



中国の個人情報保護法の概要と、 典型的な場面別の実務対応

2021年11月25日(木)

西村あさひ法律事務所
弁護士・NY州弁護士 岩瀬 ひとみ
弁護士・NY州弁護士、CIPP/E 石川 智也



岩瀬 ひとみ

Hitomi Iwase

パートナー

03-6250-6218

h.iwase@nishimura.com

主な業務分野

- 知的財産取引、知的財産争訟、模倣品対策/ブランド管理
- 個人情報・プライバシー/ビッグデータ
- ITシステム/クラウド 等

略歴

1997年 弁護士登録、2004年 米国NY州弁護士登録。1994年 早稲田大学法学部卒業、2003年 スタンフォード大学ロースクール卒業(LL.M. in Law Science & Technology)。2018年 一橋大学大学院国際企業戦略研究科 非常勤講師

知財/IT関連の各種取引や争訟(特許関連訴訟、商標関連訴訟、システム関連紛争等)を主に扱う。IT分野では、国内及び外国が絡む、様々な局面における個人情報・データ関連の規制その他の問題や、クラウド、AI、IoT等新しい技術を用いたビジネスに絡む各種法律問題についてアドバイスをを行う。

最近の主な著書・論文等

『2020年個人情報保護法改正と実務対応』(商事法務、2020年)、『個人情報保護法制大全』(商事法務、2020年)、『いますぐわかるCCPAの実務対応』(中央経済社、2020年)、『企業労働法実務相談』(共著、商事法務、2019年)、“Japan: Overview of the Act on the Protection of Personal Information” (European Data Protection Law Review, Volume 5, 2019)、『個人情報保護法制と実務対応』(共著、商事法務、2017年)

最近の主なセミナー等

「2020年改正個人情報保護法 改正政令・規則と改正ガイドラインを踏まえた実務対応ポイントと留意点」(セミナーインフォ、2021年8月)、「2020年改正個人情報保護法のポイントと実務上の留意点」(日本証券業協会大阪地区協会)、「サイバー被害と個人情報の流出—その実態と対応について—」(産業経理協会、2020年11月)、「必ず押さえるべき個人情報保護法改正内容と実務対応上の留意点」(セミナーインフォ、2020年8月)、「EU、中国、香港及び日本におけるデータ保護法の最新事情」(西村あさひ法律事務所リーガルフォーラム第126回、2019年6月)、「いつ・どのようにGDPRを遵守すればよいのか? 日本企業にとって最大のGDPRリスクとそのための解決策は何か?」(緊急シンポジウム: 欧州監督機関のトップが語るプライバシー保護のグローバル最前線、2018年11月)、「GDPRの要求事項と企業での現実的な対応方法」(Fortinet Security World 2018、2018年6月)



石川 智也

Noriya Ishikawa

パートナー

n.ishikawa@nishimura.com

2005年	東京大学法学部第一類卒業
2006年	弁護士登録(第一東京弁護士会)、 西村あさひ法律事務所入所
2015年	バージニア大学卒業(LL.M.)
2016年	独 Max Planck Institute for Innovation and CompetitionにあるMunich Intellectual Property Law Center修了 (LL.M.)
2016年	独 Noerr法律事務所ミュンヘンオフィス (IP・メディア部門)にて研修
2017年	ニューヨーク州弁護士登録
2020年	西村あさひ法律事務所欧州拠点(フランク フルト/デュッセルドルフ)代表に就任

西村あさひ法律事務所フランクフルト&デュッセルドルフ事務所共同代表。GDPR、CCPA・CPRAを初めとするグローバルでの個人情報保護法制へのコンプライアンス対応について多くの日本企業にアドバイスを提供。日本経済新聞社による「2019年に活躍した弁護士ランキング」の「データ関連分野」で、総合ランキング1位(企業票+弁護士票)。

最近の主な書籍

- 『M&A・企業組織再編のスキームと税務～M&Aを巡る戦略的税務プランニングの最先端～(第4版)』(共著、大蔵財務協会、2019年)
- 『M&A法大全(下)〔全訂版〕』(共著、商事法務、2019年)
- 『秘密保持契約の実務(第2版)』(共編著、中央経済社、2019年)
- 『いますぐわかるCCPAの実務対応』(共著、中央経済社、2020年)
- 『2020年個人情報保護法改正と実務対応』(共著、商事法務、2020年)
- 『個人情報保護法制大全』(共編著、商事法務、2020年)など多数

最近の主な論文

- 「GDPR対応の実務 対応の可否と優先順位の考え方」(共著、Business Law Journal 2018年4月号)
- 「GDPR「地理的範囲についてのガイドライン」の概要と実務上注目すべきポイント」(共著、Business Law Journal 2019年3月号)
- 「十分性認定後のEEA域内からの個人データの移転」(共著、Business Law Journal 2019年5月号)
- 「カリフォルニア州消費者プライバシー法(CCPA)対応のための重要ポイント」(NBL 2019年12月1日号)
- 「連載・実務上の疑問に答える データ保護・利活用の要点」(共著、Business Law Journal 2019年8月号～2020年5月号)
- 「連載・個人情報保護法 世界の最新動向」(共著、ビジネス法務2020年1月号～2021年3月号)
- 「連載・個人情報保護体制グローバル化の設計図」(共著、Business Law Journal 2020年7月号～2021年2月号)

概要・適用範囲・域外移転

- 2021年8月20日に全人代常務委員会で採択され、**2021年11月1日**施行
- 上記採択後、下位規範が公表されており、今後も下位規範の公表が見込まれる。特に、11月14日公表、12月13日までパブコメに付されている規則案は重要
- 解釈に際しては、個人情報安全規範も参照される
- 法律の枠組みはGDPRに似ている一方で、同意に重きが置かれている等、従前の中国での実務を反映した内容となっている
- 中国の拠点、インバウンドのビジネスについては、法律上も、リスクベースで考えたときにも対応は必須
- 適用ある場合に、リスクベースで考えるのであれば、基本的には、GDPRと同じ程度のリスクはあると考えるべき（GDPR対応をした＝中国法対応もすべき）
- 執行方法の違い、地理的な距離の近さ（インバウンドのボリュームの大きさ）、文化的な近さ（ドイツ語のサイトはなくても、中国語のサイトはあったりする）

- GDPRとは異なり、実体的適用範囲(material scope)の概念はない
- 適用除外(72条1項): 自然人が個人又は家庭の事務により個人情報を取り扱う場合は適用除外
- 地理的適用範囲(3条)
 - ・ 中国国内において自然人の個人情報を取り扱う活動(1項)
 - ・ 中国国外において中国国内の自然人の個人情報を取り扱う活動についても、次のいずれかに該当する場合には適用(域外適用)(2項)
 - 中国国内の自然人に対する製品又はサービスの提供を目的とするとき
 - 中国国内の自然人の行為を分析し、又は評価するとき
 - 法律・行政法規所定のその他の事由
- GDPRとの比較
 - 1項: 中国独自の考え方。中国国内の企業はもちろんのこと、中国に出張して取り扱う行為は常に適用
 - 2項: 枠組みはGDPRと同じ。もっとも、GDPRのように制限的な解釈が存在せず、法的には広い

■ 代表者(53条)

- 域外適用を受ける個人情報取扱者は、中国国内において専門機構を設立し、又は代表者を指定しなければならない
- GDPRにあるような免除要件は定められていない
- 代表者は、個人情報保護関連事務の処理につき責任を負う
- 設立した専門機構の名称又は指定した代表者の氏名、連絡方法等を、当局に報告・送付する必要あり

■ 国外移転の要件：

- 個人情報の国外移転は、次の①～④の全ての条件を満たす場合に認められる
 - ① 中国国外の受領者の名称又は氏名、連絡方法、取扱いの目的、取扱方法、個人情報の種類、個人が中国国外の受領者に対して個人情報保護法に定める権利の行使方法及び手続等の事項を告知し、かつ、当該個人の個別の同意を取得すること(39条)
 - ② 以下のうちいずれか一つを満たすこと(38条)。ただし、重要情報インフラ運営者又は当局の定めた数以上のデータを取り扱う者は、法律・行政法規及び当局が定める場合を除き、必ず1.の条件を満たす必要がある(40条後段)
 - 1. 国家ネットワーク情報部門が組織する安全評価に合格すること
 - 2. 専門機構が行う個人情報保護の認証を得ること
 - 3. 国家ネットワーク情報部門の制定する標準契約を受領者と締結すること
 - 4. 法律、行政法規又は国家ネットワーク情報部門の定める条件を満たすこと
 - ③ 必要な措置を講じ、中国国外の受領者による個人情報取扱活動が、個人情報保護法の定める個人情報保護の水準に達していることを保障すること(38条3項)
 - ④ 個人情報保護影響評価を実施すること(55条4号)

■ 国外移転の要件:

- 以下の場合には、前記②にかかわらず、移転が可能(規則案35条)。また、法13条2項により、個別の同意取得に代えて、他の適法性根拠に依拠できると整理できる可能性あり

- ✓個人が当事者である契約を締結し、又は履行する目的で、当該当事者の個人情報在国外に提供することが必要な場合

- ✓人の生命、健康又は財産の安全を保護する目的で、個人情報在国外に提供することが必要な場合

■ 規則案39条において、国外移転に際して個人情報取扱者が遵守すべき規律が追加

■ 規則案40条において、個人情報と重要情報を国外に提供する場合には、毎年1月31日までに、前年のデータ移転に関する状況を地方レベルのネットワーク情報部門に報告するルールが追加

■ データローカライゼーション:

- 重要情報インフラ運営者又は当局の定めた数以上のデータを取り扱う者は、中国で収集し、及び生じた個人情報を中国国内に保存する必要あり(40条前段)
- 国外移転を行うことや、(中国国内に個人情報を保存した上で)中国国外でも個人情報を保存することまで禁止されるわけではない

典型的な場面別の対応

- 個人情報取扱者: 個人情報の取扱活動において、**取扱いの目的及び取扱方法**を自主的に**決定**する組織又は個人(73条1号)→**いわゆる「管理者(Controller)」**
- 個人情報: 電子その他の方法により記録される、既に識別され、又は識別可能な自然人に関連する各種情報(4条1項)
- 匿名化(個人情報につき処理を経て、特定の自然人を識別することができず、かつ、復元することができないプロセスをいう。73条4号)処理後の情報は明示的に除外されている
- GDPRに比べると、個人情報の定義は簡潔で、手掛かりが少ない
- 個人情報安全規範では、個人情報は「電子又はその他の方法により記録される、単独で若しくはその他の情報と結びついて特定の自然人の身分を識別し得る又は特定の自然人の活動状況等を反映し得る各種情報」と定義されている
- 個人情報保護法公布後に公表されたデータ分類等級ガイドライン(パブコメ版)では、Cookieは含むとされている

GDPRとの比較(赤字は重要な差異)

規制の主要項目	中国法	GDPR
処理に適法性根拠を必要とする	○(13条1項)、 正当利益概念なし→同意対応?	○(6条)
センシティブ情報への規制加重	○(28～32条)、 スコープ広い、実体規制厳格	○(9、10条)
所定の事項の告知(ノーティス)	○(17、23、30、39)、 特則(センシティブ情報の処理、所謂第三者提供、国外移転)あり	○(13、14条)
情報主体の権利	○(24条3項、44条～48条)、 ほぼ同じ	○(15～22条)
委託先の義務	△(21条、59条)、 委託契約の内容は指定無し	○(28条)
記録保持義務	× 。但し、 安全規範にあり	○(30条)
データセキュリティに関する義務	○(51条)、 組織的措置が具体的	○(24、32条)
データ漏えい等の際の通知義務	○(57条)、 当局報告は常に、主体への報告要件のスコープも広い	○(33、34条)
域外適用時の代理人選任義務	○(53条)、 免除事由なし、連帯責任、当局報告	○(27条)
データ保護責任者	○(52条)、 選任要件明確、ルールは少ない	○(37～39条)
法令遵守に係る監査義務	○(54条)、 独自規制	該当無し
影響評価	○(55条、56条)、 スコープ広い(センシティブ個人情報、委託、提供、国外提供全て)、記録付き	○(35、36条)
越境データ移転規制	○(38条～43条)、 移転の根拠+原則同意+保護措置の実施(+告知+影響評価+記録)	○(44～49条)
データローカライゼーション規制	○(40条)、 独自規制	該当無し

①中国に出張して個人情報を受領する

■ 適用スコープ

- 中国国内において自然人の個人情報を取り扱う活動

■ 所定の事項の告知

■ 同意、同意に代わる適法性の根拠

- 同意は、個人が十分に事情を知っているという前提において、自由意思により、かつ、明確になされる必要あり
- 黙示の同意？

■ 個別同意の特則（センシティブ情報の処理、所謂第三者提供、国外移転）が問題となる場面か？

■ 日本に帰るときに、国外に持ち出すことが越境移転規制の対象になるか？

②中国の子会社から個人情報を受領する

■ 適用スコープ

- 中国の子会社: 中国国内において自然人の個人情報を取り扱う活動
- 日本の本社: 中国国内の自然人に対する製品又はサービスの提供を目的とするとき/中国国内の自然人の行為を分析し、又は評価するときに当たるか？

■ 所定の事項の告知

■ 同意、同意に代わる適法性の根拠

■ 個別同意の特則(センシティブ情報の処理、所謂第三者提供、国外移転)が問題となる場面か？

- 多くのケースで問題となる
- 取引先の担当者の情報について、個別同意は取得しきれないことがある

■ 影響評価、越境データ移転規制

③中国の個人に向けてビジネスを行う

■ 適用スコープ

- 中国国内の自然人に対する製品又はサービスの提供を目的とするとき/中国国内の自然人の行為を分析し、又は評価するとき

■ 所定の事項の告知

■ 同意、同意に代わる適法性の根拠

■ 個別同意の特則(センシティブ情報の処理、所謂第三者提供、国外移転)が問題となる場面か？

- 同意取得のフローを緻密に検討する必要がある

■ 影響評価、越境データ移転規制

④グローバル内部通報制度の対応

■ 適用スコープ

- 中国国内の自然人からの直接取得なのか、中国国内の会社からの個人情報の移転なのか？
- 中国国内の自然人に対する製品又はサービスの提供を目的とするとき/中国国内の自然人の行為を分析し、又は評価するとき？
- 通報者の情報と、通報される人の情報とがある

■ 所定の事項の告知：通報される人にどのように通知するか？

■ 同意、同意に代わる適法性の根拠：通報される人から同意を得られない

■ 同意の特則（センシティブ情報の処理、所謂第三者提供、国外移転）が問題となる場面か？

■ 影響評価、越境データ移転規制

■ 法律の文言通りに規制を遵守しきれないところへのリスクベースの対応が鍵

■ プライバシーポリシーの近時のトレンド

- ・ 現状認識

- 日本法対応(和)、GDPR対応(英)、CCPA対応(英)
- 日本法対応(和英)、GDPR対応(英)、CCPA対応(英)
- グローバルに統一したポリシーを目指しているものは少ない

- ・ どの法制に対応させるか？

- ・ グローバルに統一したポリシーの視点

- GDPRをベースにしつつも、GDPR特有の言い回しは排除
- 日本企業は、日本法の下での開示事項の記載は必須(共同利用、匿名加工情報など)
- 各国法のアデンダムを後ろに付けていく(この中で中国法への対応を行う)

- ・ 言語

- ・ 主体

- Cookieも個人情報に該当する
- 所定の事項の告知
 - ・ プライバシーポリシーとクッキーポリシーを組み合わせ、中国法の要件を網羅するように記載
- 適法性の根拠は、同意しか依拠できそうにない
- 個別同意の特則（センシティブ情報の処理、所謂第三者提供、国外移転）が問題となる場面か？
 - ・ 第三者提供と国外移転が存在するケースは多い
- 影響評価、越境データ移転規制

- 委託契約に規定すべき事項の指定はない
- 規制する国ごとに契約を締結するわけにもいかない
- GDPRで要請される文言をベースに、GDPR特有の文言を除いたグローバル対応の委託契約の準備も一案
- 委託する場合も影響評価が必要
 - 個人情報保護影響評価には、次の内容が含まれる必要あり(56条1項): 枠組みはGDPR類似。影響評価の各国別展開の実務を固める時代がやってきている
 - ① 個人情報の取扱いの目的、取扱方法等が適法、正当かつ必要であるか否か
 - ② 個人の権益に対する影響及び安全リスク
 - ③ 講じた保護措置が適法かつ効果的であり、かつ、リスクレベルにも対応しているか否か

- 現状、メニューに乏しく、対応が確定している部分に対応するしかない
 - 告知＋同意
 - 移転先の活動が、中国の個人情報保護法を遵守していることの確保
 - 越境移転影響評価
 - 移転するデータの内容の報告も求められるようになる
- 今後
 - 多くのケースで、契約の締結が必要に
- 個別の同意を取得すれば終わりということではない

(参考資料)

N&Aリーガルフォーラムオンライン11/1施行！中国の個人情報保護法の解説と
実務対応からの抜粋

<https://www.nishimura.com/ja/seminars/LFO20211014.html>

■ センシティブ個人情報の定義(28条1項)

- ひとたび漏洩し、又は違法に使用されれば、自然人の人格的尊厳が侵害を受け、又は人身・財産の安全が危害を受けることが容易にもたらされる個人情報(28条1項)
- 生体識別情報、宗教的信仰、特定の身分、医療・健康、**金融口座、行動履歴**等の情報及び**14歳未満の未成年者の個人情報**が、センシティブデータとして**例示列举**

■ 必要となる対応

- 実体要件: 特定の目的及び十分な必要性があること、かつ、厳格な保護措置が講じられていることが必要(28条2項)
- 同意の特則: 同意を適法性の根拠とする場合には、**個別同意**が必要。法律・行政法規が要求する場合には、書面による同意が必要(29条)
- 告知の特則: 告知が必要な場合には、**センシティブ個人情報を取り扱う必要性及び個人の権益に対する影響**を告知する必要あり(30条)
- 影響評価: **個人情報保護影響評価**が必要(55条1号)

■ 14歳未満の未成年者の個人情報の取扱いの特則(31条)

- **父母その他の看護人の同意 / 専用の個人情報取扱規則(所謂ポリシー)の制定**

■ 以下の基本原則が定められている

- 適法、正当、必要性及び信義誠実の原則(5条)
- 目的の明確性、合理性の原則(6条1項)
- 最小化の原則(6条2項)
- 公開・透明性の原則(7条)
 - 個人情報取扱規則(所謂ポリシー)の公開、取扱いの目的、方法及び範囲の明示
- 正確性の原則(8条)
- 安全確保の原則(9条)
- 適法性・無害性の原則(10条)

取扱いに適法性根拠が必要であること

- 次のいずれかに該当する場合に、個人情報を取り扱うことができる(13条1項)
 - 個人の同意を取得したとき(1号)
 - 個人を一方当事者とする契約を締結し、若しくは履行するために必要であり、又は法により制定された労働規則制度及び法により締結された集団契約に従い人的資源管理を実施するのに必要であるとき(2号)
 - 法定の職責又は法定の義務を履行するために必要であるとき(3号)
 - 突発的な公共衛生事件に対応するため、又は、緊急の状況において自然人の生命・健康及び財産の安全を保護するために必要であるとき(4号)
 - 公共利益のためにニュース報道、世論監督等の行為を行い、合理的な範囲内において個人情報を取り扱うとき(5号)
 - 個人情報保護法の規定に従い、合理的な範囲内において、個人が自ら公開した、又はその他の既に適法に公開された個人情報を取り扱うとき(6号)
 - 法律・行政法規の定めるその他の事由(7号)

取扱いに適法性根拠が必要であること

- GDPRとは異なり、正当利益に依拠して個人情報を取り扱うことはできない
 - 本社への従業員情報・取引先情報の共有
 - サイバーセキュリティのための情報管理
 - 防犯カメラの設置
- 同意を取得できるものは同意を取得する一方で、どうしても取得できないものをどうするかという問題は残る

■ 同意の要件：

- 同意は、個人が**十分に事情を知っている**という前提において、**自由意思**により、かつ、**明確**になされる必要あり(14条1項)
- 法律・行政法規が個人情報の取扱いにつき個人の個別同意又は書面同意を取得しなければならないと定める場合には、その規定に従う必要あり(14条1項)
- 個人情報の取扱いの目的、取扱方法及び取り扱う個人情報の種類に変更が生じた場合には、改めて個人の同意を取得する必要あり(14条2項)

■ 同意取得が必要な場合において、**個別同意**を要するケース：**同意フローの精査が必要**

- **他の個人情報取扱者への提供**(23条)、個人情報の公開(25条)
- 公共安全を維持・保護する目的以外の、個人の画像・映像及び個人の身元識別情報の利用(26条)
- **センシティブ個人情報の取扱い**(29条)
- **個人情報の国外移転**(39条)

■ 同意の撤回権：

- **撤回権あり**。簡便・迅速な同意撤回の方法を提供する必要あり(15条1項)
- 同意の撤回は、撤回前に個人の同意に基づき既に行われた個人情報取扱活動の効力に影響を及ぼさない(15条2項)

■ 同意の条件：

- 個人情報の取扱いが製品又はサービスの提供に必要である場合を除き、個人がその個人情報の取扱いに同意せず、又は同意を撤回したことを理由として、製品又はサービスの提供を拒絶してはならない(16条)

■ 収集時の告知事項(17条1項):

- ① 個人情報取扱者の名称又は氏名及び連絡方法
- ② 個人情報の取扱いの目的及び取扱方法並びに取り扱う個人情報の種類及び**保存期間**
- ③ 個人が個人情報保護法に定める権利を行使する方法及び手続
- ④ 法律・行政法規に定めるその他の告知すべき事項

■ 告知事項の特則:

- ① 他者に個人情報を提供(委託は含まない)する場合: 受領者の名称又は氏名、連絡方法、取扱いの目的、取扱方法及び個人情報の種類(23条)
- ② センシティブ個人情報を取り扱う場合: センシティブ個人情報を取り扱う必要性及び個人の権益に対する影響(30条)
- ③ 中国国外に個人情報を提供(委託も含む)する場合: 国外受領者の名称又は氏名、連絡方法、取扱いの目的、取扱方法、個人情報の種類、国外受領者に対し個人情報保護法に定める権利を行使する方法及び手続等(39条)

■ 告知事項に変更が生じたら、変更部分を個人に告知する必要あり(17条2項)

■ 告知要件(17条1項):

- 取扱い前に告知
- 顕著な方法及び明瞭かつ理解しやすい言語→「簡体字でなければならない」という条文はないが、簡体字は必須
- ありのまま
- 正確かつ完全

■ 告知方法:

- 告知事項のみ告知することも可能
- 個人情報取扱規則を制定する方法により告知する場合には、公開し、かつ、容易に閲覧及び保存ができるようにする必要あり(17条3項)
- 個人情報取扱規則の書式については、個人情報安全規範の別紙が参考になる

■ 告知義務が緩和される場合：

- ・ 法律・行政法規の定める事由があるときは、告知義務免除(18条1項)
- ・ 緊急の状況において、自然人の生命・健康及び財産の安全を保護するため、個人に対し遅滞なく告知することができない場合には、緊急の状況が解消された後に遅滞なく告知する必要あり(18条2項)

■ 実務対応：

- ・ 個別に告知事項を作成するか、個人情報取扱規則(所謂プライバシーポリシー)を制定して公表するか
- ・ 中国法独自に作成するか、既存のプライバシーポリシーに組み込むか
- ・ どの言語について用意するか(簡体字は必須)

■ グローバル対応：

- ・ 長期的には、既存のプライバシーポリシーに、差分を中国法アデンダムとして組み込んだ上で、全ての言語について作成するのが実用的かつメンテナンスが簡便

- 保存期間の告知が必須(17条1項2号)
- 法律・行政法規に別途の定めがある場合を除き、保存期間は、取扱いの目的の実現に必要な最短の期間でなければならない(19条)

■ 合併等による個人情報の移転の特則(22条):

- 告知の特則: 合併、分割、解散、破産宣告等の原因により個人情報を移転する必要がある場合には、個人に対し受領者の名称又は氏名及び連絡方法を告知する
必要あり
- 義務の承継: 受領者は、個人情報取扱者の義務を継続して履行する必要あり
- 取扱い変更時の同意: 受領者は、当初の取扱いの目的及び取扱方法を変更する
場合には、改めて個人の同意を取得する必要あり

■ 第三者提供(委託は含まれない)の特則(23条):

- 告知の特則 + 個別同意: 個人に対し受領者の名称又は氏名、連絡方法、取扱いの目的、取扱方法及び個人情報の種類を告知し、かつ、個人の個別同意を取得する
必要あり
- 義務の承継: 受領者は、上記の取扱いの目的、取扱方法及び個人情報の種類等の範囲内において、個人情報を取り扱う必要あり
- 取扱い変更時の同意: 受領者は、当初の取扱いの目的及び取扱方法を変更する場合には、改めて個人の同意を取得する必要あり
- 個人情報保護影響評価も必要(55条3号)

- 自動化された意思決定の特則(24条): **GDPRよりも規制の範囲が広い**
 - 意思決定の透明度及び結果が公平かつ公正であることを保証しなければならない、個人に対し取引価格等の取引条件において不合理な差別を行ってはならない(1項)
 - 個人に対し情報プッシュ配信及び商業マーケティングを行う場合には、同時に、**その個人的特徴に基づかない選択肢を提供し、又は簡便・迅速な拒絶方法を提供する必要あり**(2項)
 - 個人の権益に対し重大な影響を及ぼす決定をする場合には、個人は、個人情報取扱者に対し説明するよう要求する権利を有し、かつ、個人情報取扱者が自動化された意思決定の方法のみにより決定することを拒絶する権利を有する(3項)
 - **個人情報保護影響評価も必要**(55条2号)

■ 個人情報の公開(25条):

- 個人の個別同意を取得しない限り、個人情報を公開してはならない
- 公開する場合には、**個人情報保護影響評価**が必要(55条3号)

- 公共の場所における画像・映像の収集・個人身元識別の設備の設置(26条):
 - 公共の場所において、画像・映像の収集又は個人身元識別の設備を取り付ける場合には、公共安全を維持・保護するために必要でなければならず、国の関係規定を遵守し、かつ、顕著な提示標識を設置する必要あり
 - 個人の個別同意がない限り、収集した個人の画像・映像及び個人の身元識別情報は、公共安全を維持・保護する目的以外の目的に用いてはならない

- 公開された個人情報の取扱い(27条):
 - 個人が明確に拒絶している場合を除き、合理的な範囲内において、個人が自ら公開した、又はその他の既に適法に公開された個人情報を取り扱うことができる
 - ただし、個人の権益に重大な影響があるときは、個人の同意を取得する必要あり

- 情報主体には、以下の権利が認められている
 - 自己の個人情報の取扱いについて知る権利(44条)
 - 決定権(44条)
 - 取扱いの制限・拒絶請求権(44条)
 - 閲覧・複製権(45条1項、2項)
 - データポータビリティ権(45条3項)。但し、国家ネットワーク情報部門の定める条件に適合する場合に限る
 - 訂正・補充請求権(46条)
 - 削除請求権(47条)
 - 個人情報取扱規則について解釈・説明を行うよう要求する権利(48条)
 - 自動化された意思決定の方法により個人の権益に対し重大な影響を及ぼす決定をされる場合における、個人情報取扱者に対する説明要求権・自動化された意思決定の方法のみにより決定されることを拒絶する権利(24条3項)

■ 権利行使への対応

- 個人の権利行使に係る申請の受理及び取扱いにつき簡便・迅速な制度を確立する必要あり(50条1項)
- 個人の権利行使に係る請求を拒絶する場合には、理由を説明する必要あり(50条1項)
- 権利行使請求を拒絶された場合、個人は、人民法院に対し、訴訟提起が可能(50条2項)
- 具体的なタイムリミット、権利行使の方法、権利行使を受けた場合の対応方法等については、特段規定されていない

■ 安全措置(51条):

- 個人情報取扱者は、個人情報の取扱いの目的、取扱方法、個人情報の種類、並びに個人の権益に対する影響及び存在するおそれのある安全リスク等に基づいて、次の措置を講じて、個人情報取扱活動が法律・行政法規の規定に適合することを確認し、かつ、授權を経ていないアクセス及び個人情報の漏洩、改ざん又は紛失を防止する必要あり

- ① 内部管理制度及び運用規程の制定
- ② 個人情報の分類管理
- ③ 相応する暗号化、非識別化(個人情報につき処理を経て、当該個人情報をして追加情報の補助がなければ特定の自然人を識別できなくさせるプロセス。73条3号)等の安全技術措置の実施
- ④ 個人情報の取扱いに係る操作権限の合理的な確定及び業務従事者に対する定期的な安全教育・研修の実施
- ⑤ 個人情報安全事件の緊急時対応計画の制定・実施手配
- ⑥ 法律・行政法規の定めるその他の措置

■ 個人情報保護責任者の選任義務(52条):

- 取り扱う個人情報に国家ネットワーク情報部門の定める数量に達する個人情報取扱者は、個人情報保護責任者を指定する必要がある
- 個人情報保護責任者は、個人情報取扱活動及び講じた保護措置等について監督する責任を負う
- 個人情報保護責任者の連絡方法は公開する必要がある
- 個人情報保護責任者の氏名、連絡方法等を当局に報告・送付する必要がある

- 域外適用時の代表者の指定義務(53条):
 - 前述のとおり

■ 監査義務(54条)：

- 個人情報の取扱いに係る法律・行政法規の遵守状況について、**定期的に法令遵守監査**を行う必要あり

■ 個人情報保護影響評価:

- 次のいずれかに該当する場合には、**事前に個人情報保護影響評価**を行い、かつ、**取扱状況について記録を作成**する必要あり(55条): **範囲がとて広い**
 - ① **センシティブ個人情報の取扱い**
 - ② 個人情報を利用した自動化された意思決定の実施
 - ③ 個人情報取扱いの**委託**、第三者に対する個人情報の**提供**及び個人情報の公開
 - ④ 中国国外に対する個人情報の**提供(委託を含む概念)**
 - ⑤ 個人の権益に対し重大な影響を及ぼすその他の個人情報取扱活動
- 個人情報保護影響評価には、次の内容が含まれる必要あり(56条1項): **枠組みはGDPR類似。影響評価の各国別展開の実務を固める時代がやってきている**
 - ① 個人情報の取扱いの目的、取扱方法等が適法、正当かつ必要であるか否か
 - ② 個人の権益に対する影響及び安全リスク
 - ③ 講じた保護措置が適法かつ効果的であり、かつ、リスクレベルにも対応しているか否か
- 個人情報保護影響評価報告及び取扱状況記録は、最低3年保存(56条2項)
- 情報安全技術個人情報安全影響評価指針(2021年6月1日施行)を参照可

■ データ侵害時の通知義務(57条1項、2項)：

- **当局通知：常に必要、本人通知：危害を回避できない場合のみ必要、記録義務：なし**
 - 個人情報の漏洩、改ざん、紛失が発生し、又は発生するおそれがある場合には、個人情報取扱者は、直ちに**是正措置を講じ**、かつ、**当局及び個人に通知**しなければならない
 - 個人情報取扱者が講じた措置により危害を効果的に回避することができる場合には、個人に通知しないことができる。ただし、当局は、危害をもたらす可能性があると判断する場合には、個人に通知するよう要求することができる
- **直ちに通知**。72時間以内といった具体的な通知期限は定められていない

■ 通知事項(57条1項)：

- 漏えい、改ざん、紛失が発生し、又は発生するおそれがある情報の種類、原因及び生じ得る危害
- 個人情報取扱者が講じる是正措置及び個人が講じることのできる危害を軽減する措置
- 個人情報取扱者の連絡方法

■ プラットフォームの特則(58条):

- 重要なインターネットプラットフォームサービスを提供し、ユーザー数が多く、業務類型が複雑な個人情報取扱者は、次の義務を履行する必要がある
 - 国家の規定に従い、個人情報保護のコンプライアンス制度システムを確立して健全化し、主に外部メンバーから構成される独立機構を設立し、個人情報保護の状況について監督を行う
 - 公開、公平、公正の原則を遵守し、プラットフォームの規則を制定し、プラットフォーム内の製品又はサービス提供者の個人情報取扱規範及び個人情報保護の義務を明確にする
 - 法律・行政法規に重大に違反して個人情報を取り扱ったプラットフォーム内の製品又はサービス提供者に対し、サービスの提供を停止する
 - 個人情報保護社会責任報告を定期的に公布し、社会の監督を受ける

■ 受託者の監督：

- 委託する取扱いの目的、期間、取扱方法、個人情報の種類、保護措置、両当事者の権利義務等について**約定**（21条1項）→**契約内容までは決まっていない。GDPRに準拠したデータ処理契約で足りるか？**
- 受託者の個人情報取扱活動を**監督**する必要あり（21条1項）
- 受託者は、約定した取扱いの目的、取扱方法等を超えて個人情報を取り扱うことはできない（21条2項）
- 委託契約が効力を生じず、無効であり、取り消され、又は終了した場合には、受託者は、個人情報を個人情報取扱者に変換し、又は削除しなければならず、留保してはならない（21条2項）
- 受託者は、個人情報の取扱いを**再委託**するためには、個人情報取扱者の**同意**を経る必要あり（21条3項）→**同意ではなく、異議の機会を与えるだけで足りるか**
- 委託を行うためには、**個人情報保護影響評価**も必要（55条3号）

■ グローバル対応のデータ処理契約の準備が必要な時代を迎えている

■ いわゆる共同管理者の規律(20条):

- 個人情報の取扱いの目的及び取扱い方法を共同で決定する場合には、各自の権利及び義務を約定する必要あり(1項): **共同管理者契約。但し、規定すべき事項は決まっていない**
- ただし、約定にかかわらず、個人はそのうち1名の個人情報取扱者に対して権利を行使できる(1項)
- 共同管理者は、個人情報の権益を侵害して損害をもたらしたときは、連帯責任を負う(2項)

■ エンフォースメント

- 違反に対しては、是正命令、警告、違法所得の没収、個人情報等を違法に取り扱ったアプリケーションプログラムに関するサービスの一時停止・終了命令を行い、是正を拒否した場合に**100万元以下の過料**を併科し、**責任者等へは1万元以上10万元以下の過料**を課す(66条1項)
- 情状が重大である場合には、是正命令、違法所得の没収及び**5000万元又は直前会計年度の売上高の5%以下の過料**を併科し、かつ、**関連業務の一時停止又は営業停止・是正改善を命じ、関連業務許可・営業許可の取消し**を行うことができる。**責任者等へは10万元以上100万元以下の過料**を課すものとし、かつ、一定期間における関連企業の所定の役職への就任を禁止することができる(66条2項)
- 個人情報の取扱いにより、権益を侵害し、損害をもたらした場合には、故意・過失のないことを証明できない限り、民事の損害賠償等の責任を追う(69条1項)
- 金額は損害又は利益に応じて確定される(69条2項)
- 多数の個人の権益を侵害した場合には、消費者団体等も訴訟提起が可能(70条)

まとめ

適用範囲の整理

- 中国の拠点、中国での活動については、事業の規模にかかわらず個人情報保護法の適用あり
- 文言上はGDPRに類似したスコープを持つ域外適用の定めがあるため、少なくとも中国国外の拠点においても中国の消費者の個人情報を取り扱う場合には慎重な検討が必要
- 域外適用がある場合には代表者を選任する必要あり

データマッピング

- プライバシーポリシーの作成に耐え得る形で、取り扱っている個人情報について、情報を収集する
- GDPRの際のマッピングをベースに調整することも可能

個人情報の取扱いに「適法性の根拠」があるかの洗い出し

- 「正当な利益」に依拠できないため、GDPR上「正当な利益」に依拠していた個人情報の取扱いについては、同意等他の適法性根拠に依拠することが可能か、要検討
- 同意の要件が厳格なため、同意に依拠する場合には個別に要件を充足するか確認が必要

センシティブデータがあるかの洗い出し

- 金融口座、行動履歴、14歳未満の個人情報が含まれるなどスコープが広い
- 取扱いの要件(特定目的、必要性、厳格な保護措置)を充足する必要がある
- 所定の事項の告知、個別同意の取得、個人情報保護影響評価が必要となる

所定の告知事項を含むプライバシーポリシーの作成

- プライバシーポリシーと告知事項は区別されているが、プライバシーポリシーに告知事項を含めて公表することによっても対応可能

Ⅰ 個人情報の委託への対応

- 委託契約の締結
- 個人情報保護影響評価の実施も必要

Ⅰ 個人情報の提供への対応

- 所定の事項を告知
- 原則として個別同意の取得が必要
- 個人情報保護影響評価の実施も必要

Ⅰ 中国国外への個人情報の移転への対応

- 国外移転のための条件を充足するか、要確認
- 標準契約が公表されるまでの間は、2019年越境移転安全評価弁法(パブコメ稿)に規定されている内容の契約を作成することも考えられる
- 契約を締結した場合であっても、所定の事項の告知と(原則として)個別同意の取得が必要
- 個人情報保護影響評価の実施も必要

Ⅰ データローカライゼーションへの対応

- 重要情報インフラの運営者又は当局の定めた数以上のデータを取り扱う者に該当するか否かを確認

Ⅰ 自動化された意思決定への対応

- 規制の範囲が広く、Webマーケティングは広く該当
- 法律所定のパーソナライズされない仕組みの提供と、個人情報保護影響評価の実施が必要

I 安全措置

- 内部管理制度及び運用規程の制定等が必要となる
- その他、具体的に規定されている組織的措置について、体制への実装が必要
- データ漏えい・権利行使への対応に向けた体制整備

I 共同管理者の契約

- 契約に規定すべき事項は明らかでないが、GDPRの対応に準じて対応することが考えられる

I 個人情報保護責任者の選任

- 選任の可否を判断し、必要であれば選任

西村あさひ法律事務所

東京都千代田区大手町1-1-2 大手門タワー

〒100-8124

Tel | 03-6250-6200

www.nishimura.com

デュッセルドルフ事務所

Nishimura & Asahi Europe Rechtsanwaltsgesellschaft mbH

Königsallee 92a, 40212 Düsseldorf, Germany

Tel | +49-(0)211-5403-9512

フランクフルト事務所

Nishimura & Asahi Europe Rechtsanwaltsgesellschaft mbH

Neue Mainzer Str. 66-68, 60311 Frankfurt am Main, Germany

Tel | +49-(0)69-870-077-620