JETRO
日本貿易振興機構（ジェトロ）

データ三法により作成が義務付けられている重要な法的文書の作成時の留意点

～中国の安全保障貿易管理に関する制度情報専門家による政策解説～

2022 年 12 月

日本貿易振興機構（ジェトロ）
北京事務所
海外調査部

【免責条項】

本レポートは、北京市環球法律事務所に委託し、作成したものです。
本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承下さい。

中国では目下、データ分野の法律として「サイバーセキュリティ法」「データセキュリティ法」および「個人情報保護法」の 3 件（以下、データ三法）が施行されており、関連する附属規定や国家標準も続々と公布されています。こういった状況を受けて、「データ三法および現行の規定や標準に基づき、最低限作成が必要となる基本的なデータコンプライアンスに関する文書や制度にはどのようなものがあるか」という問い合わせが一部の日系企業から頻繁に寄せられています。

本稿では、データ三法および現行の規定や標準に基づき、最低限作成が必要となる基本的なデータコンプライアンスに関する文書や制度について整理します。ただし、紙幅の都合上、本稿では比較的重要度の高い文書や制度のみを取り上げますので、自社が負うべき義務や作成すべき文書および制度等について漏れなく把握したい場合は、自社の状況を踏まえたうえで、自社でより詳細な確認、整理を行うことを推奨します。

1.個人情報保護に関する文書

「個人情報保護法」およびその附属規定、関連国家標準、ならびに当所の実務経験に基づけば、個人情報保護に関し作成が必要となる主な法律文書には以下の 5 種類があります。

a.個人情報取扱規則（プライバシーポリシー）

b.特殊なシーンにおける告知・同意に関する文書

c.個人情報の共同取扱、取扱委託または第三者提供を行う場合において共同取扱者、受託者（委託者）または第三者と締結する、個人情報取扱に関する権利義務について定めた契約書（既存の契約書に条項を追加するケースを含む）

d.個人情報保護影響評価報告書

e.その他、個人情報の内部管理制度に関する文書（例：個人情報安全事件緊急対応策）

このうち、a と b（特に消費者向けの a と b）については、関係当局の注視を惹起しやすいため、作成にあたっては細心の注意を払うことが必要となります。また、d についても、実務において軽視されやすい文書であるため、特段の注意が必要です。そのため､本章では、a、b および d の 3 種類の文書に的を絞って、作成時の留意点を説明します。

（1）個人情報取扱規則（プライバシーポリシー）の作成時の留意点

「個人情報保護法」第 7 条では、個人情報を取扱う場合、個人情報取扱規則を公開しなければならないとされています。消費者等の社外向けの個人情報取規則は、通常ウェブサイトやアプリ、ミニプログラム等のいわゆる「プライバシーポリシー」という形で公開されます。その作成に際しては、以下の 3 つの点に注意を払う必要があります。

（ア） 基本内容および条項の構成

プライバシーポリシーに盛り込むべき内容については「個人情報保護法」第 17 条および「情報安全技術 個人情報安全規範」（GB/T 35273-2020）第 5.5 条等の規定を参考にできます。条項の構成については、現時点の実務状況では、次のものがよく見られます。

a.前文、重要な内容に関する条項

b.個人情報収集、使用の目的、範囲および収集方法に関する条項
c.個人情報の取扱委託、共有、譲渡、公開に関する条項
d.個人情報の保管に関する条項
e.個人情報安全保護措置に関する条項
f.ユーザーの権利に関する条項
g.未成年者の個人情報の保護に関する条項
h.プライバシーポリシーの更新に関する条項
i.紛争解決に関する条項

また、中国国内で収集した個人情報を域外に提供する場合においては、個人情報の域外提供に関する条項をプライバシーポリシーに盛り込み、個人情報の域外提供の目的、範囲、類型および提供先の所在国（地域）等について説明する必要があります。

なお、インターネット上ではプライバシーポリシーの雛形や他社のプライバシーポリシーを目にすることもできますが、あくまで参考に留め、自社の製品やサービスの実際の状況に応じた、適切な内容を盛り込んだプライバシーポリシーを作成する必要があります。

（イ） 記載事項・書き方に関する要求

プライバシーポリシーの記載事項や書き方について、「個人情報保護法」第 17 条では、「目立つ方法、明快かつ分かりやすい言葉で、関連事項を真実、正確、完全に個人に告知しなければならない」とする基本的な方針を示しています。プライバシーポリシーを作成するにあたって、「情報安全技術　個人情報安全規範」（GB/T 35273-2020）等の規定を参考にすることができます。例えば、機微な個人情報については識別マークや強調表示の方法（太字、下線、星印、斜体、配色等）を用いること等の要求が定められています。実務状況でも、機微な個人情報やその他の重点内容については、識別マークを付す、強調表示をする等の方法を用いている事例がよく見受けられます。

（ウ） 同意（一般的な同意）の取得

紙媒体でプライバシーポリシーを提供する場合、ユーザーの署名により同意（一般的な同意）を取得することができます。ウェブサイト、アプリ、ミニプログラム等のオンライン上でプライバシーポリシーを表示する場合、電子署名またはユーザーの自発的な操作（例えば、設置した同意画面において、チェックマークを入れる、「承諾する」「次へ」といったボタンをクリックする等）により同意（一般的な同意）を取得することができます。

（2）特殊なシーンにおける告知・同意に関する文書の作成時の留意点

通常のシーンであれば、上述のプライバシーポリシーによる同意（一般的な同意）を取得すれば足りますが、次の状況を含む特殊なシーンにおいては、「個人情報保護法」の規定に基づき、個人の「個別の同意」を取得する必要があります。

a.その取扱う個人情報をその他の個人情報取扱者に提供する場合（第 23 条）
b.取扱う個人情報を公開する場合（第 25 条）

c.公共の場所に、画像を収集し、個人の身元を識別する機器を設置する場合（第 26 条）
d.機微な個人情報を取扱う場合（第 29 条）
e.域外へ個人情報を提供する場合（第 39 条）

特殊なシーンにおける告知・同意の文書は、プライバシーポリシーとは別に作成する必要があります。実務状況を見ると、特殊なシーンに関連する状況を個別に告知したうえで、同意を取得する方法が多くみられま。

（ア） 告知内容

「個人情報保護法」では、特殊なシーンにおける告知内容について明確に定めています。例えば、機微な個人情報を取扱う場合、それを取扱う必要性および個人の権益に与える影響について告知し（第 30 条）、中国域外へ個人情報を提供する場合には、域外の移転先の名称または氏名、連絡先、取扱目的、取扱方法、個人情報の種類、ならびに個人が域外の移転先に対し本法の定める権利を行使する方法および手続き等の事項を告知しなければなりません（第 39 条）。このほか、「情報安全技術　個人情報安全規範」（GB/T 35273-2020）、「情報安全技術　個人情報告知同意ガイドライン」（意見募集稿）等においても、特殊なシーンでの告知内容について定めがあることから、それらを参考にすることができます。

（イ）「個別の同意」の取得

「個別の同意」の取得方法については、告知・同意に関する文書が紙媒体であれば、ユーザーの署名により「個別の同意」を取得することができます。オンライン上で操作する場合、ポップアップ通知等のユーザーがスキップできない方法を使用し、告知・同意に関する文書を表示したうえで、電子署名またはユーザーの自発的な操作（例えば、設置した同意画面において、チェックマークを入れる、「承諾する」「次へ」といったボタンをクリックする等）により、「個別の同意」を取得することができます。

実務では、個別の同意を要する事項について予めプライバシーポリシーで簡単な説明をしたうえで、個別の同意を要する状況が生じた際に改めて個別の告知を行い、同意を取得するといった方法が多く見受けられます。

また、特殊なシーンにおける告知・同意に関する文書については、プライバシーポリシーと同様に、目立つ方法、明快かつ分かりやすい言葉で、関連事項を真実に基づき、正確かつ完全に個人に告知する必要があります。具体的には、上述したプライバシーポリシーの記載事項・書き方に関する要求を参考にすることができます。

（3） 個人情報保護影響評価（Privacy Impact Assessment，以下、「PIA」）の作成時の留意点

（ア）PIA を行う必要がある事由について

「個人情報保護法」第 55 条の規定によると、次の各号に掲げる事由のいずれかに該当する場合、事前に個人情報保護影響評価を行い、かつ取扱状況を記録しなければなりません。

a.機微な個人情報の取扱

b.個人情報を利用した自動化された意思決定の実施

c.個人情報取扱の委託、その他の個人情報取扱者への個人情報提供、個人情報の公開

d.域外への個人情報提供

e.個人の権益に重大な影響を与えるその他の個人情報取扱活動

（イ）PIA の内容

「個人情報保護法」第 56 条の規定によると、PIA の内容には次の事項を含める必要があります。

a.個人情報の取扱目的、取扱方法等が合法で、正当、かつ必要であるか否か

b.個人の権益への影響および安全リスク

c.講じる保護措置が合法、有効で、かつリスクの程度に相応しいものであるか否か

なお、PIA 報告書および取扱状況記録は、3 年以上保存しなければなりません。

上述の事由に該当する場合にはいずれも PIA を行う必要がありますが、事由により重要なポイントが異なります。日本企業および日系企業が関わる可能性の高い「域外への個人情報提供」における PIA では、おそらく域外の移転先に対する評価（管理、技術措置、能力等）が重要なポイントとなります。なお、PIA は、「データ域外移転安全評価弁法」に定める「データ域外移転リスクに関する自己評価」と内容上は類似していますが、別の法的文書であり、同一視してはならないという点に注意しなければなりません。

2.サイバーセキュリティ・データセキュリティ保護に関する文書

「個人情報保護法」は主に個人情報の保護について定めたものですが、「サイバーセキュリティ法」および「データセキュリティ法」では、サイバー（コンピューターネットワーク等）およびデータを保護の対象としており、その目的は、ネットワークが妨害、破壊され、または権限を付与されていないアクセスを受けないよう保障し、ネットワークデータが漏洩し、または窃取され、改竄されることを防止するためにあります。そのため実務では、保護の対象・目的を踏まえた予防（社内制度の確立等）、監視・注意喚起、緊急対応といった「事前・事中・事後」管理体制を整え、義務付けられている法的文書および制度を作成し、抜けのない安全体系を確立する必要があります。なお、保護対象の重要度により、企業が講ずるべき保護措置も異なり、作成すべき法的文書および制度の内容も異なります。そのため、保護する対象の状況を把握するために、まずは、ネットワークの等級付け（中国語：定級）[1]を行い、また取扱うデータの分類・等級付け[2]を行う必要があります。

上述した「事前・事中・事後」の管理体制を整えるうえで、社内の日常管理制度を確立

[1]「情報セキュリティ技術　ネットワークセキュリティ等級保護定級ガイドライン（GB/T 22240-2020）」を参照

[2] 目下、データの分類・等級付けについては一元的なルールを定めた国レベルの法令が制定されておらず、データ分類・等級付けは手探りの状態にある。なお、「工業データ分類・等級付けガイドライン（試行）」（2020 年 2 月 27 日施行）、「ネットワーク安全標準実践ガイドライン――ネットワークデータ分類・等級付けガイダンス」等の特定分野向けの標準が制定されていることから、それらを参照することができる。

し、緊急対応策を制定することが最も重要なポイントであると解されます。この 2 種類の法的文書の作成において注意すべき事項を以下のとおり説明します。

（1）日常管理制度の作成時の留意点

ネットワーク運営者[3]およびデータ取扱活動を展開する主体はいずれも、サイバーセキュリティ、全プロセスにわたるデータセキュリティ管理制度[4]を確立・整備する必要があります。「情報安全技術　ネットワーク安全等級保護基本要求」（GB/T22239-2019）等の規定によると、構築すべき制度には、アクセス制御に係る制度、環境・物理的安全に係る管理、ネットワークおよびシステムに係る安全管理、セキュリティ監査、重要データのバックアップ・復元、重要な設備・機器に係る管理等を含む必要があると解されます。なお、上述の社内制度のほか、「サイバーセキュリティ法」「データセキュリティ法」では、主管機関に報告し、相応の手続きを踏み、または個人に告知する義務を果たさなければならない特定の状況について定めています。こうした対外的な対応についても、制度上で明文化しておく必要があります。例えば、「サイバーセキュリティ法」第 49 条では、ネットワーク運営者は、ネットワーク情報安全に係る苦情、通報の制度を確立し、苦情申立て、通報の方法等の情報を公表し、遅滞なく関連するネットワーク情報安全に係る苦情および通報を受理し、かつ処理しなければならないと定めていることから、社内制度上、相応の内容を明確に定めておく必要があります。また、社内の日常管理制度の構築にあたり、具体的な部門および個人を指定し、その責任の所在を明確にしておく必要があります。

（2）緊急対応策の作成時の注意点

「サイバーセキュリティ法」第 25 条では、緊急対応策の制定をネットワーク運営者に義務付けています。また、「データセキュリティ法」第 29 条では、データセキュリティ事件が発生した場合には、直ちに処置措置を講じなければならないと定めています。法令に明文の規定はありませんが、緊急対応策については、サイバーセキュリティ緊急対応と、データ（個人情報を含む）漏洩の緊急対応の内容が含まれていれば、一つの文書を制定すれば足りると解されます。作成にあたっては、「公共インターネットサイバーセキュリティ突発事件緊急対応策」（工信部網安［2017］281 号）、「国家サイバーセキュリティ事件緊急対応策」（中網弁発文〔2017〕4 号）を参考とすることができます。緊急対応策を制定するうえで、社内の各部門・部署の役割分担、セキュリティ事件の等級付け、緊急時の監視・注意喚起フロー、対応フロー等を明確にする必要があります。なお、セキュリティ事件や情報流出事件が発生する確率は低いからという理由で、緊急対応策を制定しない企業もあるようですが、ネットワーク運営者またはデータを取扱う企業に該当するのであれば、その確率の如何を問わず、いずれも緊急対応策を作成する義務があるため注意が必要です。

[3] ネットワーク運営者とは、ネットワークの所有者、管理者およびネットワークに係るサービス提供者をいう。ネットワークとは、コンピューターまたはその他の情報デバイスおよび関連機器により構成される、一定の法則およびプログラムに従い、情報の収集、保管、伝送、交換、処理を行うシステムをいう。
[4]「サイバーセキュリティ法」第 21 条および「データセキュリティ法」第 27 条の規定を参照

3. 終わりに

本稿では、一部の重要な法的文書の作成における注意点について概説しました。紙面の関係上割愛しましたが、本稿で言及していない一部の特定の状況（例：重要データおよび一定のレベルの数量に達する個人情報の域外移転は、データ三法および「データ域外移転安全評価弁法」に従い、自己評価報告を作成し、データ域外移転安全評価を申告する等）においても、法的文書を作成する必要があることから、関連企業は、これらの義務についても注意を払う必要があります。

北京市環球法律事務所

レポートをご覧いただいた後、アンケート（所要時間：約１分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20220052

本レポートに関するお問い合わせ先：
日本貿易振興機構（ジェトロ）
海外調査部 中国北アジア課
〒107-6006 東京都港区赤坂 1－12－32
TEL：03-3582-5181
E-mail：ORG@jetro.go.jp