

個人情報保護法改正2022直前チェックポイント

弁護士 水町雅子

※中央経済社「旬刊経理情報」2月20日号通巻No. 1636「改正個人情報保護法の最終チェック」の元原稿です。https://www.keirijouhou.jp/bn_new/1636.html

※筆者作成のパワーポイント版の詳細資料もあります。

<http://www.miyauchi-law.com/f/200325pii2020kaiseigaiyou.pdf>

※筆者の見解であって、当局見解とは異なる可能性もありますので、ご利用に際しては必ず法律・ガイドライン等の原本に当たってくださいませよう、お願いいたします。

【要約】

・改正個人情報保護法が2022年4月1日に施行される。

・社内規程・プライバシーポリシー・契約書等の改訂、社内フローや運用の変更、従業者教育等の対応が必要。

改正個人情報保護法の原則的な施行日は2022年4月1日と、改正法の施行が近づいているため、本稿では改正概要とともに、民間企業におけるチェックポイントについて述べてゆく。

個人情報保護法は平成15年に制定されてからしばらく法改正が行われてこなかったが、昨今の情勢を受け、近年頻繁に法改正や関連新法の制定が行われている。そして今般、個人情報保護法について令和2年法改正と令和3年法改正が成立し、同時期に施行されるという非常にわかりづらい状況が生じている。個人情報保護法改正関連の資料を確認する際は、令和2年法改正に関するものなのか、令和3年法改正に関するものなのかをよく確認する必要がある。

とはいえ民間企業に大きな影響を与える改正は令和2年法改正であり、令和3年法改正が関係する民間企業は医療・研究・公的機関と関係がある企業に限られるため、多くの企業にとっては令和2年法改正への対応のみ考えればよく、令和3年法改正は法の条文番号が変わる程度の影響しかないだろう。そこで本稿も令和2年法改正について述べていくこととした。

令和2年法改正は、以下に大別される。

1. 外国提供（越境移転）時の情報提供・提供先確認等の義務
2. 安全管理措置・プロファイリング等の公表等
3. 漏えい時等の当局報告・本人通知
4. 本人権利の強化（開示・訂正・利用停止等）
5. 個人データの提供/受領記録の開示義務
6. 個人関連情報規制の新設
7. オプトアウト規制強化
8. その他規制強化（不適正利用の禁止、罰則等の強化、域外適用）
9. 個人情報の利活用促進（仮名加工情報、公益目的、利活用相談）

このうち、特に1. 海外提供（越境移転）関連、2. 安全管理措置（・プロファイリング）等の公表等の対応が、企業にとって負荷が高いと考えられるため、これらを重点的に解説する。また該当する企業にとっては、6. 個人関連情報規制の新設、7. オプトアウト規制、5. 第三者提供記録の開示義務も非常に影響が大きい。

第1章 外国提供（越境移転）時の情報提供・提供先確認等の義務

【要約】

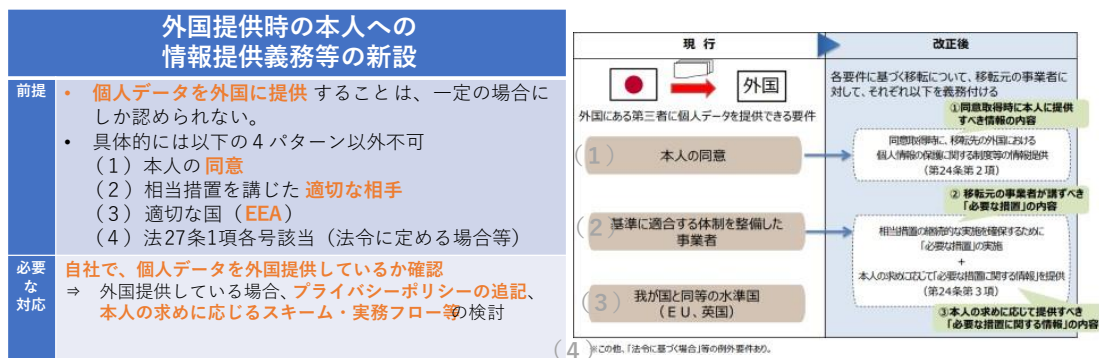
- ・外国に個人データを提供している場合は、対応負荷が高いので速やかな対応が必要。
- ・まず実態の洗い出しを行い、法的スキームごとに対応を検討する。本人同意スキームでは、外国の国名、外国の個人情報保護法制、提供先の個人情報保護措置について、あらかじめの情報提供が必要。本人同意を得ないスキームでも、EEAに提供したり法令に基づくとき等では令和2年法改正対応は必須ではないが、そうでなければ提供先と適切な契約を締結するなどして、契約の履行状況等を年1回以上確認し、同確認の頻度・方法、提供先の個人情報保護措置、外国の国名等について本人の求めに応じての情報提供が必要となる。
- ・現状、外国提供がない場合でも、今後、外国提供規制を知らずに提供してしまうことがないよう、教育・規程類の整備も必要だ。

1. 法改正概要

個人データの外国提供時の規制が強化され、本人への情報提供・提供先確認等の義務が新たに生じる。個人データを外国に提供できる場合は、（１）本人同意を得る場合、（２）提供先と適切な契約を締結するなどして相当措置を講ずる者に本人同意なく提供する場合、（３）EEA（欧州経済領域）に提供する場合、（４）法令に基づく場合等の法27条1項各号に該当する場合にこれまでも限定されてきた（法28条1項、図表1参照）。法律は国内で適用されるのが原則であり、個人データが外国に行ってしまうと、外国では個人情報保護法制が存在しない場合もあるし、法制が存在していたとしても保護レベルが弱い場合もありうる。そこで、日本相当の個人情報保護を行うために、外国に個人データを提供できる場合は制限されている。

図表1 外国提供（越境移転）できる場合

外国提供(越境移転)できる場合



https://www.ppc.go.jp/files/pdf/201104_shiryuu-2.pdfをもとに筆者修正。
条文番号は24条ではなく28条となる。

令和2年法改正では、この規制が強化された。どのような場合に個人データを外国に提供できるかについては、令和2年法改正後も変更はないものの、具体的に外国ではどのような個人情報保護法制が存在するのかや、提供先ではどのような個人情報保護措置を講じるのかなどについて、本人に情報提供しなければならなくなった。情報提供の方法は特段指定されていないが、メール、書面交付、Webサイト掲載等様々な方法がありうる。令和2年法改正対応として必要となる事項は、上記（１）（２）（３）（４）の場合ごとに異なるため、以下それぞれについて詳述する。

なお、外国法人に個人データを提供する場合であっても、外国提供規制が適用されない場合もある。それは、提供先が外国法人であっても、提供先に日本の個人情報保護法が適用されるとき、すなわち提供先が「個人情報取扱事業者」であるときである。この場合は、外国提供規制が適用されないため、本改正対応も不要である。外国の法令に準拠して設立され外国に住所を有する外国法人であっても、日本国内に事務所を設置している場合又は日本国内で事業活動を行っている場合など、日本国内で「個人情報データベース等」を事業の用に供していると認められるときは、当該外国法人は「個人情報取扱事業者」に該当するため、外国提供には該当しない¹。但し、日本国内における事業の実態を勘案して、個別の事例ごとに判断することとなるため、日本国内に出張所を有することのみをもって直ちに「外国にある第三者」に該当しないわけではない²。

（１）本人同意を得る場合

個人データを外国提供するに際して本人同意が得られれば適法なわけであるが、本人としては外国で自己の個人データがどのように取り扱われるか把握した上で同意しているわけではない可能性がある。そこで令和2年法改正では、（１）本人同意を得て外国提供する場合に、①外国の国名、②外国の個人情報保護制度、③提供先の個人情報保護措置について予め本人に情報提供する義務が新たに課せられることとなった（法28条2項）。

図表2 （１）本人同意を得る場合に必要な対応

¹ ガイドライン外国第三者提供編2-2

² 「個人情報の保護に関する法律についてのガイドラインに関するQ&A」平成29年2月16日（令和3年9月10日更新）（以下、「Q&A」という。）12-5

(1) 本人同意を得る場合に必要な対応

- **あらかじめ、本人に情報提供要**（個人情報保護法28条2項、31条1項2号、規則17条2～4項）
 - ✓ ア) 外国の国名、イ) 外国の個人情報保護制度、ウ) 提供先の個人情報保護措置を情報提供
- ア) 外国の国名
 - ✓ 特定できないときは、**特定できない旨・理由、参考情報**（外国の範囲（ヨーロッパ）など）を提供要
 - ✓ 事後的に外国が特定できた場合には、本人の求めに応じて情報提供を行うことが望ましい
- イ) 外国の個人情報保護制度
 - ✓ i 保護制度の有無
 - ✓ ii 保護水準等に関する客観的な指標となり得る情報（GDPR十分制認定取得、APEC加盟国）→ iiがあればiii不要
 - ✓ iii OECD8原則上の事業者義務・本人権利のうち、認められていないもの
 - ✓ iv 本人の権利利益に重大な影響を及ぼす可能性のある制度の存在（ガバメントアクセス、消去等請求に対応できないおそれがある個人情報の国内保存義務に係る制度等）
- ウ) 提供先の個人情報保護措置
 - OECD8原則上の事業者義務・本人権利のうち、講じていないもの
 - 特定できないときは、**特定できない旨・理由**を提供要。事後的に特定できた場合には、本人の求めに応じて情報提供を行うことが望ましい
- 方法は、書面、メール、HP、口頭等（外国提供ガイドライン41P）

外国委託先その他の外国提供先との契約で、上記の協力義務を課すのが適切（報告内容・方法・頻度も決定）。

①外国の国名

外国の国名は、サーバが所在する外国の名称ではなく、提供先の第三者が所在する外国の名称をいい³、例えばアメリカ、シンガポール、中国などと具体的に情報提供する。国名は必ずしも正式名称でなくてもよいが、どこの国に提供されるのかを本人が合理的に認識できると考えられる名称でなければならない。また州名等までは要求されないが、例えば、州法が主要な規律となっている等、州法に関する情報提供が本人の予測可能性の向上に資する場合には州名まで情報提供することが望ましい⁴。

本人同意を得ようとする時点において国が特定できない場合は、特定できない旨とその理由、そして参考となるべき情報がある場合にはその情報を提供しなければならない（規則17条3項）。例えば、製薬会社が医薬品等の研究開発を行う場合に、治験責任医師等が被験者への説明及び同意取得を行う時点では、最終的にどの国の審査当局等に承認申請するかが未確定であり外国を特定できない場合等がこの例として挙げられる。事後的に提供先の第三者が所在する外国が特定できた場合には、本人の求めに応じて情報提供を行うことが望ましい⁵。

②外国の個人情報保護制度

外国の個人情報保護制度については、日本の個人情報保護法との間の本質的な差異を本人が合理的に認識できる情報でなければならない、具体的には、i 個人情報保護制度の有無、ii 指標となり得る情報の存在、iii OECDプライバシーガイドライン8原則に対応する権利義務の不存在、iv その他本人の権利利益に重大な影響を及ぼす可能性のある制度の存在等について情報提供しなければならない⁶。

³ Q&A12-11

⁴ 個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）平成28年11月（令和3年10月一部改正）（以下、「外国提供ガイドライン」という。）5-2(1)

⁵ 外国提供ガイドライン5-3-1

⁶ 外国提供ガイドライン5-2(2)②

ii 指標となり得る情報とは、GDPR（一般データ保護規則）の十分性認定の取得国であること又はAPECのCBPRシステムの加盟国であることをいう⁷。これがあれば、iii OECDプライバシーガイドライン8原則に対応する権利義務の不存在については情報提供不要である⁸。

iii OECDプライバシーガイドライン8原則に対応する権利義務の不存在とは、OECDプライバシーガイドラインの一部として、プライバシーに関する8つの基本原則をOECDがまとめているが、その8つの原則のうち当該外国の個人情報保護制度では対応されていない事業者側の義務又は本人の権利をいう。具体的には、①収集制限の原則（Collection Limitation Principle）、②データ内容の原則（Data Quality Principle）、③目的明確化の原則（Purpose Specification Principle）、④利用制限の原則（Use Limitation Principle）、⑤安全保護措置の原則（Security Safeguards Principle）、⑥公開の原則（Openness Principle）、⑦個人参加の原則（Individual Participation Principle）、⑧責任の原則（Accountability Principle）をいい、個人データを提供する外国法制のうち、これらに対応していない部分を本人に情報提供することになる⁹。

iv 本人の権利利益に重大な影響を及ぼす可能性のある制度の存在とは、例えばガバメントアクセス（事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度等）の有無、事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度等をいう¹⁰。

③提供先の個人情報保護措置

③提供先の個人情報保護措置は、提供先が講じる個人情報保護措置と日本の個人情報保護法で求められる措置との間の本質的な差異を本人が合理的に認識できる情報でなければならない。具体的には、提供先がOECDプライバシーガイドライン8原則に対応する措置を全て講じている場合には、その旨を本人に情報提供すれば足りる。講じていない場合には、講じていない措置の内容について、本人が合理的に認識できる情報が提供されなければならない¹¹。本人同意を得ようとする時点において提供先の個人情報保護措置について情報提供できない場合は、その旨とその理由を提供しなければならない（規則17条4項）。事後的に当情報提供が可能となった場合には、本人の求めに応じて情報提供を行うことが望ましい¹²。

（２）適切な契約締結などして相当措置を講ずる者に本人同意なく提供する場合

本人同意がなくとも、また後記（３）（４）に該当する場合でなくとも、提供先において適当な個人情報保護措置が講じられれば、外国に個人データを提供することが適法となる。この場合の具体的方法としては、日本の個人情報保護法上の義務と同等の内容（個人情報保

⁷ 外国提供ガイドライン5-2(2)②（イ）、「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）の一部を改正する告示案」に関する意見募集結果（以下「外国提供パブコメ」という。）A. 72

⁸ 外国提供ガイドライン5-2(2)②（イ）

⁹ 外国提供ガイドライン5-2(2)②※2、https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf、https://privacymark.jp/wakaru/kouza/theme5_02.html

¹⁰ 外国提供ガイドライン5-2(2)②（エ）

¹¹ 外国提供ガイドライン5-2(3)

¹² 外国提供ガイドライン5-3-2

護法上では「相当措置」と呼ばれる。)を、契約で提供先に義務付けたり、海外グループ会社の場合は内規で義務付けることなどが考えられる。令和2年法改正前は、契約を締結したり内規で義務付けたりすれば、その後の定期的な確認等は不要であったが、令和2年法改正によって、一度契約や内規で義務付ければ足りるわけではなく、履行状況等の定期的な確認及び支障が生じた場合に措置を講じることが提供元に義務付けられることとなった(法28条3項、規則18条1項)¹³。また加えて、上記(1)本人同意を得る場合に類似する情報提供義務も課せられる(法28条3項、図表3参照)。

図表3 (2) 適切な契約締結などして相当措置を講ずる者に本人同意なく提供する場合に必要な対応

(2) 適切な契約締結などして相当措置を講ずる者に本人同意なく提供する場合に必要な対応

1. **相当措置の継続的な実施確保のための必要な措置を講ずる義務**
(個人情報保護法28条3項、31条3項、施行規則18条1項)。
 ① 以下アイの定期的な確認
 * 外国提供ガイドライン50Pにおいて、年1回以上という頻度が求められている
 ア) 提供先が講じている**相当措置の実施状況**
 イ) 当該措置の実施に影響を及ぼすおそれのあるその国の制度の有無・内容を定期的に確認
 ② 提供先が講じている措置の実施に**支障が出たら対応** 措置の継続的な実施の確保が困難になったら**提供停止**
2. **本人の求めに応じて本人に情報提供要** (個人情報保護法28条3項、31条3項、施行規則18条)。
 ア) 提供先の体制の整備の方法
 イ) 提供先が実施する相当措置の概要
 ウ) 1①の確認の頻度・方法
 エ) 外国の国名
 オ) 提供先の措置の実施に影響を及ぼすおそれのあるその国の制度の有無・その概要
 カ) 提供先による措置の実施に関する**支障の有無・概要**
 キ) **力に関して1②により提供元が行う対応の概要**
 ✓ 但し、情報提供することにより提供元の義務の適正な実施に著しい支障を及ぼすおそれがある場合(例) 同一人からの過剰請求等は、その全部又は一部を提供しないことができる。全部又は一部を提供しないときは、遅滞なく本人のその旨を通知要

外国委託先その他の外国提供先との契約で、上記の協力義務を課するのが適切(報告内容・方法・頻度も決定)。

①相当措置の継続的な実施確保のために必要な措置

定期的に確認しなければならないのは、ア) 提供先による相当措置(個人情報保護措置)の実施状況、イ) 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である。イ) 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とは、例えばガバメントアクセスや、事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度等をいう¹⁴。上記(1)本人同意を得る場合における②外国の個人情報保護制度中のiv 本人の権利利益に重大な影響を及ぼす可能性のある制度と同様である。定期的な確認では年に1回以上確認することが求められ¹⁵、その具体的方法としては現地監査等も考えられるが、必ず監査が求められるわけではなく、書面により契約や内規の履行状況の報告を受ける方法等も認められる¹⁶。提供先において内規等の遵守状

¹³ 個人情報保護法31条1項に基づき「個人関連情報」を提供する際も、契約履行の状況等の定期的な確認及び支障が生じた場合に措置を講じることが提供元に義務付けられることとなった(個人情報保護法31条2項・28条3項)。「個人関連情報」の提供においては、情報提供義務は課せられない。

¹⁴ 外国提供ガイドライン6-1(1)

¹⁵ 外国提供ガイドライン6-1(1)

¹⁶ 外国提供パブコメA144

況に関する内部点検が行われている場合には、当該点検結果を確認する方法でもよいが、この場合に内部点検が適切に行われていることのみを確認するだけでは不適切であり、点検内容等についても確認を行わなければならない¹⁷。

提供先において相当措置の実施に支障が生じたときには、提供元は必要かつ適切な措置を講じなければならない（法28条3項、規則18条1項2号）、例えば提供先が契約違反をして個人データを取り扱っている場合には、是正するよう要請すること¹⁸等が求められる。また相当措置の継続的な実施の確保が困難となったときは、個人データをその提供先へ提供することを停止しなければならない（法28条3項、規則18条1項2号）。例えば、提供先が契約違反をして、提供元が是正要請をしたにもかかわらず、提供先が合理的な期間内にこれを是正しない場合や、提供先において重大な漏えい等が発生した後、同様の漏えい等の発生を防止するための必要かつ適切な再発防止策が講じられていない場合等は、相当措置の継続的な実施の確保が困難となった時に当たると考えられ、提供を停止しなければならない¹⁹。

②本人の求めに応じた情報提供の義務

（２）適切な契約締結などして相当措置を講ずる者に本人同意なく提供する場合における情報提供義務で求められる事項は、（１）本人同意を得る場合とやや異なる。差異の１点目としては、（１）本人同意を得る場合には必ず情報提供しなければならないが、この場合はそうではなく、本人に求められた場合に情報提供する義務が生じる。また差異の２点目は情報提供すべき事項である。この場合に情報提供すべき事項は、ア）提供先による体制の整備方法、イ）提供先が実施する相当措置の概要、ウ）提供元による定期的な確認の頻度及び方法、エ）外国の国名、オ）提供先による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概要、カ）提供先による相当措置の実施に関する支障の有無及びその概要、キ）カの支障に関して提供元が講ずる措置の概要である（法28条3項、規則18条3項）。

ア）提供先による体制の整備方法は、例えば提供先と契約を締結している旨²⁰や、提供先と提供元とで共通に適用されるグループ企業内規による旨などを情報提供する。

イ）提供先が実施する相当措置の概要については、日本の個人情報保護法で事業者が義務付けられている義務と同等の内容を提供先においても実施することになるが、その概要を情報提供する。契約の全内容や全条文が必要なわけではなく²¹、概要が分かれば良いだろう。例えば、委託の範囲を超えた利用の禁止、第三者提供の禁止等の粒度で、法17条から40条の義務の内容を具体的にどのように提供先が果たしていくのかを明らかにする。但し、法17条から40条の全てが必ずしも必要なわけではなく、例えば開示・訂正・利用停止等は提供元にて対応するのであれば、そのような情報提供で良いだろうし、個人関連情報の取扱いがないのであれば、個人関連情報関連の義務については取扱いがないため該当しない旨を明らかにすればよいだろう。

¹⁷ 外国提供パグコメA149に類似の問に対する回答が掲載されている

¹⁸ 外国提供ガイドライン6-1(2)

¹⁹ 外国提供ガイドライン6-1(2)

²⁰ 外国提供ガイドライン6-2-2(1)

²¹ 外国提供ガイドライン6-2-2(2)

ウ) では、提供先による相当措置（個人情報保護措置）の実施状況、そして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の確認の頻度と方法を情報提供する。

エ) 外国の国名は、（１）本人同意を得る場合の①外国の国名と同様である。

オ) 提供先による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概要も、（１）本人同意を得る場合における②外国の個人情報保護制度中のiv 本人の権利利益に重大な影響を及ぼす可能性のある制度とほぼ同様である。

カ) 提供先による相当措置の実施に関する支障の有無及びその概要は、例えば提供先が契約において特定された利用目的の範囲を超えて個人データを取り扱っていた場合はその旨を情報提供する²²。

キ) カの支障に関して提供元が講ずる措置の概要は、速やかな是正要請や削除要請²³など、提供元が講ずる措置を明らかにする。

（３）EEAに提供する場合

EEAには十分な個人情報保護を図る法制のGDPRが適用されるため、EEAへ個人データを提供する場合については、法律上、提供元には特段の対応は求められていない。もっとも、EEAに個人データを提供する場合であっても、提供先に対し契約書で一定の義務は課した方が適切であろう。

（４）法令に基づく場合等の法27条1項各号に該当する場合

法27条1項では、法令に基づく場合や、人の生命、身体又は財産の保護のために必要がある場合で本人の同意を得ることが困難であるとき等に、本人同意なく個人データを第三者提供することを認めている。もっとも、これはあくまで第三者提供が例外的に認められている場合であり、民間企業が法27条1項各号に該当して個人データを提供する場合は稀であると考えられる。この場合も法律上、提供元には特段の対応は求められていない。

2. 実務対応

以上、外国提供規制強化について解説してきたが、外国提供がある場合には令和2年法改正対応として非常に負荷の高い対応を求められる可能性がある。そのため、民間企業における対応としては、まずは自社において個人データの外国提供があるのか否か、ある場合に（１）本人同意を得る場合、（２）提供先と適切な契約を締結するなどして相当措置を講ずる者に本人同意なく提供する場合、（３）EEAに提供する場合、（４）法令に基づく場合等の法27条1項各号に該当する場合のどの法的スキームで、個人データを外国提供するのかを確認する必要がある。

事実確認が終わって、（１）（２）に該当する場合があることがわかれば対応が必要である。（１）（２）の場合とも、外国の個人情報保護法制の確認や提供先の個人情報保護措置の確認などに苦勞する場合も想定されるが、これらは外国提供先との契約で、外国提供先に対し協力義務を課す方法も考えられる。その場合は、外国提供先からの報告内容・方法・頻度も契約上などであらかじめ決定しておいた方が良いでしょう。また、外国の個人情報保護法

²² 外国提供ガイドライン6-2-2（6）

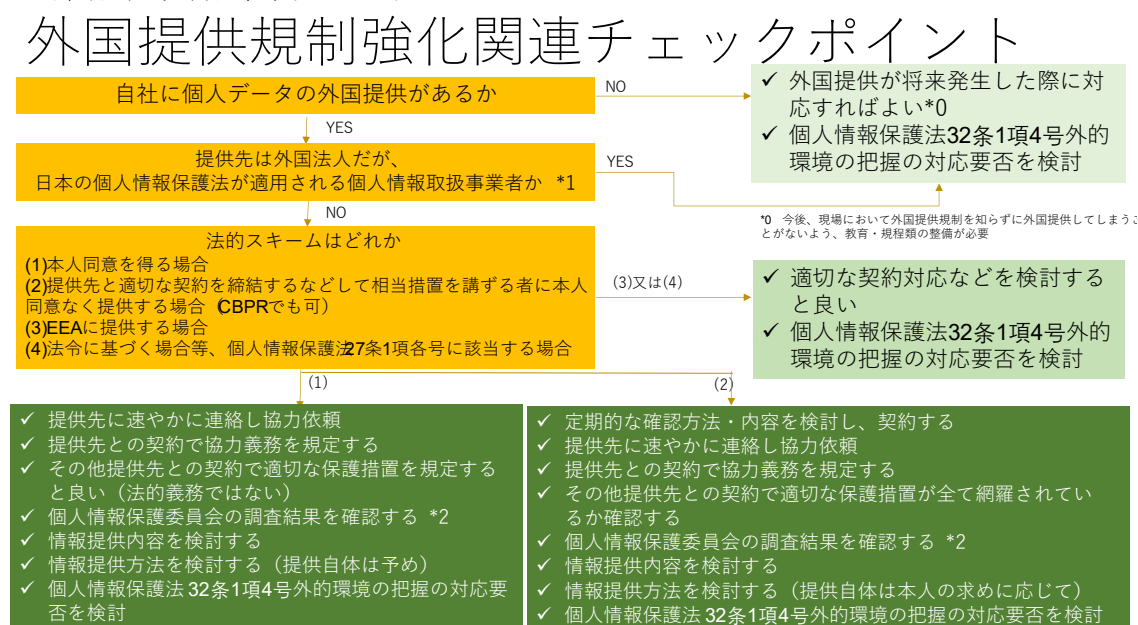
²³ 外国提供ガイドライン6-2-2（7）

制については、事業者が確認するよりも日本の行政当局が確認すべきという意見が多く、これを受け、内閣府の外局である個人情報保護委員会にて調査も行われる。米国、中国、韓国、インド、シンガポールなどの31の国と地域について調査が行われ、調査結果が公表されている²⁴ので、これを必ず確認すると良いだろう。そのうえで、自社としての情報提供内容と情報提供方法を検討し確定していくことが必要だ。

3. チェックポイント

外国提供規制強化について実務対応として実施すべきことを次の図表にまとめたので、参考にされたい。なお、「外国提供が将来発生した際に対応すればよい」というフローに進んだ場合も、今後、現場において外国提供規制を知らずに外国提供してしまうことがないよう、教育・規程類の整備が必要であろう。

図表4 外国提供規制強化関連チェックポイント



*1 日本国内に事務所を設置している場合、又は日本国内で事業活動を行っている場合などで、日本国内で「個人情報データベース等」を事業の用に供していると認められるときは、当該外国法人は、個人情報取扱事業者に該当するため、外国提供にはしない。当該外国法人のWebサイトなどで、個人情報取扱事業者が該当し日本の個人情報保護法を遵守していることが謳われている場合等もある。直ちWebサイトの記載を使用してよいわけではないが、個人情報取扱事業者に該当すれば、法的には外国提供には当たらない。

*2 https://www.ppc.go.jp/files/pdf/210917_pp_offshore_kouhyou_sywkc.pdf

第2章 安全管理措置・プロファイリング等の公表等

【要約】

・プライバシーポリシー等で安全管理措置について公表等する義務が新設。「個人情報保護法に沿って安全管理措置を実施している」といった抽象的な内容では足りず、安全管理措置の具体的項目ごとに自社で実際に講じている措置を明らかにすることが必要。

・外国提供に該当する場合でもしない場合でも、外国で個人データを取り扱っていれば、外国の国名や個人情報保護法制の把握が必須に。国名の公表等も必要。外国クラウドのほか、外国サーバを利用した国内クラウドも、これに該当するので要留意。

・ターゲティング広告等を行っている場合、利用目的の明確化も必須。

1. 法改正概要

²⁴ <https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku>

令和2年法改正により民間企業は、安全管理措置とプロファイリング等についての公表等義務に対応する必要がある。これらは、3つの分解することができる。1つは安全管理措置についての公表である。これはどのような場合でも対応が必須となる。2つ目は安全管理措置の一種ではあるが、外的環境の把握についての公表である。これは個人データを外国で取り扱う場合に対応が必須となる。個人データを外国で取り扱う場合は外国提供よりも範囲が広く、例えば自社の外国派出所や、自社管理の外国サーバ、他社クラウドの外国サーバで個人データを取り扱う場合等がこれに該当する。3つ目はプロファイリング等の公表等である。これは、ターゲティング広告その他のプロファイリング等を行っている場合にのみ対応が必要となる。以下、順に解説する。

（１）安全管理措置の公表等

個人情報保護法ではこれまでも一定の事項についての公表等が求められてきた（法21条1・3項、27条2・3項・5項2号、32条1・2項等）が、令和2年法改正により具体的にどのように安全管理措置を行っているかに関する公表も求められることとなった（法32条1項4号、令10条1号）。「公表等」と記載しているのは、必ずしも「公表」という方法でなくても足りるためである。個人情報保護法上求められているのは、「本人の知り得る状態に置くこと」である（法32条1項）。なお、本人の求めに応じて遅滞なく回答することでも良い（同項柱書かつ書き）。多くの民間企業では、個人情報保護法上の公表義務をプライバシーポリシーや個人情報保護宣言／個人情報保護方針等の形で履行している場合が多いが、必ずしもプライバシーポリシーの形で公表しなくても良い。例えば本人が求めてきたらすぐに回答する方法やパンフレットの備置や配布、ポスター掲示などでもよい²⁵。ただし、本人が知ろうと思えば知ることのできる状態におく必要があり、合理的に考えてその方法では本人が認識できないような方法では認められない。

安全管理措置の公表としては、「個人情報保護法や通則ガイドラインに沿って安全管理措置を実施している」といった抽象的な内容では足りず²⁶、通則ガイドラインで求められている安全管理措置の具体的項目ごとに自社で実際に講じられている措置を明らかにすることが必要である。安全管理措置というと暗号化や認証などの技術的なセキュリティ対策のみと誤解する向きもあるが、規程、体制、点検、教育、外的環境の把握なども含まれるので、誤解しないよう注意が必要である。安全管理措置の公表等にかかる記載例が通則ガイドライン3-8-1(1)に記載されているので参考にされたい（図表5にも同記載例を掲載）。

図表5 安全管理措置の公表等に係る記載例

通則ガイドライン3-8-1(1)から引用の上一部筆者編集（＝※7という記載のカットのみ筆者にて行って、あとはガイドラインのまま）

【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】

（基本方針の策定）

事例）個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「質問及び苦情処理の窓口」等についての基本方針を策定

²⁵ 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）平成28年11月（令和3年10月一部改正）（以下、「通則ガイドライン」という。）3-8-1(1)※1

²⁶ 通則ガイドライン3-8-1(1)④

(個人データの取扱いに係る規律の整備)

事例) 取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について個人データの取扱規程を策定

(組織的安全管理措置)

事例1) 個人データの取扱いに関する責任者を設置するとともに、個人データを取り扱う従業者及び当該従業者が取り扱う個人データの範囲を明確化し、法や取扱規程に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備

事例2) 個人データの取扱状況について、定期的に自己点検を実施するとともに、他部署や外部の者による監査を実施

(人的安全管理措置)

事例1) 個人データの取扱いに関する留意事項について、従業者に定期的な研修を実施

事例2) 個人データについての秘密保持に関する事項を就業規則に記載

(物理的安全管理措置)

事例1) 個人データを取り扱う区域において、従業者の入退室管理及び持ち込む機器等の制限を行うとともに、権限を有しない者による個人データの閲覧を防止する措置を実施

事例2) 個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、事業所内の移動を含め、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが判明しないよう措置を実施

(技術的安全管理措置)

事例1) アクセス制御を実施して、担当者及び取り扱う個人情報データベース等の範囲を限定

事例2) 個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入

(外的環境の把握)

事例) 個人データを保管しているA国における個人情報の保護に関する制度を把握した上で安全管理措置を実施

(2) 安全管理措置の公表等(外的環境の把握)

上記記載例の最後にあるように、安全管理措置には「外的環境の把握」も含まれる。外国において個人データを取り扱う場合、当該外国の個人情報保護制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じなければならない²⁷。具体的な公表等事項としては外国の国名と安全管理措置の内容となる。

①外国の国名

個人情報保護法28条の外国提供時に情報提供する外国の国名は、サーバの所在国ではなく提供先の所在国であったが、法32条1項4号で公表等する外国の国名では、サーバの所在国と取り扱われる国の双方の名称が必要だ。例えば自社パリ支店でアメリカのサーバに保存された個人データを取り扱うのであれば、フランスとアメリカということになる。シンガポール

²⁷ 通則ガイドライン10-7

のサーバを利用したデンマークの会社が提供するクラウドサービスで個人データを取り扱うのであれば、シンガポールとデンマークになる²⁸。個人データが保存されるサーバが所在する国を特定できない場合には、（i）サーバが所在する国を特定できない旨及びその理由、及び（ii）本人に参考となるべき情報（例えば、外国の候補が具体的に定まっている場合であればその外国の名称等）を本人の知り得る状態に置く必要がある²⁹。また、外国の個人情報保護制度等については、当該企業において把握することは必要だが、必ずしも公表等までは求められない³⁰。

②安全管理措置の内容

そして、何をもって「外国において個人データを取り扱う場合」に該当し、外的環境の把握にかかる公表等を行う必要があるかが、非常に複雑である。第1章の外国提供に該当しない場合であっても、該当する場合であっても、「外国において個人データを取り扱う場合」に該当するために、外国の個人情報保護制度等の外的環境の把握といった安全管理措置の公表等が求められることがある。

例えば、自社法人内だが外国にある支店から日本のサーバに保管されている個人データを取り扱わせる場合は、法28条の外国提供には該当しない³¹が、法32条1項4号の義務は発生する³²。これは当該外国がEEAであっても同様であり、法32条1項4号の観点から国名等の公表が必要となる³³。また、外国の委託先に個人データを取り扱わせる場合は、法28条の外国提供に該当するとともに、法32条1項4号の義務も発生する³⁴。これに対して委託先以外の外国法人に個人データを提供する場合は、法28条の外国提供に該当して情報提供義務が発生する一方で、事案にもよるが、概して「外国において個人データを取り扱う場合」には該当せず、法32条1項4号の観点からは公表等の義務は発生しない（もっともこの場合、法28条の情報提供義務が発生しているため、EEAへの提供や法27条1項各号該当の場合を除き、情報提供は必要となる）³⁵。

③クラウドが外国である場合

またクラウド事業者が外国である場合や、クラウドサーバが外国である場合は、さらに複雑である（図表6参照）。外国にある第三者の提供するクラウドサービスを利用する場合において、クラウド事業者が「個人データを取り扱わないこととなっている場合」には、法28条の外国提供には当たらない³⁶。「個人データを取り扱わないこととなっている場合」とは、契約条項によって当該クラウド事業者がサーバに保存された個人データを取り扱わない

²⁸ Q&A10-25

²⁹ Q&A10-25

³⁰ 「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）の一部を改正する告示案」に関する意見募集結果（以下「通則パブコメ」という。）A462

³¹ 外国提供ガイドライン2-2

³² 通則パブコメA465

³³ 通則パブコメA462・A469

³⁴ 通則パブコメA462

³⁵ 通則パブコメA462

³⁶ Q&A10-25

旨が定められており、適切にアクセス制御を行っている場合等が考えられる³⁷。しかし、外国提供に当たらずとも外国において個人データを取り扱うこととなるため、法32条1項4号の観点からはクラウド事業者が所在する外国の国名及び個人データが保存されるサーバが所在する外国の国名を明らかにし、安全管理措置について公表等する必要がある³⁸。なお、クラウド事業者が「個人データを取り扱わないこととなっている場合」には、「委託」に該当しないため、クラウドを利用する企業はクラウド事業者に対する監督義務を負わないものの、自社として個人データを取り扱っていることには変わりはないため、安全管理措置義務を負い³⁹、個人データを安全に管理しなければならない。

図表6 クラウド利用時の情報提供義務・安全管理措置等

クラウド利用時の情報提供義務・安全管理措置等

法的義務	詳細
委託先監督 (国内&国外)	- クラウド事業者が個人データを取り扱わない場合*は、委託に非該当。監督義務を負わない *契約条項によってクラウド事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合 (Q&A7 -53) **クラウド事業者が個人データを機械学習する場合等、人の目に触れなくても、クラウド事業者が利用していれば、取り扱っているものと考えられる (水町解釈)
安全管理措置 (国内&国外)	- 個人データを取り扱わないこととなっている場合であってもなくとも、クラウドを利用する側が安全管理措置を講じる必要がある。適切な対応を行っているクラウドを選定する必要等あり。 - 安全管理措置の情報公表等義務あり (法 32条1項4号・施行令10条1号)。 - 外国の場合は、①外国の名称 (クラウド事業者が所在する国及び個人データが保存されるサーバが所在する国) を明らかにし、②当該外国の制度等を把握した上で③安全管理措置を講じ、④外国の名称と当該安全管理措置の内容***を本人の知り得る状態 (本人の求めに応じて遅滞なく回答する場合を含む。) に置く必要がある (Q&A10-25)。
国外提供	- クラウド事業者が個人データを取り扱わない場合*は、クラウド事業者やサーバが外国であったとしても、外国提供には非該当。 - 取り扱うこととなっている場合には、外国提供に伴う情報提供義務が発生。

(3) プロファイリング等の公表等

海外ではプロファイリングに対する法規制を設けている例もあるが、日本ではこれまで、プロファイリングと他の個人情報の取扱いとの間で法規制に差は存在していなかった。しかし、ターゲティング広告が日常的に行われるようになって久しく、またリクナビにおける不適切な事案等、一般人から見た場合に予測が難しいような取扱いも発生し、プロファイリング等に対し、日本でも法規制を行うべきだとの議論があった。結果的には、令和2年法改正ではプロファイリング等への法規制は見送られ、従前から存在している利用目的の特定・公表等義務の一環として、プロファイリング等への対応がなされた。

すなわち、個人情報保護法では元々、本人が自分の個人情報がどのように取り扱われるかが予測できるように利用目的を特定し (法17条1項)、公表等する義務があった (法21条1項、32条1項2号)。この利用目的の特定・公表等義務の一環として、プロファイリング等を行う場合は、利用目的をわかりやすく特定・公表等することが求められる。なお「プロファ

³⁷ Q&A7-53

³⁸ Q&A10-25

³⁹ Q&A7-54

イリング等」の定義は特段設けられておらず、通則ガイドライン3-1-1では、図表7のように記載されている。

図表7 プロファイリング等の公表等（ガイドラインから引用）

例えば、本人から得た情報から、本人に関する行動・関心等の情報を分析する場合、個人情報取扱事業者は、どのような取扱いが行われているかを本人が予測・想定できる程度に利用目的を特定しなければならない。

【本人から得た情報から、行動・関心等の情報を分析する場合に具体的に利用目的を特定している事例】

事例1) 「取得した閲覧履歴や購買履歴等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。」

事例2) 「取得した行動履歴等の情報を分析し、信用スコアを算出した上で、当該スコアを第三者へ提供いたします。」

2. 実務対応

(1) 安全管理措置の公表等

この点に関し必要となる実務対応としては、まずはそもそも個人データに対して求められる安全管理措置を通則ガイドラインで確認することから始めるべきであろう。それを正確に把握した上で、安全管理措置を「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」に分け、それぞれについて自社で行われている具体的措置を確認する。確認時に、現状の安全管理措置について改善等の必要があればこの機に改善等を行うべきであろう。その後、通則ガイドライン記載例に沿って、自社で行われている安全管理措置を記述することになる。プライバシーポリシー等で公表等するのであれば公表等対応を行い、プライバシーポリシー等では対応しないのであれば、具体的にどのような方法で公表等を行うかも検討が必要である。

(2) 安全管理措置の公表等（外的環境の把握）

次に、外的環境の把握として必要となる実務対応としては、まず「外国において個人データを取り扱う場合」の有無にかかる全社の実態調査・委託先調査を行うべきであろう。外国取扱いがある場合、国名、当該国の個人情報保護法制、どのような安全管理措置を行うかを調査し、国名と安全管理措置について公表等を行うことになる。プライバシーポリシー等で公表等するのであれば公表等対応を行い、プライバシーポリシー等では対応しないのであれば、具体的にどのような方法で公表等を行うかも検討が必要である。

なお、第1章「外国提供（越境移転）関連の情報提供・提供先確認等の義務」対応と一体的に行った方が効率的だと考えられ、例えば、外国取扱いの有無を幅広く調査した上で、それを「外国提供」とそれ以外に振り分けて必要となる対応を行った方が、調査の重複がなくなる可能性も高い。

(3) プロファイリング等の公表等

プロファイリング等の公表等については、自社における個人情報の利用目的・利用方法を洗い出し、それと現在公表等されている利用目的を確認し、本人から見てわかりにくいものがないか検討し、あれば改めていくことが必要である。

（４）今後の改訂等対応

今後の運用の中で、現在の安全管理措置（外的環境も含む。）や利用目的を変更した場合には、公表等事項の改訂も必要となりうるので、安全管理措置や利用目的を変更する場合には事前に社内で協議し、公表等事項の改訂の必要性の有無を検討できるような社内体制を整備し、従業員へ周知していく必要がある。

3. チェックポイント

安全管理措置・プロファイリング等の公表等にかかる実務対応を次の図表にまとめたので、参考にされたい。なお、外的環境の把握については、図表9にさらに詳しくまとめたので、そちらも合わせて参照されたい。

図表8 安全管理措置・プロファイリング等の公表等チェックポイント

安全管理措置・プロファイリング等の公表等チェックポイント

① 安全管理措置の公表等

- ✓ 個人データに求められる安全管理措置を通則ガイドラインで確認
- ✓ 「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」について、自社で行われている安全管理措置を確認
- ✓ （上記安全管理措置について改善等の必要があれば改善等を行う）
- ✓ 通則ガイドライン 記載例に沿って、自社で行われている安全管理措置を記述
- ✓ 公表等方法（プライバシーポリシー or その他）の検討
- ✓ 公表等を行う

② 安全管理措置の公表等（外的環境の把握）

- ✓ 「外国において個人データを取り扱う場合」の有無にかかる全社の実態調査・委託先調査
- ✓ 有の場合、国名、当該国の個人情報保護法制、どのような安全管理措置を行うかを調査
- ✓ 公表等方法（プライバシーポリシー or その他）の検討
- ✓ 国名と安全管理措置について公表等を行う

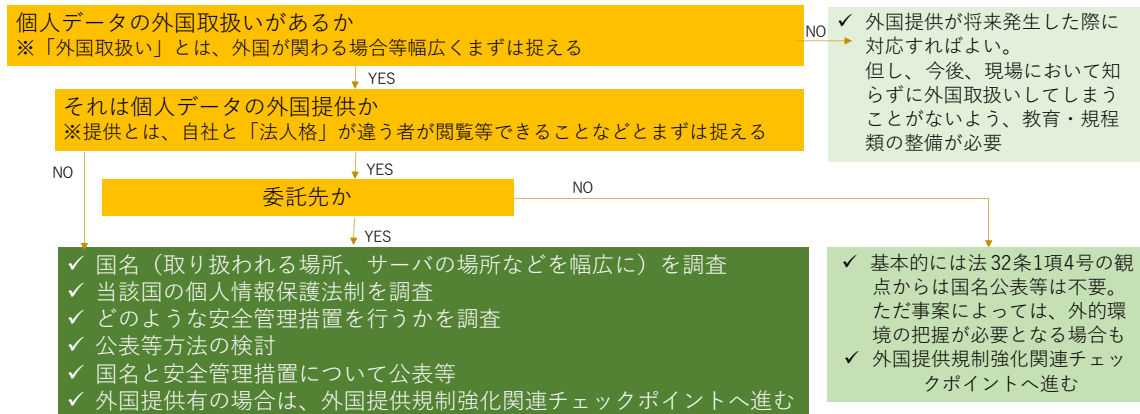
③ プロファイリング等の公表等

- ✓ 自社における個人情報の利用目的・利用方法の洗い出し
- ✓ 現在公表等されている利用目的を照らし合わせて確認
- ✓ 本人から見てわかりにくいものがないか検討し、あれば改めていく

今後安全管理措置や利用目的が変更になった場合に、あわせて公表等事項の改訂等の必要性検討も行えるよう、社内体制の整備・周知も必要

図表9 個人情報保護法32条1項4号外的環境の把握のチェックポイント

個人情報保護法32条1項4号外的環境の把握の チェックポイント



※外国取扱いを幅広く調査した上で、それぞれを外国提供とそれ以外に振り分ける作業を行った方が効率的かもしれない

第3章 その他の規制強化

【要約】

- ・漏えい時等の当局報告・本人通知、本人権利の強化（開示・訂正・利用停止等）、個人データの提供/受領記録の開示義務、個人関連情報規制の新設、オプトアウト規制強化、不適正利用の禁止、罰則等の強化、域外適用について法改正がなされている。
- ・中でも、Cookie等のWebを活用した個人関連情報規制の新設や、オプトアウトによる個人データの授受がある場合は影響が大きい。また個人データの提供/受領記録が適切に作成・保存されていない場合は、速やかな改善を行った上、記録の開示義務対応を進めていく必要がある。

1. 漏えい時等の当局報告・本人通知

（1）法改正概要

これまでは個人情報を漏えい等した場合であっても、特に個人情報保護法上は報告等の義務がなかったが、令和2年法改正によって、内閣府の外局である個人情報保護委員会に届け出る法的義務、そして漏えい等した個人情報の対象者（本人）へ通知する法的義務が新たに生じる（法26条）。

もっとも、あらゆる場合に当局報告・本人通知義務が発生するわけではなく、以下の個人データの漏えい、滅失、毀損又はそのおそれがある場合に限定される（規則7条）。

- 要配慮個人情報が含まれる個人データ
- 財産的被害が発生するおそれ（クレジットカード番号やインターネットバンキングのID・パスワード⁴⁰等）
- 故意等の不正目的又はその恐れ（不正アクセス、ランサムウェア、盗難、内部不正等）
- 100人以上

⁴⁰ 通則ガイドライン3-5-3-1(2)

高度な暗号化その他の必要な措置を講じた場合は、abcdに該当しても報告は不要となるが、その基準⁴¹は厳格であるので、企業側が「高度」だと考えれば足りるといったものではない。

報告はその事態を知った日から、abdの場合は30日以内、cの場合は60日以内に行う必要がある（規則8条2項）。GDPRで求められる場合よりも時間的余裕があるように感じられるが、とはいえ、その事態を知ったときから3～5日以内に速報を入れ⁴²、その後30日又は60日以内に確報を入れる。その事態を知った日を1日目と数え、土日祝日も1日としてカウントされるが、報告期限が土日祝日の場合はその翌日が報告期限となる⁴³。

本人通知は速やかに行うことが必要（規則10条）だが、具体的期限の目安は特に示されていない⁴⁴。

（２）実務対応

これまでの個人情報保護法の実務運用でも、この令和2年法改正上の義務に近い対応がなされてきた場合がある。例えば、プライバシーマーク付与事業者であれば、個人情報の外部漏えいその他本人の権利利益の侵害が発生した際には、JIPDEC等のプライバシーマーク指定審査機関への報告が必要であるし（プライバシーマーク付与に関する規約（PMK500）11条2項）、GDPRが適用される事業者であれば、個人データ侵害が発生した際にはデータ保護当局への報告（GDPR33条1項）及び本人への連絡（GDPR34条1項）が義務付けられている。また一部の民間企業においては、個人情報保護委員会へ自発的に報告を行ってきた場合もある。

そこで、まずは個人情報の漏えいや不正利用時等に、自社で現在どのような対応を行っているのかを整理し、現行の社内規程やプライバシーポリシー等の記載内容を確認した上で、改正法対応として、どのような時に誰がどのようなルートで個人情報保護委員会への報告及び本人通知を行うかを検討し、従業員教育を行っていくことが必要であろう。社内規程やプライバシーポリシー等の現在の規定ぶり等によっては、改正法対応としてこれらの修正を行うべき場合も考えられる。

なお、法改正によって新設される「仮名加工情報」を用いる場合は、漏えい時等にも当局報告や本人通知は不要であるため、場合によっては仮名加工情報の活用を検討することも考えられる。

本人通知義務については、個人への個別連絡等が求められる場合には、対象者数等によっては実務に多大な影響が及ぶ可能性がある。但し、「本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるとき」には、通知義務が課せられない（26条2項但書）ことから、自社実務にフィットする対応を検討していくことが重要となろう。

2. 本人の権利強化

（１）法改正概要

本人が自分の保有個人データを見せてほしいと請求（開示請求）した場合はそれに応じる法的義務が課せられており、また一定の場合には保有個人データを訂正したり利用停止等す

⁴¹ Q&A6-16

⁴² 規則8条1項、通則ガイドライン3-5-3-3

⁴³ 通則ガイドライン3-5-3-4

⁴⁴ 通則ガイドライン3-5-4-2

る義務（訂正等請求、利用停止等請求への対応義務）が課せられている。例えば、病院は請求されれば本人にカルテを開示しなければならず、違法行為を行った民間企業は請求されれば住所・電話番号等の利用停止や消去をしなければならない。

もっとも、これらの義務が正しく理解・運用されていないケースも散見され、消費者からの苦情も多く寄せられていることから、個人情報保護委員会では民間企業の対応状況を注視していくと明言している⁴⁵。さらに令和2年法改正では、①開示・訂正等・利用停止等請求対象の拡大、②開示方法のデジタル化、③利用停止等義務の拡大も行われる。

①開示・訂正等・利用停止等請求対象の拡大とは、これまでは対象外だった「6か月以内に消去する短期保存データ」も請求対象に加える改正である。

②開示方法のデジタル化とは、現行法では開示方法は原則書面であって、例外として請求者が同意した方法が認められていた（現行法28条2項・令9条）が、令和2年法改正後は、本人によるデジタル請求が前面に押し出され（法33条1項）、開示方法についても本人が請求した方法が原則とされる（法33条2項）改正である。もっとも、多額の費用を要する場合や本人請求方法による開示が困難な場合には、書面開示でもよいとされている（法33条2項）。

③利用停止等義務の拡大とは、これまでは一定の違法行為がなければ利用停止等請求ができなかったものの、令和2年法改正後は、違法行為の対象が追加されるほか、漏えい等が生じた場合や、本人の権利・正当な利益が害されるおそれがある場合には、保有個人データの利用停止、消去、第三者への提供停止を求めることができる（法35条1・3・5項）ようになる改正である。本人の請求に理由があるときには、民間企業はこれに対応し、遅滞なく保有個人データの利用停止、消去又は第三者への提供停止を行わなければならない。但し、多額の費用を要する場合その他実施が困難で、本人の権利利益保護のために必要な代替措置をとるときは、利用停止、消去又は第三者への提供停止を行わなくともよい（法35条2・4・6項但書）。

（２）実務対応

①開示・訂正等・利用停止等請求対象の拡大については、まず自社で6か月以内に消去するデータを開示・訂正等・利用停止等請求の対象としているか否かを確認する必要がある。これまでも対象としていれば、本改正事項による影響はない。これまで対象としていなかった企業においては、これらを対象とするよう運用を変更し従業員教育をする必要がある。また社内規程・プライバシーポリシー等の現在の記載が、6か月以内に消去するデータを対象から除外しているようであれば、改訂する必要がある。

②開示方法のデジタル化についても、自社でどのような請求・開示方法をとっているかを確認し、書面で実施しているならデジタル化対応を行う必要がある。また社内規程・プライバシーポリシー等の現在の記載が、書面に限定しているようであれば、改訂する必要がある。

③利用停止等義務の拡大については、プライバシーマーク付与事業者等においては既に、現行法で求められるよりも幅広く利用停止等を実施している場合があるものの、令和2年法改正後は、現行法及びプライバシーマーク制度に基づく運用と変更が生じ得る。プライバシ

⁴⁵ 「個人情報保護法 いわゆる3年ごと見直し 制度改正大綱」令和元年12月13日（以下、「大綱」という。）9頁

一マーク付与事業者か否かにかかわらず、一定の違法行為や漏えい等が生じた場合及び本人の権利や正当な利益が害されるおそれがある場合には、保有個人データの利用停止、消去、第三者への提供停止を実施するよう運用を変更し、従業員教育をする必要がある。利用停止、消去、第三者への提供停止はビジネスに甚大な影響を及ぼす可能性もあるため、自社の事業部門にこの旨を周知する必要があると考えられる。また社内規程・プライバシーポリシー等の現在の記載が、利用停止等を行う場合を限定したものになっている場合等については、これらを改訂する必要もある。

3. 個人データの提供/受領記録の開示義務

(1) 法改正概要

現行法下でも個人データを提供したり提供を受けたりする場合には、一定事項を確認し、記録を作成・保管する義務があったが、令和2年法改正により、この記録を本人が閲覧等したいと請求（開示請求）した場合にこれに対応する法的義務が設けられた（法33条5項）。これまで個人は、自分のどのような個人データが誰から誰へいつ提供/受領されたかについて、知ることができなかったと考えられる。それが令和2年法改正後は、本人が自分で提供/受領記録を確認することができるので、個人にとって非常に影響の大きい改正といえる。

もっとも、個人データの提供/受領のたびに必ず記録義務が生じるわけではなく、例外⁴⁶が認められている（法29条1項但書、30条1項但書・3項）。委託に伴う個人データの提供/受領に際しては記録を求められないし、法令に基づく場合等の法27条1項各号に該当する場合も記録を求められない。

(2) 実務対応

記録義務が発生しない企業においては影響がない法改正であるため、まずは自社において記録義務が発生する提供/受領があるかどうかを確認すべきである。そのような提供/受領がある場合は、記録に漏れや不備等がないかを今一度見直したうえで、開示請求対応を行う必要がある。企業においてはこれまでも現行法に基づき、個人データの提供/受領記録を作成・保管してきたものと考えられるが、これまでは仮に記録に漏れや不備があったとしても、外部からはそれをうかがい知ることが難しかったが、令和2年法改正後は、本人自身が記録を確認できるようになる。また社内規程・プライバシーポリシー等の現在の記載では、個人データの提供/受領記録の開示に対応していないように読めるようであれば、これらを改訂する必要がある。

4. 個人関連情報規制の新設

(1) 法改正概要

個人データの外部提供は規制されている（法27条）が、提供情報が個人データかどうかを巡り現行法及び当局解釈では規制に穴が生じる場合があり、実際にリクナビ事案⁴⁷が発生した。提供情報が個人データか否かは、当該提供情報単体を見たときに誰の情報かがわかるかどうかではなく、提供元において誰の情報かがわかるかどうかを基準に判断される（提供元基準説）。そのため、図表10では提供情報が提供先にとっては個人データでなくても、個人データの提供に該当する。これに対し図表11では、提供情報が提供先にとっては個人データ

⁴⁶ <https://www.miyauchi-law.com/f/200325pii2020kaiseigaiyou>の138ページ等参照

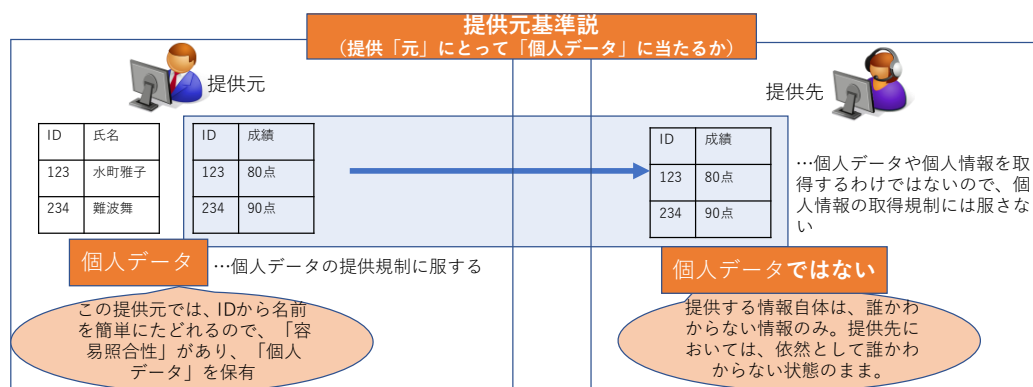
⁴⁷ <https://www.recruitcareer.co.jp/r-dmpf/>

であっても個人データの提供に該当しないとも考えられる。実際にリクナビ事案では、図表11に類似するスキームが採用されていた。

そこで令和2年法改正では、「個人関連情報」というカテゴリを新設し、提供元にとって個人情報でなくても提供先において個人データとして取得することが想定されるときは、法令に基づく場合等の法27条1項で認められた場合を除き、提供元に、本人の同意等を確認する義務が課せられた（法31条1項）。

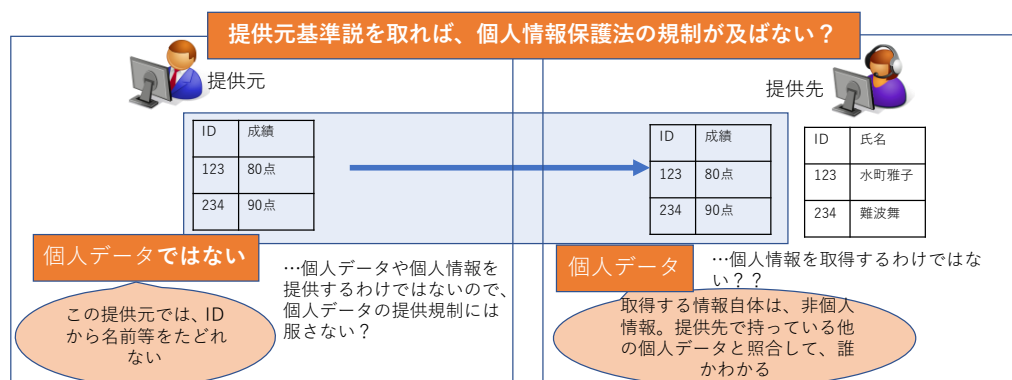
図表10 提供元基準説で個人データ提供に該当する場合

提供元基準説で個人データ提供に該当する場合



図表11 提供元基準説で個人データ提供に該当しない場合

提供元基準説で個人データ提供に該当しない場合



(2) 実務対応

個人関連情報はリクナビのCookie情報の外部提供を踏まえての規制ではあるが、法適用上は必ずしもCookieにのみ適用される規制ではない。特にWeb関連で他企業とデータ授受がある場合は、Cookie以外でも個人関連情報に該当する可能性が考えられるため、自社で個人関連情報の授受がないかどうか、網羅的な確認が必要である。

5. オプトアウト規制強化

(1) 法改正概要

個人データの外部提供に際しては本人同意が必ずしも求められるわけではなく、一定事項を届出・公表等の上、本人同意なく個人データを提供し、本人から拒否されたら提供を停止するという「オプトアウト」が法律上認められている（法27条2項）。しかし、オプトアウトによって個人データが転々流通していくといった危惧もあり、オプトアウトは徐々に規制強化されてきた。平成27年法改正では、要配慮個人情報のオプトアウトが禁止されたが、令和2年法改正では、要配慮個人情報に加え、①不適正取得されたもの、②オプトアウトの連鎖も禁止された（同項但書）。

またオプトアウトに際しては個人情報保護委員会への届出及び公表等が求められるが、令和2年法改正では届出・公表等事項の追加も行われた（法27条2項）。

(2) 実務対応

自社でオプトアウトによる個人データの授受を行っていない場合は何ら影響のない法改正であるので、まずはオプトアウトの有無を確認する必要がある。オプトアウトがある場合は、届出及び公表等を必ず令和4年4月1日より前に行い、かつ禁止された種類のオプトアウトは今後取りやめ、他の方法による個人データの授受に切り替える必要がある。

6. その他

上記のほかにも規制強化された事項があるものの、上記以外の点は影響を受ける企業が少なく、また紙幅の制限から簡単な解説にとどめることとする。

(1) 不適正利用の禁止

その他の規制強化として、まず、不適正利用の禁止の新設がある（法19条）。これもリクナビ事案を踏まえて新設された規制と考えられる。違法又は不当な行為を助長・誘発するおそれがある方法による個人情報の利用が明示的に禁止される。多くの企業では、そもそも違法又は不当な利用等が存在しないため、影響はないと考えられるが、今一度自社の個人情報の取扱いを棚卸し、違法・不当な取扱いがないか確認すると良いだろう。

(2) 罰則等の強化

令和2年法改正では罰則等が強化される。もっとも現行法下でも改正法下でも、通常のビジネス遂行時についてうっかりやってしまうことへの罰則ではないため、過剰に懸念する必要はないが、違法行為がなされないよう従業員監督を今一度徹底することが重要であろう。改正内容としては、個人情報保護委員会の命令に違反した場合は、これまで6月以下の懲役または30万円以下の罰金だったが、改正法下では1年以下の懲役または100万円以下の罰金となり（法173条）、さらに法人業務等に関する場合、法人に1億円以下の罰金が科せられる（法179条1項1号）。加えて、個人情報保護委員会は、命令違反を公表することができるようになる（法145条4項）。また個人情報保護委員会の検査等を妨害等した場合は、これまで

30万円以下の罰金だったが、改正法下では50万円以下の罰金となる（法177条1号）。業務に関して取り扱った個人情報データベース等を不正な利益を図る目的で提供又は盗用した場合には、これまで1年以下の懲役または50万円以下の罰金だったが、改正法下ではさらに法人業務等に関する場合、法人に1億円以下の罰金が科せられる（法179条1項1号）。

（３）域外適用

令和2年法改正では外国関連の規制が複数盛り込まれた。既に述べた外国提供時の情報提供・提供先確認等の義務や安全管理措置の公表等（外的環境の把握）だけでなく、個人情報保護法自体の域外適用を広く認める法改正がなされている（法166条）。

第４章 個人情報の利活用促進

【要約】

・個人情報の利活用促進のため、仮名加工情報新設といった規制緩和も行われた。一定の加工を実施して仮名加工情報化すれば、利用目的の変更が自由に行えるほか、漏えい報告義務が課せられず、開示・訂正等・利用停止等請求の対応が不要になる。

・規制緩和は必ず対応しなければならない事項ではなく、活用したい企業は活用を検討すればよい。

令和2年法改正では規制強化のほか、個人情報の利活用促進のためのいくつかの方策がとられた。

１．仮名加工情報

（１）法改正概要

プライバシー権保護と個人情報利活用の両立を図るため、平成27年法改正では「匿名加工情報」というカテゴリを設け、個人情報を法定の加工基準で匿名加工した場合に、規制を大幅に緩和し、内部利活用や外部提供を容易にした。しかし、「匿名加工」は一般の想像よりもはるかに加工基準が厳しく、法定の加工基準を満たすことが難しい場合も散見された。また個人情報に対する法規制が厳格なEUにおいても、「仮名化」を行うと若干緩やかな取扱いが認められ、国際的にもその活用が進みつつある⁴⁸。そこで令和2年法改正では、個人情報と匿名加工情報の中間形態ともいえる「仮名加工情報」を新設し、通常の個人情報よりも規制を緩和した。

仮名加工情報の作成時には、他の情報と照合しない限り特定の個人を識別できないよう規則で定める基準を遵守する必要がある（法41条第1項）。具体的には、①氏名等、②マイナンバー等の個人識別符号、③不正利用により財産的被害が生じるおそれがある記述等を削除すればよい（規則31条）。①は氏名だけではなく、住所、生年月日、性別等のほか、その情報単体や組み合わせることで特定の個人を識別できる記述等を削除する必要がある⁴⁹。②の個人識別符号は、法2条2項で定義されており、身体特徴系符号（DNA、顔、虹彩等をデジタルデータに変換したもののうち規則で定める基準に適合するもの）と番号系符号（マイナンバー、免許証番号等の公的機関が割り振る令及び規則で定める番号）を指す。③の例として

⁴⁸ 大綱21頁

⁴⁹ 「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）」平成28年11月（令和3年10月一部改正）（以下、「加工ガイドライン」という。）2-2-2-1-1

は、クレジットカード番号や、送金や決済機能のあるウェブサービスのログインID・パスワード⁵⁰等が挙げられる。これに対し、クレジットカード番号の下4桁だけや口座番号は、不正利用されても直ちに財産的被害が生じるおそれがあるとはいえないため、削除しなくてもよいとされている⁵¹。

（２）仮名加工情報に対する規制⁵²

仮名加工情報では3点について規制緩和される。1つ目は、利用目的の変更が自由に行える点である。個人情報の場合、予め特定した利用目的の範囲内で目的内取扱いすることが法律の原則である（法18条）。利用目的の変更も可能ではあるものの、変更範囲に制約があり

（法17条2項）、変更しにくい状況が続いていた。この点、仮名加工情報であれば、利用目的の変更には制限がないため（法41条9項にて17条2項が適用除外）、あらかじめ特定した利用目的の範囲外でも自由に内部利用できる。もっとも、法的手続としては、利用目的の変更を行った上で、変更後の利用目的を公表等することが必要である（法41条4項にて読み替えて適用される21条3項）。なお、利用目的の変更には制約はないものの、仮名加工情報に含まれる情報を使って、電話、郵便、FAX、電報、電子メール、SMS、住居訪問等を行うことは禁止される（法41条8項）。

規制緩和の2点目として漏えい報告義務が課せられない点が挙げられる。個人データの漏えい等時には当局報告・本人通知が義務付けられるが、仮名加工情報の場合は不要である（法41条9項にて26条が適用除外）。

3点目として開示・訂正等・利用停止等請求の対応が不要になる。保有個人データの場合は、本人はこれらの請求権を保有しているが、仮名加工情報の場合は適用除外されている（法41条9項にて32条から39条までが適用除外）。

仮名加工情報は提供規制が厳格であり、外部提供できるのは、①法令に基づく場合、②委託、③合併等の事業承継、④共同利用のみである（法41条6項）。容易に外部提供できる匿名加工情報との明確な差異であるので、十分注意する必要がある。また、仮名加工情報は本人を識別するために他の情報と照合することも禁止されている（法41条7項）。この照合禁止義務は匿名加工情報と同様である。

さらに仮名加工情報であっても、不適正利用の禁止（法19条）、適正取得（法20条1項）、安全管理措置（法23条）、従業者監督（法24条）、委託先監督（法25条）は引き続き適用されるし、利用する必要がなくなった場合の消去（法41条5項）及び苦情処理（法40条）の努力義務も適用される。

2. 公益目的の個人情報の取扱い促進

令和2年法改正に伴い、公益目的の個人情報の取扱い促進のためにガイドライン改訂が行われる予定であった。しかし現実にはQ&Aが若干追加された⁵³にとどまり、あまり企業が活用できる状態にはなっていない。

⁵⁰ 加工ガイドライン2-2-2-1-3

⁵¹ Q&A14-8

⁵² 仮名加工情報は、個人情報に該当する場合と該当しない場合があるが、個人情報に該当する場合が多いと考えられるため、本稿では個人情報に該当する仮名加工情報の規制について論じる。

⁵³ Q&A7-25等

3. PPCビジネスサポートデスク

個人情報保護法は「個人の権利利益を保護することを目的とする」が、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮」することも求めている（法1条）。そして、個人情報保護委員会も個人情報の保護だけではなく個人情報の「適正かつ効果的な活用についての広報及び啓発」がその所掌事務とされている（法129条6号）。個人情報のビジネス利活用促進のため、令和2年法改正に先立ち、個人情報保護委員会が個人情報の利活用相談等に応じる「PPCサポートデスク」が開設された。必要に応じ、適宜相談してみると良いだろう。

4. 実務対応

令和2年法改正の中でも規制強化された部分は必ず対応しなければならないが、これに対し個人情報の利活用促進のための方策については、活用したい企業だけが活用すればよい。そのため特に対応が求められるわけではないが、中でも仮名加工情報はこれを活用することで企業における負荷が下がり、本人のプライバシー権保護にも資することが考えられるため、活用を検討してみても良いだろう。

おわりに チェックポイント

最後に、令和2年法改正対応として必要な事項をまとめたので、施行直前の確認として参照されたい。

図表12 改正個人情報保護法対応のチェックポイント

改正個人情報保護法対応のチェックポイント

影響を受ける人	改訂すべき文書	法改正事項	やるべき対応案 ※太字が急ぎ	影響度
全員	・ プライバシーポリシー等 ・ 規程等 ・ 社内フロー等	2 安全管理措置・プロファイリング等の公表等 安全管理措置の具体的内容の公表等 外的環境の把握・公表等 プロファイリング等の利用目的の明確化・公表等	・ 通則ガイドライン上の安全管理措置の確認 ・ 全社的・委託先の実態調査（・必要な改善） ・ 安全管理措置の記述 ・ 情報提供方法の検討 ・ 従業員教育	★★★★★
	・ 規程等 ・ 社内フロー等	3 漏えい時等の当局報告と本人通知 漏えい時等に当局報告と本人通知が必要に。 実務フロー・社内ルールの変更が必要な場合も。	・ 現行の自社対応確認 ・ 規程・社内フロー改訂 ・ 従業員教育等 ・ 仮名加工情報の活用検討	★★
	・ プライバシーポリシー等 ・ 規程等 ・ 社内フロー等	4 本人の権利強化 ①開示・訂正等・利用停止等請求対象の拡大、②開示方法のデジタル化、③利用停止等義務の拡大	・ 現行の自社対応確認 ・ 規程・フロー・プライバシーポリシー改訂 ・ 従業員教育	★
	・ 規程等 ・ 社内フロー等	8（1）不適正利用の禁止 個人情報保護法、これまでは明確には禁止されていなかった利用も、違法になる可能性	・ 個人情報利用の全チェック	★ 規制対象がある場合は影響甚大
	・ 規程等	8（2）罰則等の強化	・ 通常想定として、特段の対応は不要だが従業員教育等	—

改正個人情報保護法対応のチェックポイント

影響を受ける人	改訂すべき文書	法改正事項	やるべき対応案 ※太字が急ぎ	影響度
海外関連	- プライバシーポリシー等 - 契約書 - 規程等 - 社内フロー等	1 外国提供時の情報提供・提供先確認等 外国に個人データが行くことを、本人が予測できるように、本人に必要な情報提供をする義務	- 外国提供の洗い出し、法的スキームごとに分ける - 提供先との契約書（協力、確認、保護措置） - 情報提供方法の検討 - 情報提供内容の検討 - 従業者教育	★★★★★
		8（3）域外適用 個人情報保護法自体の域外適用を広く認める法改正	域外適用される場合は個人情報保護法の義務遵守要	— 規制対象がある場合は影響甚大
国内委託等以外で個人データの授受がある人	- 規程等 - 社内フロー等	5 個人データの提供/受領の記録の開示義務 本人が要求したら、どことの間で個人データを提供/受領したか、記録を開示する義務が新設	- 自社に記録義務が適用される個人データの提供/受領があるか確認 - 不備・漏れがないか見直し - 規程・フロー・プライバシーポリシー改訂 - 従業者教育	★★★
CookieやWeb活用者等	- 規程等 - 契約書等 - 社内フロー等	6 個人関連情報規制の新設 提供元にとって個人情報でなくても提供先において個人データとして取得することが想定されるときは、原則同意要	- 自社に該当するものがあるか確認 - 特に広告関連 - 本人同意の取得 - 記録の作成・保存対応のスキーム・実務フロー等の検討	— ★★★★★ 規制対象がある場合は影響甚大
オプトアウトで個人データを提供・取得している人	- 規程等 - 社内フロー等 - 契約書等	7 オプトアウト規制強化 個人データをオプトアウトで外部提供していた場合、これまで通りのやり方だと違法になるリスク	- 自社でオプトアウトで取得/提供しているものがあるか確認 - 自社で、禁止される類型をオプトアウトで取得/提供しているものがあるか確認 - 禁止対象は提供・取得不可 - 届出・公表等事項の追加対応	— ★★★★★ 禁止類型がある場合は、影響甚大

11

筆者略歴

弁護士 水町雅子（みずまちなまさこ）。宮内・水町IT法律事務所。内閣官房及び特定個人情報保護委員会にてマイナンバー法立法担当。首相官邸IT総合戦略本部「パーソナルデータに関する検討会」参考人、東京都都政改革アドバイザリー会議委員、総務省・厚生労働省・地方公共団体等の委員を務める。『あなたのマイナンバーへの疑問に答えます』（中央経済社、2015年）、『Q&Aでわかる医療ビッグデータの法律と実務』（日本法令、2019年）、『Q&A個人情報取扱実務全書』（民事法研究会、2020年）等の著書・論文・講演・TV出演・新聞取材等多数。