2020 年 8 月 11 日

経済産業省商務情報政策局情報経済課 御中

一般社団法人 電子情報技術産業協会
法務・知的財産部会
個人データ保護専門委員会

「DX 企業のプライバシーガバナンスガイドブック ver1.0（案）」に対する意見

本ガイドブックは、Society5.0 の実現に向けて企業がデータの高度な利活用を進める上で、プライバシー保護を従来のようなコンプライアンス（コスト）として捉えるのではなく、自社の製品・サービスの社会的信頼を獲得し、企業価値を高めるための重要な経営戦略として捉えることと、そのための体制や仕組みづくりを可能とするものであり、大変に時宜を得たものと認識しています。

当委員会では、本ガイドブックを企業にとってより一層使い勝手のよいものとするために、以下の 14 項目について意見を述べさせていただきます。

今後、本ガイドブックの普及啓発を進めていただくとともに、企業実務上の意見や国内外の環境変化を継続的にガイドブックに反映していただければ幸いです。

■意見１
・該当箇所
全体

・意見内容
本ガイドブックでは、プライバシー保護は、個人情報保護法で守られるべき範囲の外側も含めての配慮が必要と説明されており、この点については理解できるが、個人情報保護法の中身や精神とリンクさせた説明が（例えば、利用目的、告知、問合せ対応といった観点で）記載されていると、より分かりやすい。

・理由
個人情報には必ずしも該当しない、パーソナルデータに関する情報の取り扱いが主になるであろう今後のデータ事業において、現行法との関係記載は重要な拠り所になると考えるため。

■意見２
・該当箇所
全体

・意見内容
本ガイドブックが対象としている事業者の範囲を明確にしてほしい。Business Contact 情報等、プライバシー保護の対象から外れる個人情報のみを取扱っている事業者については、個人情報保護法を遵守すればよく、本ガイドブックの対象ではないことを明確にしていただきたい。

・理由
Business Contact 情報等、プライバシー保護の対象から外れる個人情報のみを取扱っている事業者については、個人情報保護法を遵守すればよいため。

■意見３
・該当箇所
全体

・意見内容
現在ポピュラーになりつつあるデータ事業における以下の観点を、今後のバージョンアップの際に記載していただきたい。
① AI 機械学習時の留意観点
② データ売買時の留意観点
③ 海外事業者との取引での留意観点

・理由
商談成立前後は、法律（契約）で管理することができるが、案件アプローチ進行過程での現場への理解促進の意味からも上記観点は重要な知見と考えるため。

■意見４
・該当箇所
「1.　本ガイドブックの位置づけ」
「2.　ガイドブックの前提」
「4.5 その他のステークホルダーとのコミュニケーション」

・意見内容
DX においては、クラウドベースによるサービスの開発提供やクラウドリソースの戦略的利活用が不可欠である。そこで、クラウド利用におけるプライバシーガバナンスについて言及すべきと考える。よって冒頭総論部分にクラウド利用を推進しリソース配分を適

切に図る現代においては、それに合わせたプライバシーガバナンスのアプローチが求められていることを追加すべきと考える。

また案文の「4.5」は、経済産業省が「2025 年の崖」とも指摘している、従来型のシステム開発委託を念頭に置いたと思われる記述であるため、これを改め、クラウドを利用した場合のいわゆる「責任共有モデル」等と言われる責任分担についても言及し、DX とクラウド利用におけるプライバシーガバナンスについて述べるべきと考える。その場合、データ処理基盤を提供するクラウド事業者が、直接プライバシーにかかわるデータを取り扱わない場合において、クラウドを利用する側の企業がクラウドにおけるプライバシー保護について責任を負うことを明示すべきと考える。また、責任分担の一環として、クラウド事業者側は、クラウド利用者がサービス上の情報を保護するための機能や情報を提供することが望ましいこと、クラウド事業者側のセキュリティについて第三者評価を実施するなどして説明責任を果たすこと、等についても言及されると、クラウドにおける責任共有の考え方が更に明確になると考える。また、こうした修正は、後述の経済産業省の DX レポート及び個人情報保護委員会の方針等にも沿うものと解される。

・理由

1．経済産業省のもとに置かれたデジタルトランスフォーメーションに向けた研究会の「DX レポート」（平成 30 年）などを始めとして、経済産業省の DX 資料には、DX におけるクラウド利活用の推進が明記されており、プライバシーガバナンスにおいてもクラウドを念頭においた言及があるべきと考える。

2．個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関する Q&A」（平成 29 年、令和元年更新）の Q5-33 以下にも、特定の条件を満たす場合、クラウドの利用は個人情報保護法第 23 条の「提供」に該当せず、その場合には、クラウドサービスを利用する事業者側において、自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる必要がある旨説明されている。

3．総務省「IoT・５G セキュリティ総合対策 2020」9 ページ等においても、「クラウドサービスのセキュリティは一般的に『責任共有モデル』が採用されており、クラウドサービス提供者と利用者・調達者の共通の認識の下、それぞれの管理権限に応じた責任分担を行うものである。そのため、クラウドサービス提供者と利用者・調達者は、それぞれの役割を適切に果たすことで、クラウドサービスに関するセキュリティリスクを最小化するために、共に協力することが望ましい」とある。

以上より、クラウドにおける「責任共有」の考え方はプライバシーガバナンスにおいても不可欠となっており、「DX 企業のプライバシーガバナンスガイドブック」においても言及されるべきものと考える。

■意見５

・該当箇所

5 ページ

「機械学習は、静的に記述されたルールではなく、既存状況のデータを統計的に処理したモデルを通じて、対象に関する推定や判断をすることから、新規の対象には対処できず」

・意見内容

人間による推定や判断についても上記と同様なことが言えるのに、AI の機械学習に対しては「新規の対象には対処できない」と言い切る表現に違和感がある。

・理由

企業の取り組みを支援するガイドブックに馴染まないと思われるため。

■意見６

・該当箇所

10 ページ図表 3、18 ページ図表 6 等、全般

・意見内容

「個人情報保護」と「プライバシー保護」の包含関係を明確に整理・定義していただきたい。個人情報保護の一部はプライバシー保護の領域に包含されていないように図示されていが、包含されない事項があれば具体的に示していただきたい。

・理由

個人情報保護の一部はプライバシー保護の領域に包含されていないように図示されているが、図表 3 においては、個人情報保護とプライバシー保護全体「事業者が配慮すべき範囲」、図表 6 においては、個人情報保護とプライバシー保護全体をプライバシー関連としており、企業経営者等にとって、このガイドブックの対象範囲の特定が難しいと思われるため。

■意見７

・該当箇所

15 ページ

・意見内容

ガイドブックの15ページにアカウンタビリティの重要性についてコメントが記載されているが、概要版にもアカウンタビリティの重要性に関してコメントを記載いただきたい。

・理由
GDPR第5条などにもアカウンタビリティが定義されており、グローバルな動きとしてもキーワードになっているため。

■意見８
・該当箇所
15ページ
3.1. プライバシーガバナンスに係る姿勢の明文化（プライバシーステートメント、行動原則）に関して

・意見内容
脚注20に、現行よく見られる「プライバシーポリシー」とは異なる旨、記載があり、個人情報保護法との関係が説明されているが、なぜこれでは足りないと示唆されているのかが馴染みにくく、わかりにくい。個人情報保護法の観点に係る「プライバシーポリシー」に加えて、プライバシーステートメントや行動原則をさらに設ける必要性を訴えるにあたっては、それぞれの明文規定の守備範囲（コンプライアンス/アカウンタビリティ）、およびその連動性を示していただき、双方の明文規定を整備しようと考える事業者が参考にできるような規定の体系例を示していただきたい。

・理由
個人情報保護法の外側にある、プライバシー遵守精神の明文化については議論が成熟しておらず、理解が難しいのが現状であると考えるため。

■意見９
・該当箇所
19ページ5行目
「プライバシー保護責任者は、経営者が姿勢を明文化した内容等を踏まえて、実践のための方針を確立し、プライバシーリスクを把握、評価し、対応策を検討できる体制を構築して、方針の実施を徹底する。」

・意見内容
下線部のようにプライバシー保護責任者に明確な権限を付与する旨を追加すべきであ

る。
「プライバシー保護責任者は、経営者が姿勢を明文化した内容等を踏まえて、経営者から委譲された権限に基づき実践のための方針を確立し、プライバシーリスクを把握、評価し、対応策を検討できる体制を構築して、方針の実施を徹底する。」

・理由
経営者は、複数部署の間に立って調整することも求められるプライバシー保護責任者に対して、責任だけでなく権限も付与しなければ、関連部署の協力が得られない場合に機能しなくなるおそれがあるため。図表９からプライバシー保護責任者は事業部等に指示を出す権限があるように読み取ることもできるが、本文にも記載し明確化を図るべきと考える。

■意見１０
・該当箇所
24 ページ以降全般

・意見内容
全般的に「消費者」という表現は「個人」や「データ主体」(GDPR 等で使われている data subject の邦訳)等のような表現に統一していただきたい。

・理由
DX の対象となるパーソナルデータは、B2C 事業の受益者としての「消費者」から収集するケースが多いものの、「従業員」や B2B 事業における「法人顧客」のデータ、さらにはパブリックスペースで収集した「大衆」のデータを活用することもあり、一般的な意味での「消費者」に限定されないため。

■意見１１
・該当箇所
26～27 ページ　消費者とのコミュニケーション

・意見内容
表現が B2C の運用ベースで記載されている。B2B2C の場合での、左端の B の立場（システムベンダー・データ分析企業・ソリューション提供企業等）は、情報オーナーではないため、基本的に直接的な消費者コミュニケーションを取ることが難しいことが想定されるが、その場合であっても例示されている「意識調査」のほかに、そうしたベンダーの立場としての取り得る施策について、具体化していただきたい。例えばベンダーの立場とし

てのプライバシーステートメントを公表していくことは効果的なのか、あるいはそこまでは不要なのかについて、指針をお示しいただきたい。

・理由
　ソリューション提供者＝情報オーナーではないが、その立場としての消費者コミュニケーションに関する指針が不明確であるため。

――――――――――――――――――――――――――――――

■意見１２

・該当箇所
　28 ページ図表 13

・意見内容
　図の左側の「消費者」に向かっている矢印の示す「行為」を明記していただきたい。

・理由
　図中、他の矢印に関しては、ステークホルダーに対する行為が記載されているが、上記に関してのみ未記載であるため。

――――――――――――――――――――――――――――――

■意見１３

・該当箇所
　29 ページ　ステークホルダーとのコミュニケーション

・意見内容
　表現が P26～27 と同様に、B2C の運用ベースで記載されている。取引先コミュニケーションのシミュレーション例示がより具体的に記載され、かつ取引関係のバリエーションを想定した記載があればより良いと考える。

・理由
　ステークホルダーの位置付けの図が B2C ベースであって、B2B2C のモデルとの差異がある。例示されている事例では、プライバシー保護観点の対応に応える技術や説明の充実については取引先（ベンダー）の責任とされており、発注側企業はそれを要求するにとどまるケースのみが記載されているが、取引形態によっては、どのような技術や説明ツールを備えるべきかを、発注側企業が仕様としてベンダーに指定する一次責任を負うケースもあるのではないかと考えるため。

――――――――――――――――――――――――――――――

■意見１４

・該当箇所

32～33 ページ

・意見内容

「データの再提供」という表現があるが、図表 15 を見る限り、単に A 社から B 社にデータを提供するだけであるから、「データの提供」という表現の方が適切である。

・理由

個人情報保護法における表現に合わせた方が、読者が理解しやすいため。

（以上）