

仮訳：「データ越境安全評価弁法（意見募集案）」

2021年10月29日に中華人民共和国の国家インターネット情報公弁室が公表した「データ越境安全評価弁法（意見募集案）」の仮訳を掲載いたします。

意見募集期間は2021年11月28日です。

[意見募集ページ]

[国家互联网信息办公室关于《数据出境安全评估办法（征求意见稿）》公开征求意见的通知](#)

執筆者：渡邊雅之

* 本ニュースレターに関するご相談などがありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所

弁護士渡邊雅之

TEL 03-5288-1021

FAX 03-5288-1025

Email m-watanabe@miyake.gr.jp

国家互联网信息办公室关于《数据出境安全评估办法（征求意见稿）》公开征求意见的通知

国家インターネット情報公弁室による「データ越境安全評価弁法（意見募集案）」の公開協議のお知らせ

为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，我办起草了《数据出境安全评估办法（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

1. 登录中华人民共和国司法部 中国政府法制信息网（www.moj.gov.cn、www.chinalaw.gov.cn），进入首页主菜单的“立法意见征集”栏目提出意见。
2. 通过电子邮件将意见发送至：shujuju@cac.gov.cn。
3. 通过信函将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络数据管理局，邮编：100044，并在信封上注明“数据出境安全评估办法征求意见”。

意见反馈截止时间为2021年11月28日。

データ越境の活動を規制し、個人情報の権益を保護し、国家安全と社会公共の利益を守り、国境を越えたデータの安全で自由な流れを促進するために、中華人民共和国ネットワークセキュリティ法、中華人民共和国データセキュリティ法、中華人民共和国個人情報保護法およびその他の法令に基づき、当事務所は「データ越境安全評価弁法（意見募集案）」を起草しました。現在、一般の方からのコメントを募集しています。一般の方からのご意見は、以下のような経路・手段でお寄せいただけます。

1. 中華人民共和国司法部 中国政府法律情報ネットワーク (www.moj.gov.cn, www.chinalaw.gov.cn) にアクセスし、ホームページのメインメニューの「立法意見集」からコメントを投稿する。
2. ご意見はメールで shujuju@cac.gov.cn までお送りください。
3. ご意見は、封筒に「Data Exit Security Assessment Measures for Comments」と明記の上、100044年北京市西城区車公庄街11号国家インターネット情報公弁室ネットワークデータ管理局宛に手紙でお送りください。

意見募集の締め切りは2021年11月28日です。

数据出境安全评估办法（征求意见稿）

データ越境安全評価弁法（意見募集案）

第一条 为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进

数据跨境安全、自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第1条 本办法は、データ越境活動を規制し、個人情報の権利と利益を保護し、国家安全保障と社会公共の利益を守り、国境を越えたデータの安全かつ自由な流れを促進するために、中華人民共和国ネットワークセキュリティ法、中華人民共和国データセキュリティ法、中華人民共和国個人情報保護法、およびその他の法令に基づいて制定される。

第二条 数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和依法应当进行安全评估的个人信息，应当按照本办法的规定进行安全评估；法律、行政法规另有规定的，依照其规定。

第2条 中華人民共和国での業務の過程で収集・生成された重要なデータおよび個人情報を、法律に基づいて安全評価を行うべき外国に提供する情報処理者は、本弁法の規定に従って安全評価を行わなければならない、法律または行政法規に別段の定めがある場合には、その規定に従って安全評価を行わなければならない。

第三条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。

第3条 データ越境の安全評価は、事前評価と継続的な監督の組み合わせ、およびリスクの自己評価とセキュリティ評価の組み合わせを主張し、データ越境のセキュリティリスクを防止し、本弁法に基づいて秩序あるデータの自由な流れを保証する。

第四条 数据处理者向境外提供数据，符合以下情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

- (一) 关键信息基础设施的运营者收集和产生的个人信息和重要数据；
- (二) 出境数据中包含重要数据；
- (三) 处理个人信息达到一百万人的个人信息处理者向境外提供个人信息；
- (四) 累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息；
- (五) 国家网信部门规定的其他需要申报数据出境安全评估的情形。

第4条 国外にデータを提供するデータ処理者は、次のいずれかの状況に該当する場合、その所在地の省のインターネット情報部門を通じて、国家インターネット情報公弁室にデータ越境の安全評価を申告しなければならない。

- (1) 重要情報インフラストラクチャー運用者が収集・生成する個人情報や重要なデータである場合。
- (2) 送信データには重要なデータが含まれている場合。
- (3) 中国国外で個人情報を提供する 100 万人に達する個人情報を処理する個人情報処理業者である場合。

(4) 外国への個人情報の累計提供数が10万人以上、または1万人以上のセンシティブ個人情報の提供する場合。

(5) その他、国家インターネット情報公弁室が規定するデータ越境安全評価の申告が必要な場合。

第五条 数据处理者在向境外提供数据前，应事先开展数据出境风险自评估，重点评估以下事项：

(一) 数据出境及境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

(二) 出境数据的数量、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

(三) 数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险；

(四) 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

(五) 数据出境和再转移后泄露、毁损、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等；

(六) 与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务。

第5条 データ処理者は、国外にデータを提供する前に、以下の事項に着目して、データの越境のリスクに関する事前の自己評価を行わなければならない。

(一) データ越境の合法性、正当性および必要性、ならびに国外の受領者によるデータ処理の目的、範囲および方法。

(二) 輸出されるデータの量、範囲、種類、および感度、およびデータの輸出が国家安全保障、公共の利益、および個人または組織の合法的な権利と利益に及ぼすリスク

(三) データ移転プロセスにおける情報処理者の管理上および技術上の対策と能力が、データの漏洩や破壊などのリスクを防止できるかどうか。

(四) 国外の受領者が負う責任と義務、およびその責任と義務を果たすための管理・技術的手段と能力が海外に移転するデータのセキュリティを保証できるかどうか。

(五) 輸出・再輸出後のデータの漏洩、破壊、改ざん、誤用等のリスクと、個人が個人情報の権利・利益を保護するためのルートが開かれているかどうか等。

(六) 海外の受領者と締結したデータ輸出関連契約において、データセキュリティ保護の責任と義務が適切に合意されているかどうか。

第六条 申报数据出境安全评估，应当提交以下材料：

(一) 申报书；

- (二) 数据出境风险自评估报告；
- (三) 数据处理者与境外接收方拟订立的合同或者其他具有法律效力的文件等（以下统称合同）；
- (四) 安全评估工作需要的其他材料。

第6条 データ越境安全評価を宣言するには、以下の書類を提出しなければならない。

- (1) 誓約書
- (2) データ流出のリスクに関する自己評価報告書。
- (3) 情報処理者と海外の受領者との間で締結された契約書その他の法的拘束力のある文書等（以下、総称して「契約書」という。）
- (4) その他安全評価に必要な資料。

第七条 国家网信部门自收到申报材料之日起七个工作日内，确定是否受理评估并以书面通知形式反馈受理结果。

第7条 国家インターネット情報公弁室は、申告資料の受領日から7営業日以内に、評価を受け入れるかどうかを決定し、書面による通知の形で受け入れ結果をフィードバックする。

第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：

- (一) 数据出境的目的、范围、方式等的合法性、正当性、必要性；
- (二) 境外接收方所在国家或者地区的数据安全保护政策法规及网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规规定和强制性国家标准的要求；
- (三) 出境数据的数量、范围、种类、敏感程度，出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险；
- (四) 数据安全和个人信息权益是否能够得到充分有效保障；
- (五) 数据处理者与境外接收方订立的合同中是否充分约定了数据安全保护责任义务；
- (六) 遵守中国法律、行政法规、部门规章情况；
- (七) 国家网信部门认为需要评估的其他事项。

第8条 データ越境安全評価は、データ越境活動が国家安全保障、公共の利益、および個人または組織の正当な権利と利益に及ぼす可能性のあるリスクを評価することに重点を置き、主に以下の事項を含む。

- (一) データ輸出の目的、範囲および方法の合法性、正当性および必要性
- (二) 国外の受領者が所在する国・地域のデータセキュリティ保護政策・規制およびネットワークセキュリティ環境が輸出データのセキュリティに与える影響、国外の受領者の

データ保護レベルが中華人民共和国の法律、行政法規および強制的な国家基準の要件を満たしているかどうか。

(三) 送出データの量、範囲、種類および感度、送出中および送出後のデータの漏洩、改ざん、紛失、破壊、転送または不正アクセス、不正使用のリスク

(四) データセキュリティおよび個人情報の権利と利益が完全かつ効果的に保護されるかどうか

(五) データ処理者と国外の受領者との間で締結された契約において、データのセキュリティ保護に関する責任と義務が適切に合意されているかどうか。

(六) 中国の法律、行政規則、部門規則の遵守

(七) その他、国家インターネット情報管理局が評価するために必要と考える事項。

第九条 数据处理者与境外接收方订立的合同充分约定数据安全保护责任义务，应当包括但不限于以下内容：

(一) 数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

(二) 数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者合同终止后出境数据的处理措施；

(三) 限制境外接收方将出境数据再转移给其他组织、个人的约束条款；

(四) 境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区法律环境发生变化导致难以保障数据安全时，应当采取的安全措施；

(五) 违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款；

(六) 发生数据泄露等风险时，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。

第9条 データ処理者と国外の受領者との間で締結される契約は、データセキュリティ保護の責任と義務について完全に合意しており、以下の内容を含むが、これに限定されるものではない。

(一) データの越境の目的と方法、データの範囲、国外の受領者によるデータ処理の目的と方法等。

(二) 国外でデータを保管する場所、その期間、および保管期間に達した後、合意された目的が完了した後、または契約が終了した後、国外に移転したデータを処理するための手段

(三) 国外の受領者が輸出されたデータを他の組織または個人に再譲渡することを制限する拘束条項

(四) 実質的な支配力や事業範囲に重大な変化が生じた場合や、国外の受領者が所在する国や地域の法的環境に変化が生じ、データの安全性を確保することが困難になった場合に、国外の受領者が講ずべきセキュリティ対策

(五) データ安全保護義務の違反に対する責任および拘束力と執行力のある紛争解決条

項

(六) 情報漏洩などのリスクが発生した場合の適切な緊急対応、および個人が個人情報の権利・利益を守るための円滑なルートの保護

第十条 国家网信部门受理申报后，组织行业主管部门、国务院有关部门、省级网信部门、专门机构等进行安全评估。

涉及重要数据出境的，国家网信部门征求相关行业主管部门意见。

第 10 条 国家インターネット情報公弁室は、申告を受理した後、管轄の業界部門、国务院の関連部門、省のインターネット情報部門、専門機関を組織して、安全評価を行う。

2 重要なデータの越境が関係する場合、国家インターネット情報公弁室は、関連業界の主管部門の意見を求める。

第十一条 国家网信部门自出具书面受理通知书之日起四十五个工作日内完成数据出境安全评估；情况复杂或者需要补充材料的，可以适当延长，但一般不超过六十个工作日。

评估结果以书面形式通知数据处理者。

第 11 条 国家インターネット情報公弁室は、受理通知書の発行日から 45 営業日以内に、データ越境安全評価を完了しなければならない。状況が複雑な場合や追加資料が必要な場合は、適切に延長することができるが、通常は 60 営業日を超えないものとする。

2 評価の結果は、データ処理者に書面で通知するものとする。

第十二条 数据出境评估结果有效期二年。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：

(一) 向境外提供数据的目的、方式、范围、类型和境外接收方处理数据的用途、方式发生变化，或者延长个人信息和重要数据境外保存期限的；

(二) 境外接收方所在国家或者地区法律环境发生变化，数据处理者或者境外接收方实际控制权发生变化，数据处理者与境外接收方合同变更等可能影响出境数据安全的；

(三) 出现影响出境数据安全的其他情形。

有效期届满，需要继续开展原数据出境活动的，数据处理者应当在有效期届满六十个工作日前重新申报评估。

未按本条规定重新申报评估的，应当停止数据出境活动。

第 12 条 データ越境評価の結果は、2 年間有効とする。データ処理者は、有効期間中に以下のいずれかの状況が発生した場合、評価を再申告するものとする。

(一) 国外の相手先に提供されるデータの目的、方法、範囲、種類、および国外の受領者でのデータ処理の用途や方法の変更、または個人情報や重要なデータの国外での保管期間の延長。

(二) 国外の受領者が所在する国または地域の法的環境の変化、情報処理者または海外の

受領者の実質的な支配力の変化、情報処理者と国外の受領者との間の契約の変更など、送信データのセキュリティに影響を与える可能性のあるもの。

(三) その他、送信データのセキュリティに影響を与える状況が発生した場合。

2 有効期間が満了し、当初のデータ輸出活動を継続する必要がある場合、データ処理者は有効期間満了の 60 営業日前に評価を再申告するものとする。

3 本条の規定に従って評価が再申告されない場合は、データ輸出活動を中止するものとする。

第十三条 数据处理者应当按照本办法的规定提交评估材料，材料不齐全或者不符合要求的，应当及时补充或者更正，拒不补充或者更正的，国家网信部门可以终止安全评估；数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理。

第 13 条 データ処理者は、本弁法の規定に従って評価資料を提出しなければならない、資料が不完全であったり、要件を満たしていない場合は、適時に補足または修正しなければならない、補足または修正を拒否した場合は、国家ネットワーク情報公弁室は安全評価を終了することができる。データ処理者は、提出された資料の真正性に責任を負い、意図的に虚偽の資料を提出した場合は、評価ができなかったものと扱われる。

第十四条 参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第 14 条 安全評価業務に携わる関係機関および人員は、国家機密、個人のプライバシー、個人情報、商業機密、業務上の秘密情報および職務遂行上知り得たその他のデータを、法律に基づいて秘密に保持し、他人に開示したり、不正に提供したりしてはならない。

第十五条 任何组织和个人发现数据处理者未按照本办法规定进行评估向境外提供数据的，可以向省级以上网信部门投诉、举报。

第 15 条 データ処理者が本弁法の規定に従って国外にデータを提供するための審査を行っていないことを発見した組織または個人は、省レベル以上のインターネット情報部門に苦情または報告を提出することができる。

第十六条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当撤销评估结果并书面通知数据处理者，数据处理者应当终止数据出境活动。需要继续开展数据出境活动的，数据处理者应当按照要求进行整改，并在整改完成后重新申报评估。

第 16 条 国家インターネット情報公弁室は、評価に合格したデータ輸出活動が実際の処理過程でデータ輸出セキュリティ管理要求事項を満たさなくなったと判断した場合、評

価結果を撤回し、データ処理者に書面で通知し、データ処理者はデータ輸出活動を終了しなければならない。データ輸出活動を継続して行う必要がある場合、データ処理者は要求事項に従って修正を行い、修正完了後に評価を再申請しなければならない。

第十七条 違反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。

第 17 条 本弁法の規定に違反した場合は、「中華人民共和国ネットワーク安全法」、「中華人民共和国データセキュリティ法」、「中華人民共和国個人情報保護法」およびその他の法令の規定に基づいて処理され、犯罪に該当する場合は、法令に基づいて刑事責任が追及される。

第十八条 本办法自 年 月 日起施行。

第 18 条 本弁法は、年 月 日より施行される。

(参考) 越境データ移転に関する規定

○中華人民共和国ネットワーク安全法

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第 31 条 国は、ネットワークセキュリティレベルの保護システムに基づき、公共通信・情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政府その他の重要な産業・分野、及びその他の重要な情報インフラであって、損傷、機能喪失、データ漏洩が発生した場合に国家安全保障、国民生活、公共の利益に重大な危険を及ぼす可能性のあるものについて、重点的な保護を実施するものとする。重要情報インフラストラクチャーの具体的な範囲及び安全保護に関する弁法は、国務院が策定する。

2 国は、重要情報インフラストラクチャー以外のネットワーク事業者が、重要情報インフラストラクチャー保護システムに自主的に参加することを奨励している。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第 32 条 国務院が定めた責任分担に基づき、重要情報インフラストラクチャーの安全保護を担当する部門は、それぞれ自分の産業・分野における重要情報インフラストラクチャーの安全計画の実施を準備・整理し、重要情報インフラストラクチャーの運用の安全保護を指導・監督する。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第 33 条 重要情報インフラストラクチャーの構築は、それが事業の安定性及び継続的な運用をサポートする性能を備えていることを保証し、安全上の技術的措置が同時に計画、構築及び使用されることを保証するものとする。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

(一) 设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

- (二) 定期对从业人员进行网络安全教育、技术培训和技能考核;
- (三) 对重要系统和数据库进行容灾备份;
- (四) 制定网络安全事件应急预案, 并定期进行演练;
- (五) 法律、行政法规规定的其他义务。

第 34 条 重要情報インフラストラクチャー事業者は、本法第 21 条の規定に加えて、以下のセキュリティ保護義務を履行しなければならない。

- (一) 特別なセキュリティ管理機関および安全管理担当者を設置し、当該担当者及び重要な地位にある者のセキュリティバックグラウンドチェックを行うこと。
- (二) 実務者向けのサイバーセキュリティ教育、技術研修、スキル評価を定期的に行う。
- (三) 重要なシステムやデータベースの耐災害性のあるバックアップ。
- (四) ネットワーク・セキュリティ・インシデントに対する緊急計画の策定および定期的な訓練の実施。
- (五) その他法律や行政法規で定められた義務。

第三十五条 关键信息基础设施的运营者采购网络产品和服务, 可能影响国家安全的, 应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第 35 条 重要情報インフラストラクチャー事業者は、国家安全に影響を与える可能性のあるネットワーク製品・サービスを調達する場合、國務院の関連部門と連携して国家インターネット情報公弁室が組織する国家安全審査に合格しなければならない。

第三十六条 关键信息基础设施的运营者采购网络产品和服务, 应当按照规定与提供者签订安全保密协议, 明确安全和保密义务与责任。

第 36 条 ネットワーク製品・サービスを調達する重要情報インフラストラクチャー事業者は、規定に基づき、提供者とセキュリティ・機密保持契約を締結し、セキュリティ・機密保持の義務と責任を明確にしなければならない。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。

因业务需要, 确需向境外提供的, 应当按照国家网信部门会同国务院有关部门制定 的办法进行安全评估; 法律、行政法规另有规定的, 依照其规定。

第 37 条 重要情報インフラストラクチャー運営者によって、中華人民共和国の国内において業務上、収集および生成された個人情報および重要なデータは、国内に保存されるものとする。

業務上、中国国外に提供する必要がある場合は、国家インターネット情報公弁室が國務院の関連部門と共同で策定した弁法に従って安全評価を行う。法律または行政規則で別の規定がある場合は、その規定に従うものとする。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第 66 条 重要情報インフラストラクチャー運営者が本法第 37 条の規定に違反してネットワークデータを国外に保存し、またはネットワークデータを国外に提供した場合、関係当局は是正を命じ、警告を發し、違法所得を没収し、5 万元以上 50 万元以下の罰金を科し、さらに関連事業の停止、事業是正の停止、ウェブサイトの閉鎖、関連事業免許の取消し、事業免許の取消しを命じることができる。責任者およびその他の直接の責任者は、1 万元以上 10 万元以下の罰金に処する。

○中華人民共和国データセキュリティ法

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第 31 条 中華人民共和国の国内の重要情報インフラストラクチャー運営者によって収集及び生成された重要なデータの海外越境の安全管理は、中華人民共和国ネットワーク安全法の規定に準拠するものとする。他のデータ処理者は中華人民共和国国内業務で収集及び生成された重要なデータの海外越境安全管理措置は、中国國務院の関連部門と共同で中国国家インターネット情報安全公弁室によって策定されるものとする。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第 46 条 本法第 31 条の規定に違反し、海外で重要なデータを提供する者に対しては、関係する所管官庁からは是正を命じられ、警告を受け、同時に 10 万元から 100 万元までの罰金を科すことができる。担当の直接責任者およびその他の直接責任者は、1 万元から 10 万元の罰金を科すことができる。状況が深刻な場合は、100 万元から 1000 万元未満の罰金を科すことができる。営業の一時停止、是正のため閉鎖、関連事業免許の取消し又は取消し、直接の責任者その他の直接の責任者は、10 万元から 100 万元の罰金を科される場

合がある。

○中国個人情報保護法

第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第 40 条 重要情報インフラストラクチャ—運営者及び国家インターネット情報公弁室によって定められた数を超える個人情報を処理する個人情報処理者は、中華人民共和国の国内で収集及び生成された個人情報を保存するものとする。真に国外に提供する必要がある場合は、国家インターネット情報公弁室が主催する安全評価に合格しなければならない。法律、行政規則、国家インターネット情報公弁室が安全評価を不要であると規定している場合は、当該手続に従うものとする。

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第 66 条 個人情報が本法の規定に違反して処理される場合、又は個人情報の処理が本法に基づく個人情報保護義務を履行していない場合、監督機関は、是正を命じ、警告を発し、没収するものとする。個人情報の処理に関しては、サービスの提供を停止又は終了するよう命じられ、是正を拒否された場合は、100 万元未満の罰金が科せられる。担当者及びその他の直接責任者は、10,000 元以上、100,000 元以下の罰金を科されるものとする。

2 前項の違法行為があり、事態が深刻な場合は、省レベル以上の監督機関が、是正を命じ、違法な利益を没収し、5000 万元以下又は前年の売上高の 5 % 未満の罰金を科す。また、関連事業の停止または是正のための事業の停止を命じたり、関連する管轄当局に関連する事業許可を取り消すか、事業許可を取り消すように通知するか、直接責任者及びその他の直接責任のある担当者に 10 万元以上最高 100 万元の罰金を科すこともできる。また、一定期間内に、関連会社の取締役、監督者、上級管理職および個人情報保護の責任者を務めることを禁止する場合がある。