



個人情報保護管理体制の 構築・整備

中華人民共和国個人情報保護法（個保法）の挑戦と対応

kpmg.com/cn



個保法の要点整理

「中華人民共和国個人情報保護法」（以下、「個保法」）は約2年間の立法準備、3回の審議を経て、2021年8月20日に第13期全国人民代表大会常務委員会第30回会議で可決され、2021年11月1日より施行される。一次審議稿と二次審議稿を比較すると、個保法最終稿は、個人情報処理の適法根拠、個人情報処理の法令遵守義務、個人情報の越境提供および法的責任などの分野において、程度の差こそあれ更新されている。

適用範囲



- 中国国内における個人情報活動の処理
- 一定の条件を満たした中国国外における中国国内の自然人の個人情報活動の処理

個人情報処理者



- 処理の目的、方式などの個人情報処理事項を自ら決定できる組織、個人
- 「特殊」な処理者：共同処理、委託・受託処理、第三者など

適法根拠



- 個人の同意を取得している場合
- 個人が一方の当事者となる契約の締結又は履行で必要となる場合、又は法律で定められた労働規則や法律に基づき締結された団体契約に基づく人的資源管理で必要となる場合
- 個人が自ら公開している個人情報、又はその他の合法的に公開されている個人情報を、本法の規定に従い合理的な範囲内で処理する場合
- 法定の職責若しくは義務履行、緊急事態への対応、公共の利益のためのニュース報道、世論監督等の行為、その他法律、行政法規が規定する状況

法令遵守義務



- 組織スタッフ、制度・プロセス、技術的保護など
- 機微な個人情報の処理に関しては追加要件を満たさなければならない。14歳未満の未成年者の個人情報処理に関しては、専用の個人情報処理規則を制定しなければならない
- 個人の権利行使の申請を受理・処理し、個人情報ポータビリティの権利、自然人死亡後の主体の権利行使などをさらに約定しなければならない
- 事前に個人情報保護影響評価を行い、法規定への適合性に係る監査を定期的に行わなければならない

個人情報の越境提供



- 重要情報インフラ運営者および処理した個人情報の量が、国家ネットワーク情報部門が定める量に達した個人情報処理者は、中国国内で収集および生成した個人情報を中国国内に保存しなければならない
- 合法的な越境提供の要件とは、国家ネットワーク情報部門によるセキュリティ評価に合格すること、国家ネットワーク情報部門の規定に従い専門機関による個人情報保護の認証を受けること、国家ネットワーク情報部門が定める標準契約書に基づき国外受領者と契約を締結し、双方の権利および義務を約定することなどを含む
- 事前に個人情報保護評価を行い、個別同意を取得し、かつ中国国外の受領者による個人情報処理活動が個保法に規定される個人情報保護基準を満たしている

法的責任



- 是正を命じる、違法所得の没収、組織とスタッフに対する罰金、信用ファイルへの記録、損失賠償など
- 個人情報を違法に処理するアプリケーションプログラムに対してサービスの暫定停止若しくは永久停止を命じる
- 5,000万元以下若しくは前年売上高の5%以下の罰金を科す
- 直接責任を負う主管人員およびその他の直接責任者に対して10万元以上100万元以下の罰金を科し、更に、一定期間において関連企業の董事、監事、上級管理職および個人情報保護責任者に就くことを禁ずることができる

中華人民共和国
サイバーセキュリティ法
(サイバーセキュリ
ティ法)
Cybersecurity
Law of the
People's Republic
of China

2017年6月1日より発効
Enacted June 1st, 2017

中華人民共和国
データセキュリティ法
(データセキュリティ法)
Data Security Law
of the People's
Republic of China

2021年9月1日より発効
Enact from September 1st,
2021

中華人民共和国
個人情報保護法
(個保法)
Personal
Information
Protection Law of
the People's
Republic of China

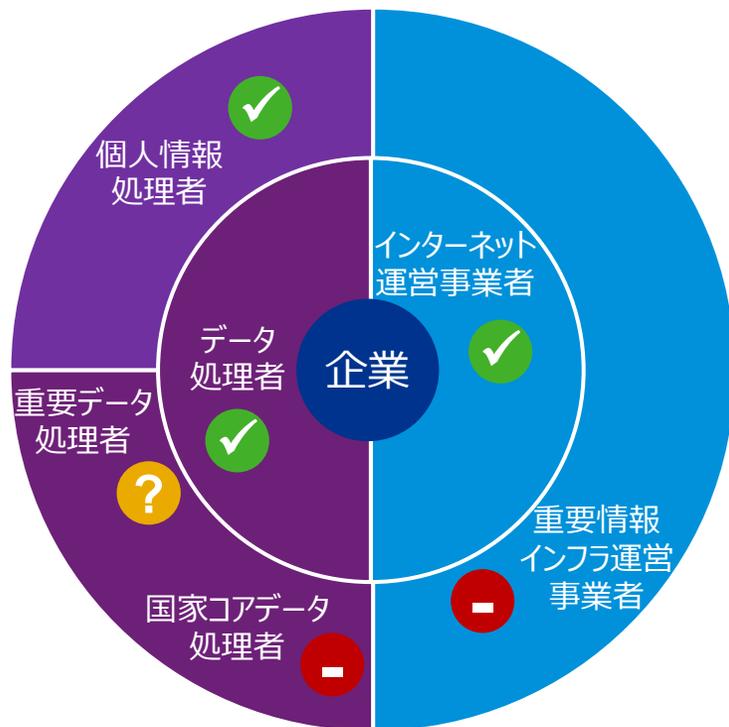
2021年11月1日より発効
Enact from November 1st,
2021

個保法は個人情報の保護に特化した法律として、個人情報の保護において主に参考・依拠すべき法律であり、EU一般データ保護法規（GDPR）、カリフォルニア州消費者プライバシー法（CCPA）など、その他のデータ保護法に匹敵する。

出所：KPMGが整理したデータによる

注：太字部分は個保法最終稿の更新内容の一部をまとめたものである。

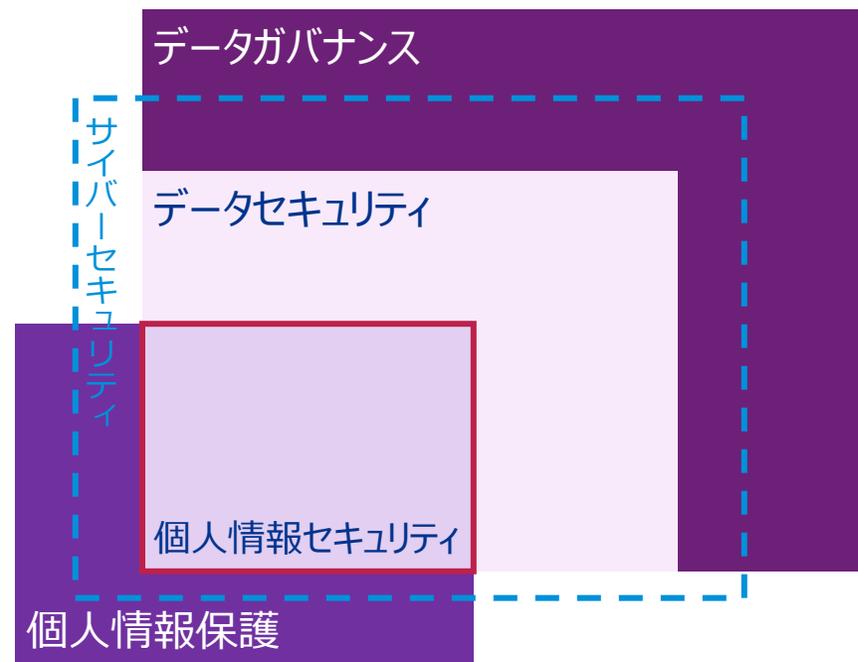
企業の複数の役割に対する理解



- ✔ 企業は通常、**インターネット運営事業者**（サイバーセキュリティ法）、**データ処理者**（データセキュリティ法）および**個人情報処理者**（個保法）としての役割を担っている
- ? 一部の企業は重要なデータの処理に関与する可能性がある
- 少数の企業は国家コアデータの処理および（または）重要情報インフラ運営に関与する可能性がある

✔ 企業は基本的な法令順守義務の観点から、下記の体制を構築・整備する必要がある。

1. 情報セキュリティ管理体制
2. データセキュリティ管理体制
3. 個人情報保護管理体制



出所：KPMGが整理したデータによる

関連情報：個保法とEU GDPRとの比較



適用範囲	<ul style="list-style-type: none"> 個保法の適用範囲は個人情報処理活動が行われる地理的地域に基づいているのに対し、GDPRの適用範囲はデータ所有者およびデータ処理者の設立場所に基づいている
個人情報処理者	<ul style="list-style-type: none"> 個保法で定義されている「個人情報処理者」および特殊なタイプの「個人情報処理者」とGDPRで定義されている「データ所有者」および「データ処理者」との間には少し差異がある 個保法における機微な個人情報の定義には少し差異がある
適法根拠	<ul style="list-style-type: none"> 個保法では、個人が自ら公開している個人情報、又はその他の合法的に公開されている個人情報を合理的な範囲内において処理することをカバーしている 個保法では、法律に基づき定められた労働規則や法律に基づき締結された団体契約に従った人的資源管理の必要性を明確にした 個保法では、特定の個人情報の処理に対して「個別同意」の取得を求めている
法令順守義務	<ul style="list-style-type: none"> 個保法においてプライバシーに係る声明・要求事項には少し差異がある 個保法では、14歳未満の未成年者の個人情報を処理する場合、専用の個人情報処理規則の制定を求めている 個保法で定められている個人情報主体の権利に少し差異があり、特に個人は個人情報処理者が個人情報の処理規則に関する説明を求める権利を有すること、また、自然人死亡後の主体の権利行使において差異がある 個保法では、個人情報の分類保護を求めている 個保法で定められている個人情報保護影響評価の開始条件と記録保存期間に少し差異がある 個保法では、アプリによる個人情報の収集、「大数据殺熟」（ビッグデータを活用して、同一商品・サービスに対して、新規顧客が常連顧客よりも安い価格で入手できること）、公共の場での画像収集などに対して的を絞った処理規則を定めた 個保法では、中国国内の自然人の行為を分析・評価する個人情報処理者は、中国国内で専門機関の設置又は代表者を指名することを求めている

個人情報の越境提供

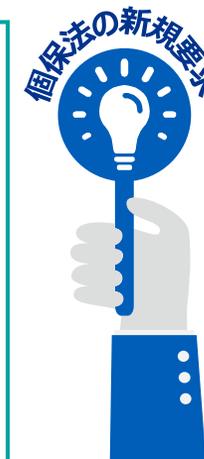
- 個保法で定められている越境提供要件：1) 国家ネットワーク情報部門によるセキュリティ評価に合格すること、2) 専門機関による個人情報保護認証を受けること、3) 国家ネットワーク情報部門が定める標準契約書に基づき国外の受領者と契約を締結すること又は4) 法律、行政規則、または国家ネットワーク情報部門が定めるその他の条件
- 個保法では、国外の受領者による個人情報処理活動が本法規定の個人情報保護標準を満たすよう求めている
- 個保法では、重要情報インフラ運営者および処理する個人情報の件数が、国家ネットワーク情報部門が定める件数に達した個人情報処理者は、中国国内で収集および生成した個人情報を中国国内に保存しなければならないことを明記している
- 個保法では、事前に個人情報保護評価を行い、個別に同意を取得するよう求めている

法的責任

- 個保法では違反行為に対する罰則がより厳格であり、是正を命じたり（アプリケーションプログラムに対しサービスの暫定停止若しくは永久停止を命じる）、違法所得の没収、組織とスタッフに対する罰金、上級管理者の登用禁止、信用ファイルへの記録、損失賠償などを含む

注：EU GDPRとは、EU一般データ保護法規、即ち General Data Protection Regulationを指す。

関連情報：個保法とGB/T 35273-2020(PISS)との比較

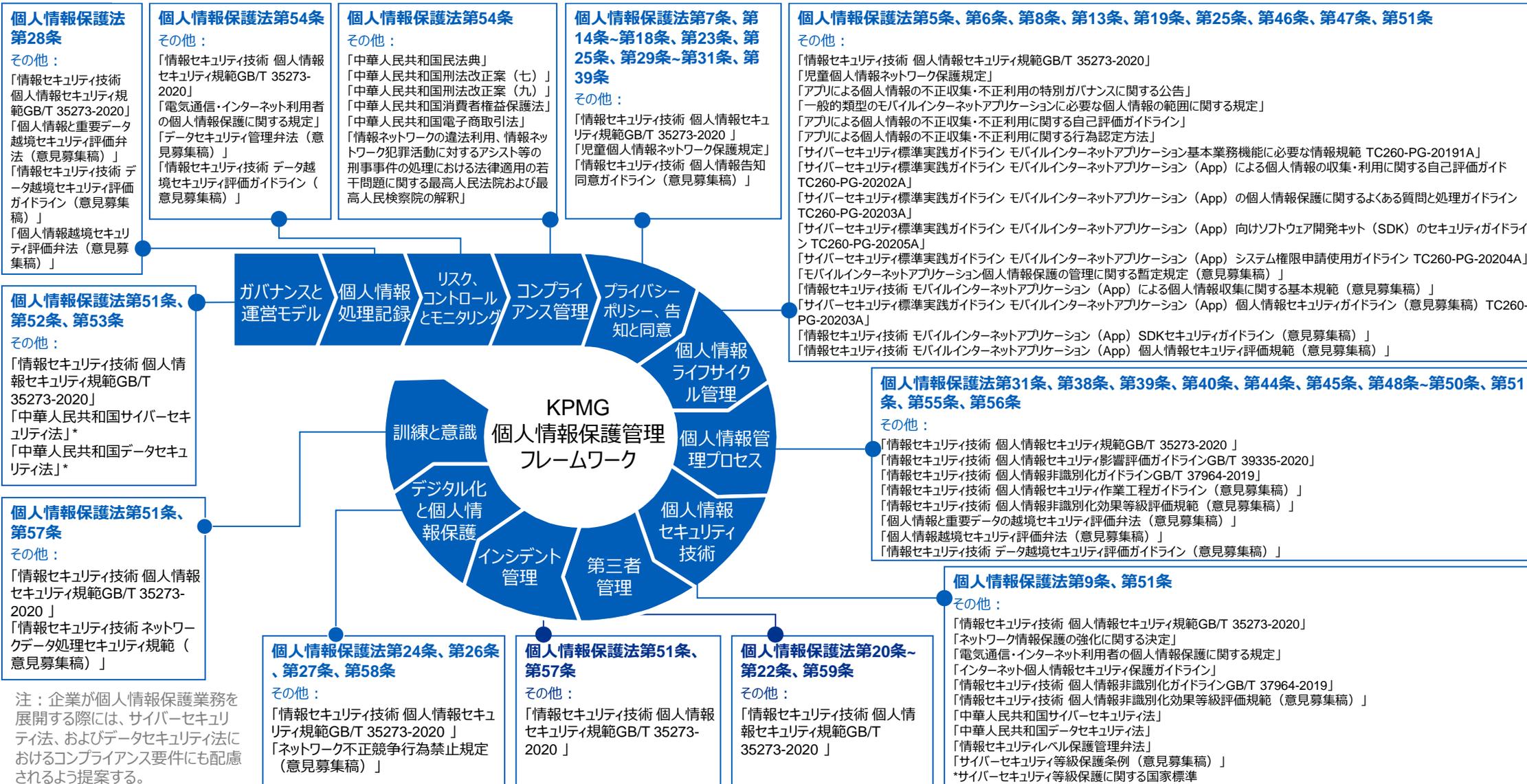


適用範囲	<ul style="list-style-type: none"> -
個人情報処理者	<ul style="list-style-type: none"> 個保法で定義されている「個人情報処理者」および特殊なタイプの「個人情報処理者」と個人情報セキュリティ規範で定義されている「個人情報管理者」との間には少し差異がある
適法根拠	<ul style="list-style-type: none"> 個保法では、個人情報の処理において個人から同意を取得する場合の例外に少し差異がある。具体的には、個人が自ら公開している個人情報、又はその他の合法的に公開されている個人情報を合理的な範囲内で処理できる。また、法律に基づき定められた労働規則や法律に基づき締結された団体契約に従った人的資源管理で必要となる個人情報を処理できる
法令順守義務	<ul style="list-style-type: none"> 個保法では、14歳未満の未成年者の個人情報を処理する場合、専用の個人情報処理規則の制定を求めている 個保法で定められている個人情報主体の権利には少し差異がある。特に知る権利の新規追加、個人が個人情報処理者に対し、個人情報の処理規則に関する説明を求める権利を有することや、自然人死亡後の主体の権利行使において差異がある 個保法では、個人情報の分類保護を求めている 個保法で定められている個人情報保護影響評価の開始条件と記録保存期間に少し差異がある 個保法では、アプリによる個人情報の収集、「大数据殺熟」（ビッグデータを活用して、同一商品・サービスに対して、新規顧客が常連顧客よりも安い価格で入手できること）、公共の場での画像収集などに対して的を絞った処理規則を定めた 個保法では、中国国内で国内自然人の行為を分析・評価する個人情報処理者は、中国国内で専門機関の設置又は代表者を指名するよう求めている

個人情報の越境提供	<ul style="list-style-type: none"> 個保法で定められている越境提供要件：1) 国家ネットワーク情報部門によるセキュリティ評価に合格すること、2) 専門機関による個人情報保護認証を受けること、3) 国家ネットワーク情報部門が定める標準契約書に基づき国外の受領者と契約を締結すること又は4) 法律、行政規則、または国家ネットワーク情報部門が定めるその他の条件 個保法では、国外の受領者による個人情報処理活動が本法規定の個人情報保護標準を満たすよう求めている 個保法では、重要情報インフラ運営者および処理する個人情報の件数が、国家ネットワーク情報部門が定める件数に達した個人情報処理者は、中国国内で収集および生成した個人情報を中国国内に保存しなければならないことを明記している 個保法では、事前に個人情報保護評価を行うよう求めている
法的責任	<ul style="list-style-type: none"> -

注：GB/T 35273-2020とは、「情報セキュリティ技術 個人情報セキュリティ規範」を指す。

個人情報保護コンプライアンス要件の理解



注：企業が個人情報保護業務を展開する際には、サイバーセキュリティ法、およびデータセキュリティ法におけるコンプライアンス要件にも配慮されるよう提案する。



個人情報保護機能を果たしている機関

❖ 国家インターネット情報弁公室

個人情報保護に係る監督・管理業務を統括的に調整する

❖ 国务院関連部門

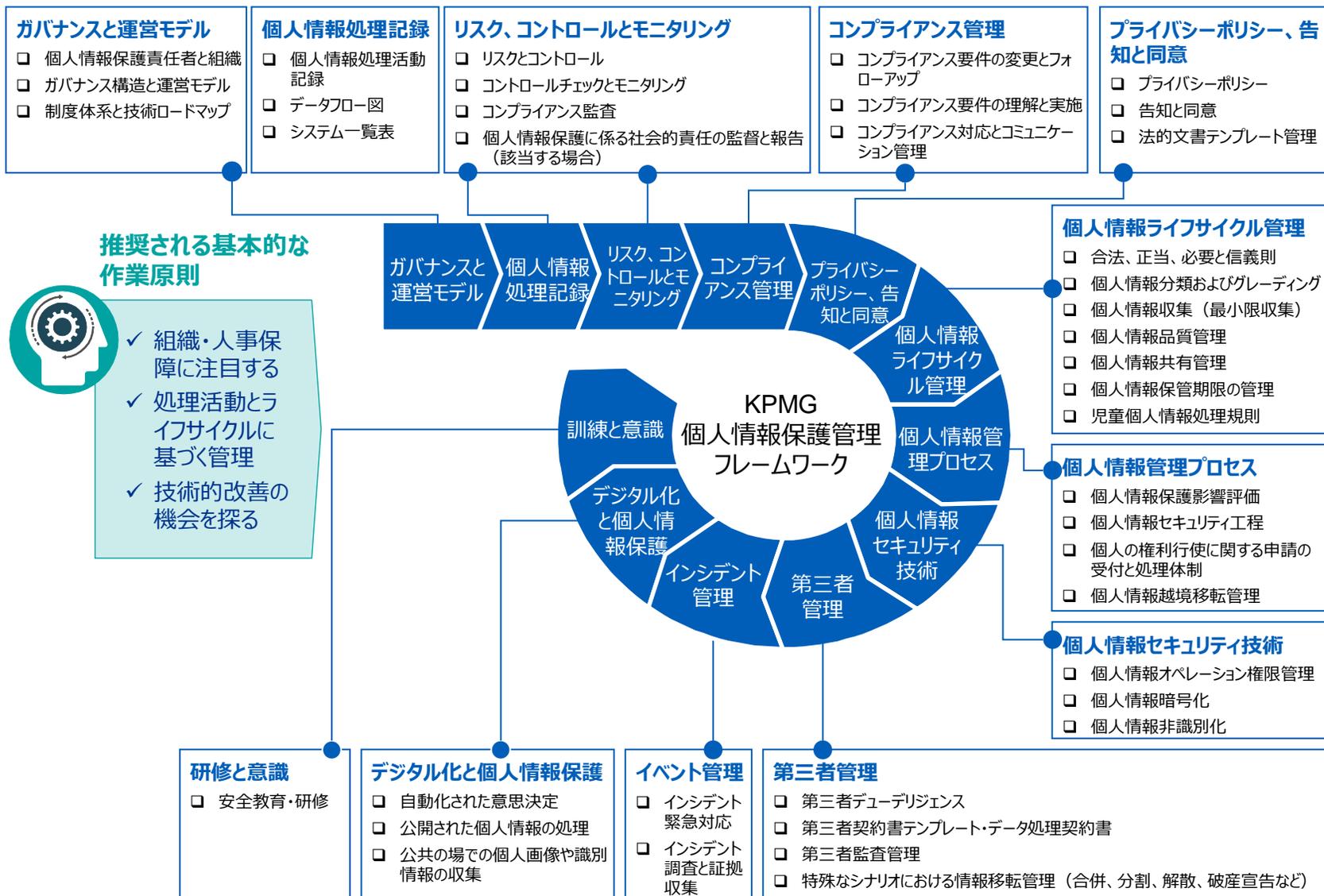
本法および関連する法律、行政法規に基づき、それぞれの責任範囲内で個人情報の保護および監督・管理に責任を負う

❖ 県レベル以上の地方人民政府の関連部門

国家の関連規定に従って個人情報保護と監督管理の職責を確定する



個人情報保護管理体制の構築・整備



優先的に実施すること



- ガバナンスと運営モデル
- 個人情報処理記録
- プライバシーポリシー、告知と同意
- 個人情報管理プロセス
- インシデント管理
- 研修と意識

重点的に把握すること



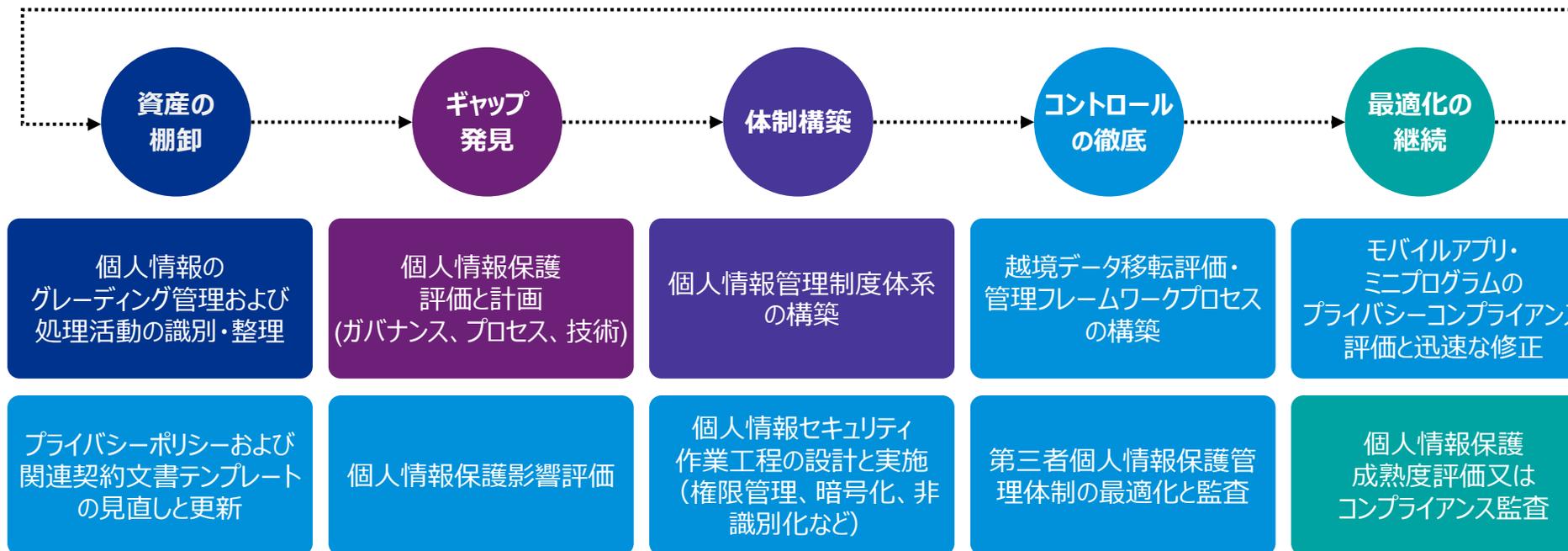
- コンプライアンス管理
- 個人情報のライフサイクル管理
- 個人情報セキュリティ技術
- 第三者管理
- デジタル化と個人情報保護

継続的に改善すること



- リスク、コントロールとモニタリング

個人情報保護課題に対するKPMGの支援内容



お問い合わせ先

石浩然 Henry Shek

KPMG中国
サイバーと情報セキュリティコンサルティング
パートナー
Tel : +852 2143 8799
henry.shek@kpmg.com

張倪海 Brian Cheung

KPMG中国
サイバーと情報セキュリティコンサルティング
ディレクター
Tel : +852 2847 5062
brian.cheung@kpmg.com

張令琪 Richard Zhang

KPMG中国
サイバーと情報セキュリティコンサルティング
パートナー
Tel : +86 (21) 2212 3637
richard.zhang@kpmg.com

黄芃芃 Quin Huang

KPMG中国
サイバーと情報セキュリティコンサルティング
ディレクター
Tel : +86 (21) 2212 2355
quin.huang@kpmg.com

郝長偉 Danny Hao

KPMG中国
サイバーと情報セキュリティコンサルティング
ディレクター
Tel : +86 (10) 8508 5498
danny.hao@kpmg.com

Global Japanese Practiceメンバー

華北



Ichiro Takabe
高部 一郎
Partner 北京・上海



Jenny Hui
許 秀儀
Partner 北京



Akihiko Kishi
岸 皓彦
Partner 北京



Lisa Li
李 輝
Partner 北京



Nan Jiang
姜 楠
Director 北京



Yixuan Min
閔 義鉉
Director 瀋陽

華中



Ichiro Takabe
高部 一郎
Partner 北京・上海



Tadashi Morimoto
森本 雅
Partner 上海



Masakazu Mokuta
李田 正和
Partner 上海



Zhewei Wang
王 哲蔚
Partner 上海



Naoko Hirasawa
平澤 尚子
Partner 上海



David Qian
錢 則徐
Director 上海



Hironori Hayashida
林田 弘徳
Partner 上海



Jie Xu
徐 潔
Partner 上海



Sky Yang
楊 佳枚
Director 上海、杭州

GBA



Vivian Chen
陳 蔚
Partner 深圳



Masakatsu Tamashiro
玉城 正勝
Director 広州



Keigo Yoshida
吉田 圭吾
Director 香港



Shigeru Inanaga
稲永 繁
Partner 深圳



Nancy Zheng
鄭 予輝
Director 広州



Chui Bayern
徐 建邦
Partner 香港



Ryan Li
李 良
Director 広州

お問合せ先

GJP China Markets:

gjpmarkets.china@kpmg.com

Tel: +86 (21) 2212 2247 (日本語)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG Advisory (China) Limited, a limited liability company in China and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.