

個人情報保護委員会殿

# 個人情報保護法の3年ごと見直し に関する意見

2023年12月21日

**JEITA** 一般社団法人  
電子情報技術産業協会

- 現行の個人情報保護法は事業者の視点から見て、個人の権利利益の保護と個人情報の有用性への配慮において非常にバランスの取れた法制度となっています。また、個人情報保護法ガイドラインやQ & Aにおける充実した情報提供につきましても、大変に有難く活用しています。このような方向性を維持して頂くことを希望いたします。
  
- 次頁以降、下記の2項目について意見を述べさせていただきます。
  - 1. 政令、規則、またはガイドラインを通じて明確化をお願いしたい事項
  - 2. その他、個人情報保護委員会へのご要望事項

## ○事業者の守るべき責務の在り方

### ■ 個人データの漏えい等の報告義務

- 法第26条において個人情報保護委員会殿への報告及び本人への通知が義務化され、報告対象となる事態は委員会規則において4つ明示されている。そのうち、「不正の目的によるおそれがある漏えい等」については、漏えいしたデータ項目や件数が極めて限定的な場合など、事案によっては個人の権利利益を害するおそれ大きいとは必ずしも整理できない場合もあり、現状一律に報告対象とされているのは事業者側の負担が大きいため、一律に報告対象とするのではなく、下記のような一定の条件を付けることの検討をお願いします。
  - 「不正の目的によるおそれがある漏えい等」については、漏えいした個人データが「氏名」や「公にされている個人情報」に限定されており住所・電話番号・メールアドレス等の連絡先を含まない場合は、一定件数を超える漏えい等とする。
- また、報告対象となる4つの事態には、それぞれ「又は発生したおそれがある事態」という報告対象が追加されていますが、「発生したおそれがある」か否かは事業者での判断が難しく、また続発するサイバー攻撃において「おそれのある事案」をすべて報告することは、事業者に過度の負担が生じる可能性があります。ガイドラインには「個別の事案ごとに蓋然性を配慮して判断する」とありますが、「おそれのある事態」において実際に「漏えい等事案」となったケースは非常に少ないと考えられますため、個人データの漏えい等がほぼ確実になった段階で報告する等、「おそれのある事案」の定義に関して、個人の権利利益へのリスクと事業者の負担とのバランスを考慮した見直しをお願いします。

## ○事業者の守るべき責務の在り方

### ■ 委託先の監督義務

- 事業者が委託先の監督を行うにあたっての、標準的な委託契約条項の記載例をガイドライン等で示すことの検討をお願いします。

### ■ 外国にある第三者への提供の制限

- 外国の提供先がいわゆる「体制整備」を行っていることを担保する方法の1つに契約がありますが、上記と同様に、標準的な契約条項の記載例をガイドライン等で示すことの検討をお願いします。
- また、ガイドラインQ&A7-53に「クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことはない」とありますが、個人データを取り扱わないこととなっている場合に該当する（させる）ための標準的な契約条項の記載例や、適切なアクセス制御例を具体的にガイドライン等で示すことの検討をお願いします。
- 但し、記載例はあくまでガイドラインであり、契約文言が全く同一でなくても良く、民間の自主的な取組を尊重していただく方向での記載としていただきたく、よろしくをお願いします。

## ○事業者による自主的な取組を促す仕組みの在り方

### ■ PIA（プライバシー影響評価）の努力義務規定化

- 最近のプライバシー問題はレピュテーションリスクであると同時に、最終的には法令リスク（個人情報保護法違反）となるケースが多く、個人情報保護法違反を防止するためにPIA制度を自主的に導入するケースも増えています。また、PIAは安全管理措置としても有効な措置であることを明確にするためにも、対象案件を限定した上で、努力義務規定化することが望ましいと考えます。

### ■ DPO（データ保護責任者）設置の努力義務規定化

- 現在、海外の多くの個人情報保護法令においてDPO（GDPRにいうDPOではなく、一般的な意味でのDPO）の設置が義務規定化されており、個人情報の保護と管理においてはこのような個人情報保護実務専門家の設置が必要不可欠になっています。国際間でのハーモナイズされた法令遵守や、事業者における個人情報保護と管理の強化を実現するためには、対象事業者や事業分野を限定した上で、DPO設置を努力義務規定化することが望ましいと考えます。

### ○AI等の新技術への対応の在り方

#### ■ 生成AIサービスへの個人データ入力

- 個人情報保護委員会殿の「生成AIサービスの利用に関する注意喚起等」（2023年6月）にも関連しますが、事業者が他事業者の生成AIサービスを利用し、当該サービスに個人データを含むプロンプトを入力する場合、どのようなケースが第三者提供に当たり、どのようなケースが委託に当たるのかについて、事業者におけるAI利用を促進するためにも、以下も含め、ガイドラインやQ&Aでの明確化をお願いします。
  - 上記の注意喚起において「（入力したプロンプトに含まれる）個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合」は、第三者提供に当たるのかどうか。
  - 上記において「個人データが当該プロンプトに対する応答結果の出力」の目的のみで取り扱われる場合は、委託に当たりうるのかどうか。
- また上記と関連して、生成AIサービスに個人データを含むプロンプトを入力する場合、（ガイドラインQ&A7-53との関連で）第三者提供や委託に当たらないケースがありうるのかについて、ガイドラインやQ&Aでの明確化をお願いします。

## ○AI等の新技術への対応の在り方

### ■ プロファイリングによって推測された個人データの位置付け

- 事業者の内部で、いわゆるプロファイリングを通じて既知の個人データから新たな個人データを推測すること（例えば、就職希望者のサイト閲覧履歴等から内定辞退率を算出して個人のプロフィールに追加することや、宗教に関する書籍の購買履歴等から当人の信仰を推測して個人のプロフィールに追加すること）が「個人データの取得」に該当するか否かについて、諸説がありますが、AI時代にプロファイリングの利用拡大が予想されるため、事業者における利用環境を整備するためにも、個人情報保護法またはガイドライン等において明確化をお願いします。

### ■ 生成AIが出力した個人情報の取扱い

- 生成AIが出力した内容に個人情報が含まれる場合、事業者はその個人情報をどのように取り扱うべきか（例えば、どのような場合に個人データに該当し個人データとして保護しなければならないか、出力内容に含まれる個人データの正確性をどのように確保したらよいか等）について、ガイドラインやQ&Aにおいて明確化（または論点整理）をお願いします。
- 事業者の義務が強化される可能性がある場合には、技術面や運用面について事業者に十分にヒアリングを行って頂くことを希望いたします。

## ○AI等の新技術への対応の在り方

### ■ 学習済みモデル（生成AIを含む）の学習時における公開情報の扱い

- 学習済みモデル（生成AIを含む）の開発に当たって、Web上で公開されている個人情報については（要配慮個人情報を除き）利用目的を公表していれば、学習データとして取得および利用することができると考えられますが、事業者におけるAI開発を促進するためにも、そのような解釈についてガイドラインやQ&Aでの明確化をお願いします。
- また、要配慮個人情報についても、法第20条第2項（7）では「当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、第57条第1項各号に掲げる者その他委員会規則で定める者により公開されている場合」は本人同意なく取得が可能とされ、ガイドラインでその範囲が列挙されています。Web上で公開されている要配慮個人情報について、どのようなWebサイト（例えばWikipedia等）で公開されているものであれば、本人同意なく（利用目的の公表により）学習データとして取得および利用することができるかについて、ガイドラインやQ&Aでの明確化をお願いします。



### ■ 日EU間・日英間のデータ越境移転

- 個人情報保護委員会殿の「日EU相互認証に係る第1回レビュー完了に関する共同プレス声明」（2023年4月）でも言及されていますが、令和3年改正において学術研究分野や公的部門にも個人情報保護法の対象および個人情報保護委員会の所管範囲を拡大したことを踏まえ、日本に対するEU（および英国）の十分性認定の範囲をこれらの分野・部門にも拡大するよう働きかけをお願いします。

### ■ CBPR等のグローバルなデータ越境移転ツール

- 海外では、日本と同様、個人情報保護法令において個人データ越境移転を規制する国（中国、韓国、台湾、シンガポール、タイ、フィリピン、マレーシア、インドネシア、ベトナム、オーストラリア、ロシア、カナダ、メキシコ、ブラジル等）が増えています。これらの国からのデータ移転を十分な保護レベルを確保しながらスムーズに行えるよう、Global CBPR（越境プライバシールール）への参加国を増やすとともに、データ越境移転においてCBPRを活用する方策の検討をお願いします。具体的には、日本の個人情報保護法ガイドラインと同様、各国のデータ越境移転を規制する法令やガイドラインに、CBPRを用いた移転方法を明示してもらえよう働きかけをお願いします。
- また、CBPR認証とEUの認証制度の相互運用性や、各国・地域の標準契約条項（SCC）・モデル契約条項の相互運用性など、グローバルなデータ移転ツールのハーモナイゼーションに向けた働きかけをお願いします。

### ■ 個人情報等の情報区分

- 現行の個人情報保護法では個人情報等の情報区分（個人情報、個人データ、保有個人データ、個人識別符号、要配慮個人情報、仮名加工情報、匿名加工情報、個人関連情報）が非常に多く、またそれらの関係が複雑化しているため、事業者内部での個人情報等の情報分類や管理業務は複雑化しており、多大な管理負担が生じています。また、個人情報等の情報区分の関係が複雑であることから、個人情報等の適正な管理が難しくなり、結果として個人情報保護違反のリスクが潜在的に発生する可能性もあります。そのため、新たな情報区分の定義や創設は回避して頂くようお願いします。