innoventier Power for the Business 弁護士法人イノベンティア

企業法務相談室

〈第78回〉 弁護士 秦野（はたの） 真衣（まい）

2010年京都大学法学部 卒業、2012年3月京都大学大学院法学研究科法曹養成専攻修了、同年司法試験合格。2013年に弁護士登録（大阪弁護士会）し、国立大学法人におけるインハウス弁護士としての勤務を経て、2019年12月から弁護士法人イノベンティアに勤務。

今回のご相談

生成AIを利用してメール等の文書の下書きや、マーケティングのための顧客分析などを行いたいと考えていますが、個人情報保護法との関係が心配です。生成AIに個人情報を読み込ませることで、個人情報保護法に抵触する恐れはないでしょうか。

生成AIと個人情報について

一．はじめに

生成AI（Generative AI）は、画像や文章といったコンテンツを生成できる人工知能のことをいいます。近時、ChatGPT等の生成AIを業務に導入する動きが一部の企業や地方自治体等において進んでいることは報道されている通りですが、利用の方法によっては、個人情報保護法上の問題が生じえます。

例えば、生成AIの業務利用として考えられるものとして、カスタマーサポートやメールの自動作成、社内資料の要約等も考えられます。これらの場合、顧客や取引先の個人情報が中に入っている、ということは十分ありえるところです。

また、より高度な利用の方法として、顧客データ、購買履歴や属性データを分析させて、マーケティングに用いることなども考えられます。

生成AIに入力された個人情報を含む指示については、その内容が当該AIの学習に利用されることにより、意図しない形で、第三者への回答に反映される可能性があり、世界的にプライバシーの侵害につながるとの懸念が広がっており、実際にも、イタリアでは、三月末から約一か月間、ChatGPTの使用を禁止しています。

上記事情を背景とし、個人情報保護委員会は、生成AIサービス利用者及び生成AIサービスの提供事業者に対し、注意喚起（以下、「本件注意喚起」といいます。）を行いました。

二．生成AIサービスの利用に関する注意喚起等①利用目的ルールの遵守

本件注意喚起では、生成AIへの個人情報入力につき、「特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること。」と述べられており、これは、個人情報保護法上の利用目的に関するルールを遵守すべきことを改めて示したものであると考えられます。

同法上、個人情報は、取得の際にきちんと利用目的を特定せねばならず、また、特定した当該利用目的の範囲内でしか利用できないこととなっています（法一七条、一八条一項）。更に、特定された利用目的は通知・公表する必要があり（法二一条）、当初の利用目的と関連性を有すると合理的に認められる範囲を超える利用目的の変更は本人の同意が必要とされています（法一八条二項）。

生成AIサービスに個人情報を入力する行為も、個人情報の利用の一場面であり、生成AIへ個人情報を入力する場合、それが当該個人情報の利用目的の達成のために必要な範囲内と言えるか、確認が必要となります。

具体的に、どのような場合に利用目的の達成のために必要な範囲内と言えるのかは、本件注意喚起には記載はありませんが、近時、個人情報保護法ガイドラインにおいて、プロファイリング等の処理技術の出現を背景に、利用目的の特定については、「本人が、自らの個人情報がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できないような場合は、この趣旨に沿ってできる限り利用目的を特定したことにはならない」と明記されたことは参考になるものと思われます。

同ガイドラインによると、例えば、個人情報から、本人に関する行動・関心等の情報を分析する場合、どのような取扱いが行われているか（処理の方法）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こととされています（通則編三―一―一）。

これをもとにすると、生成AIサービスに個人情報を入力し、本人に関する行動・関心等の情報を分析する場合についても、利用目的において、「分析」を行う旨を明らかにしておく必要があると考えられます。

三．生成AIサービスの利用に関する注意喚起等②当該生成AIサービスを提供する事業者が、当該個人データを機械学習に利用しないこと等の確認

（一） 本件注意喚起の内容

本件注意喚起では「あらかじめ本人の同意を得ることなく生成AIサービスに個人データを含むプロンプトを入力し、当該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」につき、個人情報保護法違反になる可能性があるとし、入力にあたっては「当該生成AIサービスを提供する事業者が、当該個人データを機械学習に利用しないこと等を十分に確認すること」が求められています。具体的に個人情報保護法のどの規定に違反するのかについてははっきりとした記載はありませんが、第三者提供規制を示唆したものと考えられます。

（二） 個人情報保護法の第三者提供規制

前提として、個人情報保護法の第三者提供規制を概観しますと、まず、個人データを第三者に提供する場合は、原則として、本人の同意が必要となります（法二七条一項）。また、海外の第三者に提供する場合は、原則として、本人に対して国名や当該外国の制度といった情報をあらかじめ提供する必要があります（法二八条一項）。

ただし、これにはいくつかの例外があり、例えば、国内の場合、個人データの取扱いの委託に伴う提供の場合には、例外的に同意は不要とされています（二七条五項一号）。

また、いわゆる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にはならないとされています（「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 Q7―53）ため、「提供」にすらあたらないと考えられています。

（三） 機械学習の学習用データセットとしての用いる場合

以上を前提に、生成AIサービスの提供を行う事業者が、入力された個人データを機械学習の学習用データセットとして用いる場合を検討してみます。

まず、学習用データセットとして用いていることから、「個人データを取り扱わないこととなっている場合」には該当しません。

また、入力を行った者からの委託に伴った利用、すなわち「応答結果の出力」を越えて、生成AIサービス事業者固有の目的である機械学習に個人データを利用していることから、「委託」の範囲も越えて「第三者提供」にあたる可能性が高いものと思われます。従って、この場合は、本人の同意が必要と考えられます（法二七条一項。なお、生成AIサービスの提供を行う事業者が海外法人である場合は、上述の通り、「委託」に該当するか否かにかかわらず、原則として同意（法二八条一項）が必要となります。）。

生成AIサービスが入力された個人データを機械学習の学習用データセットとして用いているかどうかについては、当該サービスの利用規約を確認して判断することとなります。サービスによっては、機械学習への利用を設定の変更により止めることが可能となっているものもあるため、事前によく確認しておくことが重要です。

四．おわりに

以上より、本件注意喚起によると、生成AIサービスに個人情報を入力する際には、当該個人情報の利用目的を確認すること、及び、当該生成AIサービスの利用規約を確認し、第三者提供に該当し同意が必要とならないかを検討することが必要と考えられます。

社内業務の利用においては、セキュリティ面の基準や入力してもよいデータなどを整理したマニュアル等を整備したうえでの利用とすることが望まれます。 Ⓡ