M&P Legal Note 2024 No.1-1

生成 AI と個人情報

2024 年 1 月 12 日
松田綜合法律事務所
弁護士　木舩 恵

1　生成 AI と個人情報

生成 AI を含め AI にはデータ学習が必要になります。AI は、大量のデータを学習することで、より正確なデータ予測、生成が可能になります。そのため、AI の開発場面においては、大量のデータが必要になります。

また、社外の事業者が提供する生成 AI を利用する場合においては、利用者が意図した情報が得られるように適切なプロンプトを入力する必要があります。

以下では、生成 AI の開発場面と利用場面における個人情報保護法（以下「個情法」といいます。）との関係について、現時点での留意点について記載します。

2　生成 AI の開発場面

学習データを収集する際、もっとも問題になり得るのが、個人情報との関係においてです。個情法においては、「個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない」（個情法 20 条 1 項）と規定されています。そのため、個人情報であっても要配慮個人情報に該当しない限り、個人情報を含むデータの取得について、本人の同意は不要とされています。

しかしながら、個情法 21 条 1 項においては、「個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。」と規定されているため、個人情報を取得するのであれば、原則としてあらかじめ利用目的を公表しておくことが求められます。

また、要配慮個人情報[1]については、個情法 20 条 2 項各号の場合を除き、本人の同意を得ないで取得することが認められていません[2]。

---

[1] 要配慮個人情報とは、「人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」（個情法 2 条 3 項）をいいます。

[2] 個人情報保護委員会は、OpenAI 社に対して、令和 5 年 6 月 2 日、あらかじめ本人の同意を得ないで ChatGPT の利用者から要配慮個人情報の取得を行わないよう注意喚起を行っています。

したがって、現行の個情法のもとにおいては、AI の学習のために収集するデータに要配慮個人情報が含まれているか否かにより、本人の同意の有無を判断する必要があります。

3　生成 AI の利用場面

生成 AI から利用者が意図した情報を取得するためには、適切なプロンプトの入力が不可欠です。他方でプロンプトの入力場面においては、個情法との関係で、以下の点に留意する必要があります。

まず、社内のみで運用される生成 AI（スタンドアローン AI などと呼ばれることがあります。）については、クラウドサービスを含め外部の事業者にデータを移転することなく、社内の物理的なインフラストラクチャー内で必要な計算やデータ処理等を行うため、適切に取得した個人情報をプロンプトに入力することについて、取得時の利用目的に沿うものである限り、個情法違反の問題が生じることはありません。

他方で、外部事業者が提供する生成 AI を利用する場合には、その生成 AI は外部事業者が利用するクラウドサービス上で必要な計算やデータ処理が行われることになるため、プロンプトに個人情報を入力する際には、単なる個人情報（散在情報）なのか、それとも個人データに該当するか否かにより個情法の規制が異なります。

まず、個人データとは、個人情報データベース等を構成する個人情報をいいます。個人情報データベースを構成する個人データについては、その個人データの利用が容易になる一方で漏えいの危険性が高まることから、個情法上の様々な規制が適用されることになります。

生成 AI との関係においては、プロンプトに個人データを入力することが個情法上の第三者提供に該当するか否かが問題となります。すなわち、「個人データの取扱いの委託」等の例外規定に該当しない限り、個人データの第三者提供に該当し、本人の同意を取得する必要があります[3]。

個人情報保護委員会においては、令和 5 年 6 月 2 日、「生成 AI サービスの利用に関する注意喚起等」（以下「注意喚起」といいます。）[4]において、「**個人情報取扱事業者が、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、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、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。**」との注意喚起を行っています。この注意喚起の内容からすれば、プロンプトに入力

---

https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf

[3] なお、「個人データの取扱いの委託」に該当したとしても、委託先、すなわち生成 AI の提供元に対して、必要かつ適切な監督を行わないといけないとされています（個情法 25 条）。

[4] https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

した個人データが「**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**」でない限り、本人の同意を得ていなかったとしても個情法違反の問題にならないと反対解釈することができます[5]。この点、OpenAI 社が提供する ChatGPT においては、プロンプトの内容をモデルのトレーニングに利用しない、すなわち、機械学習には利用されないとの設定をすることができます。もっとも、当該設定をしたとしても、OpenAI 社は不正使用の監視のため、プロンプトの内容を３０日間保存するとことなっており、不正使用の監視が「**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**」に該当する可能性が否定できません。そのため、現状においては、プロンプトの内容が ChatGPT のモデルのトレーニングに利用されないとの設定にしたとしても、プロンプトの内容が不正使用の監視のため OpenAI 社に利用される可能性があるため、プロンプトに個人データを入力することは個情法との関係では避けるべきであるといえます。

なお、Microsoft 社が提供する Azure OpenAI Service においては、プロンプトの内容について、不正使用の監視機能をオフにすることが設定上可能となっており、「**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**」には該当しないと判断することが可能になるものと考えます。

４　越境移転の問題

上記したように、プロンプトに個人データを入力したとしても、「**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**」には該当しない場合には、本人の同意を得る必要なく、個人データを入力することができると考えられます。この場合、個情法との関係でいえば、生成 AI を提供する事業者に個人データの取扱いを「委託」していると整理するものと考えます。

もっとも、当該生成 AI を提供する事業者が海外の事業者である場合にはたとえ個人データの取扱いの委託であったとしても、第三者提供の場合と同様に越境移転規制の問題が生じます。個人データの越境移転にあたっては、原則として本人の同意を得ることが必要になり、以下のいずれかに該当する場合に限り、例外的に本人の同意をえることは不要と

---

[5] なお、現時点でクラウド例外との関係については解決されていません。個人情報保護委員会が公表している「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（https://www.ppc.go.jp/files/pdf/2312_APPI_QA.pdf）Q&A７－５３によれば、クラウドサービスに個人データを保存などする場合、当該クラウドサービスを提供する事業者において、「個人データを取り扱わないこと」となっているときには、個人データを提供したことにはならないとの回答が示されています（クラウド例外）。この点、当該回答において示されている「個人データを取り扱わないこと」に生成 AI が回答を生成するためのデータ処理等及び不正使用の監視が含まれているか否か明確にされておらず、実務上も見解が対立しています。そのため、プロンプトに個人データを入力することについては、たとえプロンプトの内容が機械学習に利用されないことが明示されていたとしても「個人データを取り扱わないこと」（クラウド例外）に該当しない可能性が否定できず、個人データの第三者提供に該当する可能性が少なからず残っています。

されています（個情法２８条）。

①提供先の第三者が、日本と同等の水準にあると認められる個人情報保護制度を有している国として個人情報保護委員会規則で定める国にある場合
②提供先の第三者が個人情報取扱事業者が講ずべきこととされている相当措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している場合

現時点で、米国は上記①に該当するとはされておらず、生成 AI を提供する事業者が米国にある場合には、当該事業者とデータ処理契約（いわゆる「DPA」といいます。）を締結し、上記②の要件を満たす必要があります。

５　まとめ

生成 AI を開発・利用する場面では、個情法との関係において、上記の点に留意する必要があります。とりわけ生成 AI を利用する場合、生成 AI を提供する外部事業者において個人データがどのように利用されることになるのか、正確に把握する必要があり、個情法との関係で不安が解消できないのであれば、個人データの入力は避けるべきと考えます。

また、生成 AI については、個情法以外の法律との関係においても様々な問題点があり、各事業者において、適法性を確認することは非常に困難な状況にあります。

他方で多くの場合、生成 AI を利用することにより事業活動を効率化することが可能になり、事業者における生成 AI の利用が拡大していくことは確実であるといえます。生成 AI を事業において利用することを検討している事業者におかれましては事前に弁護士にその適法性についてご確認頂いたほうがよいものと考えます。

この記事に関するお問い合わせ，ご照会は以下の連絡先までご連絡ください。

弁護士　木舩 恵
https://jmatsuda-law.com/members/satoshi-kibune/

info@jmatsuda-law.com

松田綜合法律事務所
〒100-0004　東京都千代田区大手町二丁目１番１号　　大手町野村ビル 10 階
電話：03-3272-0101　FAX：03-3272-0102

この記事に記載されている情報は，依頼者及び関係当事者のための一般的な情報として作成されたものであり，教養及び参考情報の提供のみを目的とします。いかなる場合も当該情報について法律アドバイスとして依拠し又はそのように解釈されないよう，また，個別な事実関係に基づく具体的な法律アドバイスなしに行為されないようご留意下さい。