「個人情報の保護に関する法律についてのガイドラインの一部を改正する告示」に関する意見

2021年6月18日

BSA｜ザ・ソフトウェア・アライアンス[1]（以下、**「BSA」**）は、令和２年６月に公布された改正個人情報保護法に関する「ガイドラインの一部を改正する告示」（以下**「ガイドライン案」**）に関し、個人情報保護委員会（以下、**「貴委員会」**）に対して、以下のとおり意見を提出致します。

総論

BSA は、政府やグローバル市場において、世界のソフトウェア産業を代表する主唱者です。BSA の会員は、他の企業を強化する、B to B テクノロジー製品やサービスを創造するエンタープライズ・ソフトウェア企業です。BSA 会員は、クラウドストレージサービス、カスタマー・リレーションシップ・マネジメント（CRM）ソフトウェア、人事管理プログラム、ID 管理サービス、コラボレーション・ソフトウェアなどのツールを提供しています。企業は、個人情報を含む最も重要な情報を BSA 会員に託しています。その結果、プライバシーとセキュリティの保護は BSA 会員の業務の基本であり、そのビジネスモデルはユーザーのデータを収益化することに依存していません。

BSA は、各国における個人データ保護法の実施に関し、以下を世界的に提唱しています：個人データの収集・利用の透明性の向上、その収集と利用に関するガバナンスを通じて十分な情報に基づいた選択を尊重・可能とすること、消費者による自らの個人データの管理、強固なセキュリティの実践、正当な事業目的のためのデータ利用促進[2]。

[1] BSA の活動には、Adobe, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zoomが会員企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] BSAの「Global Privacy Best Practices」に関しては以下を参照ください。
https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

BSA は以前、「個人情報の保護に関する法律施行規則の一部を改正する規則（案）」について意見[3]を提出しており（以下**「前回意見書」**）、貴委員会が改正個人情報保護法の施行に関し、説明を加えてくれたことに感謝しています。全てのステークホルダーに明確となるようガイドライン案を改善するために、以下、見解と提言を述べさせて頂きます。

ガイドライン案に対しての我々の意見は主に以下の三点に関してとなります。
（1）個人情報の漏えい[4]に関する個人情報取扱事業者の義務
（2）第三国の事業者へのデータ移転に関する規定
（3）個人情報の利用停止に関する個人の請求権

提言

［通則編］3　個人情報取扱事業者等の義務 / 3-5　個人データの漏えい等の報告等

BSA は、貴委員会がセキュリティ・インシデントのリスクを最小限に抑え、インシデント発生時の影響を軽減し、セキュリティ・インシデントの通知に関するコンプライアンスの複雑さを軽減して、その実効性を高めようとしていることを高く評価しています。

特に、BSA は、貴委員会が「漏えい等」の報告・通知の要件をさらに明確にしたことに感謝します。我々は、透明性を高め、個人の権利を強化するという貴委員会の意図を支持します。しかし、ガイドライン案は、事業者が真に意味のある事故報告・通知に注力できるよう、以下で推奨するように修正することでさらに改善することができます。

我々が前回意見書で指摘したように、実際には発生していないかもしれない「発生したおそれがある」漏えいの報告と通知を義務付けることは、関係する全てのステークホルダーに懸念をもたらします。「可能性のある」漏えいの報告を要求することは、組織に負担をかけるだけでなく（インシデントの調査と対応には時間とリソースがかかるため）、貴委員会への報告が殺到し、また当該本人にとっては、取るに足らないデータ・セキュリティ・インシデントと、重大な損害をもたらす可能性があり、適切な是正措置を取るべき漏えい等との区別がつかない情報が氾濫することになります。

これらの懸念を軽減するために、ガイドライン案の以下の箇所における記述を修正することを推奨します。

3-5-1-1 「漏えい」の考え方

[3] https://bsa.or.jp/wp-content/uploads/20210125j.pdf

[4] 英語では一般的に”personal data breach（個人データ侵害）”とも表現されます。
一般データ保護規則（General Data Protection Regulation/GDPR) 4条 (12): https://gdpr-info.eu/art-4-gdpr/

ガイドライン案では「個人データを第三者に閲覧されないうちに全てを回収した場合は、漏えいに該当しない」とありますが、「全てを回収」の意味するところが明確ではありません。ユーザーのシステム設定ミスなどにより意図せず個人データが閲覧可能な状態になっていても、実質的なデータ漏えいに至らないことが多くあります。したがって、ユーザーによる不適切なシステム設定により他人がアクセスできる状態になったとしても、そのようなデータへの不正アクセスの客観的な痕跡がなく、結果的に当該本人に損害を与える危険性が低い場合はデータは「回収された」と認識される、と本箇所に補足することを推奨します。

3-5-3-1 報告対象となる事態 / (4) 個人データに係る本人の数は千人を超える漏えい等が発生し、又は発生したおそれがある事態 (＊2) (*3)

本ガイドライン案では、報告すべき漏えい等が発生したおそれがある事例を挙げています。上記同様、漏えい等が「発生したおそれがある」事態は、「その時点で知り得た事実と、個人情報取扱事業者の過去の経験、知見、セキュリティ対策等に基づく判断により、合理的に高い確実性が認められる場合」とすることで、ガイドライン案をさらに改善することができます。
上記のように、報告・通知をステークホルダー全員にとって意味のあるものにするために、ガイドライン案では、(*3)の（ア）から（エ）の場合であっても、その漏えい等により、利用可能な個人情報への不正アクセスが発生し、当該本人に重大な危害が及ぶ可能性が低い、あるいは無い、と事業者が判断した場合には、報告の対象外とすることを明確に記述することを推奨します。

3-5-3-5 委託元への通知による例外

また、ガイドライン案には、特定の状況下では、「速やかな」通知とされる標準的な 3-5 日以上に通知にかかる可能性があることを明示的に認識することを推奨します。例えば、委託先が再委託している場合に、再委託先のシステムでデータの漏えいが発生した場合、委託先は漏えいの通知をするのに適切な情報を確認するために、通知すべき漏えいを委託元に知らせるための標準的な 3-5 日以上の時間を要する場合があります。このような場合には、標準的な 3-5 日の期間を延長することが適切な場合があることをガイドライン案にて認識することを奨めます。

[外国にある第三者への提供編] 5 同意取得時の情報提供 / 5-2 提供すべき情報 / (2) ②「当該外国における個人情報の保護に関する情報」

個人データの国際的な移転が可能になることは、あらゆる規模や産業分野の企業にとって極めて重要です。ガイドライン案では、国際的なデータ移転に関し、一定の情報を本人に提供するという改正個人情報保護法により課せられた要件を記しています。

ガイドライン案では、提供先の第三者が所在する外国の個人情報保護制度について、本人に提供すべき情報の例が挙げられています。しかし、このような方法では、企業ごとに異なる情報が提供され、本人の混乱を招き、結果的に個人情報の利用に支障をきたすことになるのではないかと我々は懸念しております。従って、外国の個人情報保護制度に関する情報が、貴委員会が貴委員会のウェブサイトで提供する情報に基づいて提供されることを推奨します。

また、ガイドライン案では、(エ)「本人の権利利益に重大な影響を及ぼす可能性のある他の制度の存在 」を含む、提供すべき情報の範囲を特定しております。そのような影響を与える可能性のある制度として記されている二つの事例について、以下、意見を述べます。

事例１）では、「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」と記されていますが、この例では、何が「広範な情報」また「政府による情報収集活動」に分類されるのかが明確でないため、いくつかの不明確な点があります。

事例 2）では、「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」と記されています。しかし、「国内保存義務」と「消去等の請求に対応できないおそれがある」との関連が、ガイドライン案では明確になっていません。

「その他重大な影響を及ぼす可能性のある制度」に関連してガイドライン案の規定を実施するにあたっては、「国の法律により、企業が消去等の請求に応じたり、消去実施をすることが禁止されている場合」と記すなど、本人の消去請求に事業者が応じられない事態に焦点を当てて記述することを奨めます。

[通則編] 3　個人情報取扱事業者等の義務/ 3-8 / 3-8-5 保有個人データの利用停止等 / 3-8-5-1 利用停止等の要件　(3) ③当該本人の権利又は正当な利益が害されるおそれがある場合

貴委員会は「当該本人の権利又は正当な利益が害されるおそれがある場合」として、ダイレクトメールの送付を受けた本人が、送付の停止を求める意思を表示したにもかかわらず、個人情報取扱事業者が応じない例を挙げています。

このような停止請求を受け、それに従うべき適切な事業者（本人が停止請求を送るべき相手）は、メール送付を決めたことに責任を負う事業者であり、メール送信のみに責任を負う第三者の仲介業者やメールサービスではないことをガイドライン案において明示することを推奨します。これは、第三者である仲介業者やメールサービスは、メール送付を決めた事業者の指示に従い、実施することになるからです。

結語

BSA は、ガイドライン案に意見を提出する機会に感謝します。本提言が、新たな要件をより明確にするために、ガイドライン案を修正し、今後、Q&A を策定する上での貴委員会の引き続きの検討に有用であれば幸いです。ガイドラインの策定において、貴委員会が複数のステークホルダーを関与させ、進捗状況を共有する過程をとって頂いたことに感謝致します。本意見に関して、ご質問がある場合又はより詳細に議論をされたい場合には是非ご連絡下さい。