左より、岡本直己弁護士、吉良一真弁護士、今枝史絵弁護士、堀部道寛弁護士、田中瑞紀弁護士、髙木佑衣弁護士。

読者からの質問に答える！

生成AIサービス利活用上の個人情報の取扱いに係るリスクとその対応

弁護士法人御堂筋法律事務所
今枝史絵　岡本直己　髙木佑衣　田中瑞紀　堀部道寛　吉良一真

生成AIサービスの利活用にあたっては事前のリスク分析が不可欠

事業において生成AIサービスを利活用する場合、個人情報の不適正な利用、秘密情報の漏洩、知的財産権の侵害、ハルシネーション、バイアスによる不適切情報の生成等、さまざまなリスクが生じる可能性が存在し、政府が国内のAI（人工知能）政策の司令塔として立ち上げたAI戦略会議においても、個人情報、機密情報に関するリスクを筆頭に、七つのリスクが挙げられている。このうち、特に、近時の事業環境を踏まえた個人情報・プライバシーに関連するリスクについて、弁護士法人御堂筋法律事務所の今枝史絵弁護士、堀部道寛弁護士は次のとおり指摘する。

「個人情報保護法との関係では、利用目的規制や第三者提供規制等の検討が欠かせません。たとえば、児童の学習内容等をAIがデータ分析のうえ、個々の児童に最適な問題を提示すること等を謳った学習支援業や、体形サイズ等を瞬時に計測してデータを分析しパーソナライズされたファッションアドバイスを提供して購買につなげる事業、さらには、B to Cの企業に限らず、従業員の離職原因となる要素を分析し採用に役立てるためのサービスといったさまざまな事業や場面で個人情報が生成AIサービスによって分析、学習され、利用されるようになってきています」（今枝弁護士）。

「開発段階やサービス導入初期の段階に、当該事業や利用方法に応じた具体的なリスクを分析したうえで対応しておかなければ、当初意図していなかった範囲まで個人情報が分析、学習され、利用されてしまう事態が生じかねず、そうなれば、サービス提供事業者やサービス利用事業者が個人情報保護法違反等に問われたり、レピュテーションの低下等の信用問題に至ったりするリスクを抱えてしまう可能性があります」（堀部弁護士）。

同意取得の要否が分かれる“委託に伴う提供”該当性

生成AIサービスの利活用の形態として、たとえば、顧客の属性等に応じてパーソナライズされた出力結果を得るため、第三者である生成AIサービス事業者が提供している生成AIサービスに、当該顧客等の個人情報が含まれる情報等を入力するケース（プロンプトに個人情報が含まれるケース）が想定されるが、このような場合に個人情報保護法との関係で生じるリスクについて、吉良一真弁護士は次のとおり説明する。

「このケースでは、生成AIサービスへの個人データの入力行為が、AI提供者に対する“個人データの第三者提供”に該当すると評価される可能性があります。この場合、個人情報保護法上、原則として個人データの本人から同意を取得したうえで生成AIサービスに個人データを入力しなければならない一方で、個人データの取扱いの“委託に伴う提供”に該当すると整理できれば、本人からの同意の取得は不要となります。“委託に伴う提供”といえるか否かは、当該個人データの取得時に特定する利用目的や、その生成AIサービスにおいて入力された情報の取り扱われ方（たとえば、モデルの学習に使用されることがないか）等の事情を踏まえ、個々の事案に即して検討、判断されますので、生成AIサービスの利活用の具体的な態様についての検討が必要不可欠です」（吉良弁護士）。

また、ChatGPTに代表されるように、生成AIサービスの提供者は海外の事業者であることが多いが、そのような海外事業者の提供する生成AIサービスを使用する場合には別途注意が必要であると、髙木佑衣弁護士は指摘する。

「個人情報保護法上、“外国にある第三者”に対して個人データを提供するときは、“委託に伴う提供”にあたる場合であっても、原則として、本人からの同意の取得が必要になります。同意を取得せず、あるいは同意取得の例外となる法令に基づく要件を充足することなく第三者提供を行った場合、個人情報保護委員会による指導・助言や勧告、ひいては命令の対象となるおそれがありますので、慎重な検討、対応が必要です」（髙木弁護士）。

生成AI“サービス”のメリットを享受するためのリスク対応

このように、事業者が生成AIサービスを利活用して事業活動を展開するうえでリスクは不可避ともいえるが、その対応策について、田中瑞紀弁護士は以下のように指摘する。

「昨今、生成AIサービスを利用する事業者においては、社内ガイドライン等の社内ルールを整備する動きがさかんになっています。社内ルールを策定する際には、各従業員の適切な生成AI利用のための指針とするため、事業者において、AI利用を促進する目的や、AI利用を可能とする範囲、実際の事業活動との関係で手当てすべきリスク等を具体的に検討し、個人情報保護法をはじめとする法令上のリスクにとどまらず、自社の事業に生じうるリスクを把握し、たとえば顧客ごとにパーソナライズされた販促案内を生成・送信する場合には“生成物に誤情報や個人情報が含まれていないか”等のチェック体制を規定する等、的確にカバーする内容にすることが肝要です」（田中弁護士）。

生成AIサービスの利用にはさまざまなリスクが存在するが、一方で生産性の向上をはじめ、さまざまなメリットも享受できる可能性もあり、昨今の事業環境において、競争力を左右すると言っても過言ではないといえる。開発段階やサービス導入当初といった初期の段階に、各事業者の具体的な事業活動や利用方法を踏まえ、リスクを慎重に分析し、個別的な対応を進めることが欠かせない。

読者からの質問

Q **生成AIに対する各国の法制度がまちまちである状況ですが、グローバル企業として、社内ルールの整備等にどのように取り組んでいくべきでしょうか。**

A グローバルな事業展開をしている事業者においては、“事業展開をしている国・地域で実際にどのような規制の適用を受けるのか”という視点が必要です。特に、個人データの取扱いに関しては、主たる生成AIサービス事業者がいずれも海外事業者であることや、域外適用のある海外の個人情報保護規制が多く存在することも相まって、規制の適用関係が複雑になりやすい傾向にあり、より慎重な検討が必要不可欠です。国・地域ごとに異なる生成AIに対する法規制を理解しこれを遵守するためには、当該規制を敷いている国・地域の法律事務所の助言を得ることが有用ですので、生成AI法制や個人情報保護法制に知見を有する海外法律事務所とのネットワークが期待できる国内法律事務所をハブとして起用し、その日本における実務への十分な理解と海外法務の対応力を活用して社内ルールの整備を図ることをお勧めします（岡本直己弁護士）。

連絡先
弁護士法人御堂筋法律事務所
〒542-0081 大阪府大阪市中央区南船場4-3-11 大阪豊田ビル2階
TEL：06-6251-7266　FAX：06-6245-5520
E-mail：info@midosujilaw.gr.jp　URL：https://www.midosujilaw.gr.jp/
主事務所の所属弁護士会：大阪弁護士会