ 米国企業が独自に取得した情報が貴社と共有される場合

改正Q&A^[4] 8-9は、以下の通り規定しています。

個人データの取扱いの委託に伴って委託元が提供した個人データが、委託先にとって個人データに該当せず、個人関連情報に該当する場合において、委託先が委託された業務の範囲内で委託元に当該データを返す行為については、法第26条の2第1項は適用されません。

ただし、委託先が、委託先で独自に取得した個人関連情報を当該データに付加し、その付加後の当該データを委託元に返す場合には、法第26条の2第1項が適用されます。

上記の改正Q&Aの「委託」とは異なり、設問の事例は第三者提供に該当すると思われますが、上記の改正Q&Aは設問の事例を検討する上でも参考になります。すなわち、上記の改正Q&Aのただし書きによれば、プランAにおいて、米国企業が、その独自に取得した情報（各個人のデータとサブリのとの相性など）を貴社と共有する場合、米国企業に個人情報保護法が域外適用されることを前提として（下記「(3)」を参照）、改正法26条の2第1項が適用されます。

他方、米国企業がサブリの購入者の氏名・購入履歴をなどの個人を識別できる情報を貴社と共有する場合（これは、プランAの趣旨に反するように思われますが）、個人データの第三者提供・越境移転の規制が適用されることとなると思われます。

[2] 改正ガイドライン（通則編）3-7-1-1

https://www.ppc.go.jp/files/pdf/210802_guidelines01.pdf

[3] 改正ガイドライン（通則編）3-7-2-3

[4] https://www.ppc.go.jp/files/pdf/2109_APPI_QA_4ejj3t.pdf

エ 「本人の同意」を取得する主体

「本人の同意」を取得する主体は、本人と接点を持ち、情報を利用する主体となる提供先の第三者とされていますが、提供元の個人関連取扱事業者が代行することも認められます。

どちらの場合であっても、個人関連情報の提供を受けて個人データとして取得する主体、対象となる個人関連情報の項目、個人関連情報の提供を受けて個人データとして取得した後の利用目的等について、本人が認識できるようにする必要があります（改正ガイドライン（通則編）3-7-3-2）。

オ 第三者提供に係る記録作成・保存義務

改正法 26 条の 2 第 3 項によると、個人関連情報取扱事業者は、本人の同意の取得に関する確認を行ったときは、当該個人関連情報を提供した年月日、当該確認に係る事項等に関する記録を作成するとともに、これを一定期間保存しなければなりません。

もっとも、個人関連情報取扱事業者が、本人に対する物品又は役務の提供に係る契約を締結し、かかる契約の履行に伴って、当該本人に係る個人関連情報を当該個人関連情報取扱事業者から第三者に提供する場合、当該契約書その他の書面をもって記録とすることができます（改正ガイドライン（通則編）3-7-5-2-3）。

(3) 個人関連情報の越境移転に係る規制内容（改正法 26 条の 2 第 2 項・3 項）

法第 26 条の 2（第 1 項）

1 個人関連情報取扱事業者・・・は、第三者が個人関連情報を個人データとして取得することが想定されるときは、第 23 条第 1 項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ個人情報保護委員会規則で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。

(1)（略）

(2) 外国にある第三者への提供にあつては、前号の本人の同意を得ようとする場合において、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報が当該本人に提供されていること。

2 第 24 条第 3 項の規定は、前項の規定により個人関連情報取扱事業者が個人関連情報を提供する場合について準用する。この場合において、同条第 3 項中「講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供し」とあるのは、「講じ」と読み替えるものとする。

規則第 11 条の 3（第 1 項・第 2 項）

1 法第 24 条第 2 項又は法第 26 条の 2 第 1 項第 2 号の規定により情報を提供する方法は、電磁的記録の提供による方法、書面の交付による方法その他の適切な方法とする。

2 法第 24 条第 2 項又は法第 26 条の 2 第 1 項第 2 号の規定による情報の提供は、次に掲げる事項について行うものとする。

- (1) 当該外国の名称
- (2) 適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報
- (3) 当該第三者が講ずる個人情報の保護のための措置に関する情報

規則第 11 条の 4（第 1 項）

1 法第 24 条第 3 項（法第 26 条の 2 第 2 項において読み替えて準用する場合を含む。）の規定による外国にある第三者による相当措置の継続的な実施を確保するために必要な措置は、次に掲げる措置とする。

- (1) 当該第三者による相当措置の実施状況並びに当該相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容を、適切かつ合理的な方法により、定期的に確認すること。
- (2) 当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データ（法第 26 条の 2 第 2 項において読み替えて準用する場合にあつては、個人関連情報）の当該第三者への提供を停止すること。

個人関連情報取扱事業者は、個人関連情報の提供先が外国にある第三者であり、本人の同意を得る方法により越境移転させる場合、当該同意を得ようとする時点において、改正規則 11 条の 3 第 2 項各号の情報を提供する必要があります。

この点、「個人データ」の国外移転の場合と同様に海外の制度の情報提供が課題となるところ、改正 Q&A において、「施行規則 11 条の 3 第 2 項から第 4 項までの規定により求められる情報が掲載された Web ページが存在する場合に、当該 Web ページの URL を自社のホームページに掲載し、当該 URL に掲載された情報を本人に閲覧させる方法」も認められるとされています（改正 Q&A12-10）。

また、個人情報保護委員会は、2021 年 9 月 17 日に「年内を目途に、調査対象とする国又は地域の個人情報の保護に関する制度と我が国の個人情報保護法との間の本質的な差異の把握に資する一定の情報を公表する予定」と公表しました。^[5]

[5] https://www.ppc.go.jp/files/pdf/210917_pp_offshore_kouhyou_sywqkc.pdf

実務的には、海外の制度の情報提供については、この個人情報保護委員会が公表する Web ページの URL を自社のホームページに掲載する方式を採用することが多くなると予想されます。

ただし、データの提供先である海外の会社が「講ずる個人情報の保護のための措置に関する情報」（施行規則 11 条の 3 第 1 項第 3 号）や「相当措置の実施」（施行規則 11 条の 4 第 1 項 1 号）については、その URL を掲載するだけでは不足することとなります。特に「相当措置の実施状況」（施行規則 11 条の 4 第 1 項 1 号）については、「定期的な確認」が必要とされていますので、データの提供先である海外の会社との契約により、海外の会社から情報提供を受けることを規定しておく必要があります。

(4) 改正による域外適用の拡大（改正法 75 条）

令和 2 年改正により、個人情報保護法の域外適用の範囲が拡大されました（改正法 75 条）。改正前においては、域外適用が認められる外国の事業者は、国内にある者に対する物品又は役務の提供に関連して、その者を本人とする個人情報等を本人から直接取得した場合に限られると解釈されていましたが、令和 2 年改正により、条文上、国内にある者の個人情報等の取扱いが、国内にある者に対する物品又は役務の提供に関連していれば足りることが明らかにされ、外国の事業者が、個人情報等を本人から直接ではなく、間接的に取得した場合であっても、域外適用が認められるようになりました（改正ガイドライン（通則編）5-1 の事例 3、事例 4 及び改正 Q&A11-4）。

また、令和 2 年改正前においては、域外適用される個人情報保護法上の規定が限定列挙されており、報告及び立入検査並びに命令に係る規定（法 40 条、法 42 条 2 項及び 3 項）は対象外とされていましたが、令和 2 年改正により、それらの規定が適用されることとなりました。

域外適用の範囲が拡大された結果、日本企業が、外国企業に対して、日本国内にある者の個人情報等の取扱いを委託等した場合には、当該外国企業は、当該日本企業との契約上の義務を遵守するのみならず、法文上は、個人情報保護法上の規定を遵守する必要があります。^[6]

プラン A では、米国企業は、ランナー向けのサブリース・販売のために、貴社から位置情報等の提供を受けます。その米国企業は日本のランナーへのサブリースを企図していると思われるので、「国内にある者に対する物品の提供に関連して」、個人関連情報の提供を受けるといえます。したがって、改正法 75 条により、当該米国企業は、法文上、個人情報保護法上の義務を遵守することが必要になります。^[7]

2. プラン B：個人情報を取得する場合

プラン B については、当然、個人情報保護法の適用があります。特に以下の点にご注意ください。

(1) 第三者提供規制適用の有無（個人情報該当性に関する提供元基準説）

ア 問題点（提供元と提供先が取得する情報の違い）

プラン B では、貴社はお客さまから氏名等の提供を受けるので、貴社は容易に特定のお客さまを識別することができますようになります。

他方、個人を特定できる情報については、米国企業に提供しない予定とのことですので、米国企業は貴社のお客さまを識別することはできません。この場合に、改正法 23 条 1 項（第三者提供規制）が適用されるのかどうか問題となります。

イ 提供元基準説

この点に関し、以前は、改正法 23 条 1 項に基づき個人データを第三者に提供する際に、容易に特定の個人を識別することができるかどうかについて、提供元の事業者を基準に判断する説（提供元基準説）と、提供先の事業者を基準に判断する説（提供先基準説）との間で争いがありました。現在では、提供元基準説が非常に有力^[8]とされています。

ウ 設問の場合

提供元基準説を前提とした場合、貴社は、容易に特定のお客さまを識別することができるので、貴社が米国企業に提供するデータは個人データとみなされ、第三者提供規制が適用されることとなります。

すなわち、貴社は、原則として、本人から同意を得る必要があります。このことから、第三者提供規制に関しては、プラン B よりプラン A の方が軽度なものとなるといえます。

提供先基準説を前提とした場合、貴社から米国企業へのデータの提供について第三者提供規制は適用されません。ただ、このように第三者提供規制の適用を避けるべく提供先基準説を採用することは、現状ではお勧めできません。

[6] 実務的には、外国企業に日本の個人情報保護法を遵守させることが容易ではないケースも少なくないと思われます。

[7] なお、設例の米国企業は、米国連邦法及び州法を遵守する必要があることは当然です。

[8] <https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000151056> (No.19 の回答参照)

2021年9月A&S_015

(2) 安全管理措置（改正法 20 条、27 条）

ア プラン A とプラン B の違い（安全管理措置の規定の適用の有無）

プラン B の場合、貴社は「個人情報取扱事業者」に該当するので、個人データについて安全管理措置を講じなければなりません（改正法 20 条）。

他方、プラン A の場合、貴社は個人関連情報のみを取得し、「個人情報取扱事業者」に該当しないので、安全管理措置に関する義務を負いません。これは、個人関連情報取扱事業者に対する規制は必要最低限のものとされたため、安全管理措置の義務は課されないこととされたためです^[9]。

イ プライバシーポリシー上の安全管理措置に関する記載

改正により、保有個人データについて、その安全管理措置の内容を本人の知り得る状態に置かなければならないとされました（改正法 27 条 1 項 4 号、改正施行令 8 条 1 号）。改正ガイドラインに、「安全管理のために講じた措置として本人の知り得る状態に置く内容の事例」が記載されており^[10]、実務的にはこの改正ガイドラインの記載を参考としてプライバシーポリシーの記載を検討することとなると思われます。

改正ガイドラインは、「基本方針の策定」、「個人データの取扱いに係る規律の整備」、「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」、「外的環境の把握」に関して、プライバシーポリシーに記載することの検討を求めています。これは、事業者にとって大きな負担となるようにも思います。この点、法が求める「本人の知り得る状態」については、「本人の求めに応じて遅滞なく回答する場合を含む」と規定されているため、講じた措置の概要や一部をホームページに掲載し、残りを本人の求めに応じて遅滞なく回答を行うといった対応も可能です。実務上、どこまでをプライバシーポリシーに記載すべきか検討が必要になります。^[11]

プラン B では、怪我や薬に関する要配慮個人情報を取得する可能性が高いので、具体的な安全管理措置の記載について、積極的な検討が必要となると思われます。

ウ 外国の委託先や外国のサーバと安全管理措置の記載

改正 Q&A によれば、外国の業者に個人データの取扱いを委託した場合や外国にあるサーバに個人データを保存した場合、①外国の個人情報の保護に関する制度等を把握した上で、委託先の監督その他の安全管理措置を講じる必要があり、②外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要があります（改正 Q&A10-24、10-25）。

貴社が外国の企業に個人データを委託していたり、外国にあるサーバに個人データを保存している場合、上記①及び②に対応する必要があります。

エ 以上のことから、安全管理措置に関する規制は、プラン B よりプラン A の方が軽度といえます。^[12]

(3) 要配慮個人情報該当性

「要配慮個人情報」とは、個人情報の中でも「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」をいい（改正法 2 条 3 項）、①身体等の障害、②健康診断等の結果、③診療情報・調剤情報、④刑事事件の手術が行われたこと、⑤少年法の保護手続が行われたことが政令で定められています。

貴社が、お客さまのランニング状況改善に向けたアドバイス等を行うにあたり、お客さまから怪我の診断結果等に関する情報を取得する場合、「要配慮個人情報」を取得することとなります。^[13] その取得・提供に際して事前の同意を取得し、漏えい時の報告義務（改正法 22 条の 2、施行規則 6 条の 2 第 1 号）に注意するなど、慎重な対応・管理が必要です。

「要配慮個人情報」を取得する場合、プラン B に課される規制は、プラン A に課される規制より相当重いものとなるといえます。

(4) コメント

以上の通り、プラン B に課される規制は、プラン A に課される規制より重いものであり、プラン A は規制対応コストという観点からは魅力的に思えます。ただし、高い価値のサービスを提供するためには、プラン B を選択する必要があるかもしれません。プラン B を選択される場合、クオリティの観点から、貴社のプライバシー保護が十分であることをストレスなくお客さまに理解していただく方法もご検討ください。

[9] 佐脇紀代志「一問一答 令和 2 年改正個人情報保護法」p63

[10] 改正ガイドライン（通則編）3-8-1、p110

[11] なお、単に「個人情報の保護に関する法律についてのガイドライン（通則編）に沿って安全管理措置を実施している」という記載のみでは不適切とされている点にご留意ください（改正ガイドライン（通則編）3-8-1）。

[12] 他にも、利用目的などの規制も個人関連情報取扱事業者には適用されません。これは、上述した通り、個人関連情報取扱事業者に対する規制は必要最低限のものとされたためです。このことからプラン B よりプラン A の場合に課される規制の方が軽度といえます。

[13] 他方、体重は体調に関係する重要な情報ですが、直ちに「要配慮個人情報」に該当することはありません。

3. フィットネスデータの利用について、GDPR の観点からフランクフルト提携オフィスのコメント

The General Data Protection Regulation (GDPR) contains in Article 9 strict requirements for the “processing of special categories of personal data”. This is due to the special nature of such data and the associated increased risk to the data subjects.

Article 9 para (1) GDPR specifically mentions “data concerning health” as one category of special types of personal data, also commonly referred to as sensitive data. "Sensitive" data is any data that directly or indirectly conveys information about the categories of data specified in Article 9 para (1) GDPR.

On the one hand, health data includes direct information about a person's health, such as disease diagnoses, disabilities or alcohol or drug abuse. However, in order to effectively protect data subjects, health data must be interpreted broadly. Therefore, it comprises not only data that directly relates to a disease, but also includes for example a data subject's physical condition in general which also allows to draw conclusions about the state of health (so-called “indirect” health data).

Such indirect health data (in our above example including e.g. location, distance traveled, calories burned, weight) can be used to draw conclusions about the health of the person concerned if they go beyond a mere snapshot. This is in particular the case, if such data is stored over a longer period and/or combined with other data.

The above assessment entails several duties for our sporting goods manufacturer in connection with the planned App. The requirement under Article 6 (3) in connection with Article 13 para (1) lit. c) GDPR to specify a precise purpose means that if the provider of the App, which is our sporting goods manufacturer as controller, also stores health-related data, this must be stated in the privacy policy for the App users. The provider must specifically name the data that is collected.

Irrespective of the duty to provide information about the processing (which is done by the relevant privacy policy), the special requirements under Article 9 GDPR apply to the processing of this indirect health data, the collection or other processing which is only permissible if the data subject has explicitly consented to or the law permits it (as set forth in more detail in Article 9 para (2) GDPR).

As the App in our case is not used for medical reasons (also the potential cooperation with a food supplement manufacturer, does not make this a medical necessity), the health data collected is not necessary to protect vital interests of the data subject or a third party (Article 9 para (2) lit (c)). Nor is it data that the data subject has manifestly made public ((Article 9 para (2) lit (e)). The intended cooperation with the food supplement manufacturer, is not to be considered somehow in the public “health” interest). The other exceptions mentioned in Article 9 para (2) are also not relevant.

Accordingly, the App providers must obtain consent for the collection and use of health data from the App users. Regardless of the question of whether consent to the privacy policy can constitute such consent, the consent must meet the strict requirements of Articles 4 para (11) and 7 GDPR.^[14] In particular the consent must be based on the free decision of the data subject and explicitly refer to the specific types of personal data collected and used. Furthermore, the data subject must be able to identify beyond doubt which sensitive data is to be collected, processed and used, for which precisely defined purpose, and in which context of use.

The App provider's duty to provide information within the scope of the data protection declarations includes informing the user about where his or her personal data is processed. However, data transfer to a third country outside the EU - as described in our above example - is according to Art 44 GDPR only permissible, if an exemption for such international data transfer applies. This can be for example a “transfers on the basis of an adequacy decision” as set forth in Article 45 GDPR, by which adequacy decision the EU Commission acknowledges that the level of data protection in the destination country is adequate within the meaning of Article 45 GDPR.

If no other exceptions apply, the transfer is mostly made by using the EU standard contractual clauses (SCCs) or the so-called "Binding Corporate Rules" (BCR).

In our example a data transfer to the US was often based on the so called “Privacy Shield” . However, in July 2020, the European Court of Justice (ECJ) has ruled that the EU-US Privacy Shield is not an appropriate basis for data transfers to the US.^[15] Standard contractual clauses can in principle continue to be used, but must - as before - be reviewed by users and supervisory authorities on a case-by-case basis.

4. 改正個人情報保護法の公布から施行までのスケジュール

令和2年・令和3年改正個人情報保護法の公布から施行までのスケジュールは、以下の通りです。

令和2年6月12日	令和2年改正法公布
令和3年3月24日	政令・規則公布
令和3年5月19日	令和3年改正法（デジタル社会の形成を図るための関係法律の整備に関する法律）公布
令和3年8月2日	ガイドラインを公表
令和3年9月10日	Q&Aを公表
令和4年4月1日	令和2年改正法施行

5. 今後の連載予定

今後、「データと内部統制・ガバナンス」、「中国法」、「韓国法」、「ベトナム法」、「台湾法」、「医療製薬ヘルスケア分野」、「金融分野」をテーマとするニュースレターを連載する予定です。

[14] Article 4 para (11) defines consent as follows: "Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

The GDPR further clarifies the conditions for consent in Article 7:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

[15] C-311/18 "Schrems II" - <https://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=EN&occ=first%C3%A2%C2%88%C2%82%3D1&mode=DOC&pageIndex=0&cid=1925369>

The ruling invalidates a decision of the European Commission concerning the EU-US Privacy Shield (adequacy decision). Anyone wishing to transfer data to the USA under the General Data Protection Regulation (GDPR) can therefore no longer rely on this adequacy decision, but must use other legal instruments for this purpose. There is no transitional period during which the Privacy Shield can still be used in the sense of the GDPR. The ruling has also confirmed as lawful decisions of the European Commission concerning standard contract clauses. From such standard contractual clauses, in principle, the necessary safeguards can exist, which are provided for data transfers to countries outside the EU and the European Economic Area (standard data protection clauses, Article 46(2)(c) of the GDPR). However, the users of these clauses must check for themselves whether these guarantees are sufficient or need to be supplemented by further measures - especially if poor data protection conditions prevail in the destination country. A data exporter that already uses standard contractual clauses has thus committed to suspend the data transfer if the clauses are not complied with in the destination country, or at least to inform the competent supervisory authority. If such clauses are not sufficient and no appropriate additional measures have been taken in this respect, the data protection authorities can order that the transfer be suspended.

他プラクティスグループのニュースレターも配信しております。
配信を希望される方は下記メールアドレス宛にご連絡ください。
マーケティング・PR部門宛 prcorestaff@aplaw.jp

※お名前、部署、役職をご明記ください。
また、右記の一覧よりご興味ある分野をお選びください。

【日本語】

- ジェネラル／様々な分野の旬な法律トピックス
- ベトナムビジネス
- インドビジネス
- ロシアビジネス
- 再生可能エネルギー
- 農林水産
- イノベーション／テクノロジー
- その他（ご興味のある分野をご教示ください。）

【英語】

- ジェネラル／様々な分野の旬な法律トピックス

執筆者

渥美坂井法律事務所・外国法共同事業

〒100-0011 東京都千代田区内幸町2-2-2富国生命ビル (総合受付: 16階)



弁護士 松岡 史朗

パートナー / 第一東京弁護士会

E: fumiaki.matsuoka@aplaw.jp

> [View Profile](#)



熊澤 春陽*

顧問

* 弁護士資格はない (法律事務の取扱い・周施はしていない)

> [View Profile](#)



弁護士 平岡 亜紀子

アソシエイト / 第一東京弁護士会

E: akiko.hiraoka@aplaw.jp

> [View Profile](#)



弁護士 鈴木 陽一

アソシエイト / 東京弁護士会

E: yoichi.suzuki@aplaw.jp

> [View Profile](#)



弁護士 福原 聡

アソシエイト / 第二東京弁護士会

E: satoshi.fukuhara@aplaw.jp

> [View Profile](#)

フランクフルト提携オフィス

(Atsumi Sakai Janssen Rechtsanwalts- und Steuerberatungsgesellschaft mbH**)

OpfernTurm (13th Floor), Bockenheimer Landstraße 2-4, 60306
Frankfurt am Main, Germany



ドイツ連邦共和国弁護士*** フランク・ベッカー

パートナー

E: frank.becker@aplaw.de

> [View Profile](#)

** ドイツ連邦共和国における弁護士・税理士法人

*** 但し、日本における外国法事務弁護士の登録はない。

お問い合わせ先

渥美坂井法律事務所・外国法共同事業

E: info@aplaw.jp

このニュースレターに掲載されている情報は、法的アドバイスを構成するものではありません。弊所は質の高い情報を提供しよう努めておりますが、このニュースレターのすべての情報は「現状のまま」提供されており、完全性、正確性、適時性、またはこれらの情報を使用して得られた結果を一切保証するものではありません。また、明示、黙示を問わず、性能、商品性、特定目的への適合性の保証を含むがこれに限定されるものではない、いかなる種類の保証もありません。