



世民律師事務所 SHIMIN LAW OFFICES

简析《个人信息出境标准合同办法》

国家互联网信息办公室于 2023 年 2 月 24 日发布《个人信息出境标准合同办法》^{【1】}，该办法自今年 6 月 1 日起施行。

订立个人信息出境标准合同属于《中华人民共和国个人信息保护法》第三章“个人信息跨境提供的规则”第 38 条^{【2】}规定的个人信息出境合规途径之一，该条款列举了境内个人信息处理者向境外提供个人信息的可行途径包括：①通过安全评估；②申请安全认证；③与境外接收方订立标准合同；④法律、行政法规或者国家网信部门规定的其他方式。

截至目前，安全评估之《数据出境安全评估办法》^{【3】}已于 2022 年 9 月 1 日正式施行，安全认证之《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》^{【4】}也于 2022 年 12 月 16 日公布，此次《个人信息出境标准合同办法》的出台，使得《个人信息保护法》项下的个人信息出境合规途径在具体操作时全都有了可供遵循的依据。

本文仅对《个人信息出境标准合同办法》简要分析如下：

一、适用主体

《个人信息出境标准合同办法》第 4 条规定，个人信息处理者只有同时满足以下条件，才

¹ 《个人信息出境标准合同办法》（国家互联网信息办公室令第 13 号，自 2023 年 6 月 1 日起施行）

² 《个人信息保护法》（第十三届全国人民代表大会常务委员会第三十次会议通过，自 2021 年 11 月 1 日起施行）

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

- （一）依照本法第四十条的规定通过国家网信部门组织的安全评估；
- （二）按照国家网信部门的规定经专业机构进行个人信息保护认证；
- （三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；
- （四）法律、行政法规或者国家网信部门规定的其它条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

³ 《数据出境安全评估办法》（国家互联网信息办公室令第 11 号，自 2022 年 9 月 1 日起施行）

⁴ <https://www.tc260.org.cn/front/postDetail.html?id=20221216161852>

能选择订立标准合同后向境外提供个人信息：①非关键信息基础设施运营者；②处理个人信息不满 100 万人；③自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人；④自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人；⑤不属于法律、行政法规或者其他国家网信部门规定限制出境的情形（例如《国家健康医疗大数据标准、安全和服务管理办法（试行）》第 30 条等）。

同时该条第 3 款明确禁止个人信息处理者采取数量拆分等手段逃避出境安全评估的行为。

如果个人信息处理者不能同时满足以上情形，就不得不放弃订立标准合同而寻求安全评估和安全认证的方式向境外提供个人信息。

二、适用步骤

《个人信息出境标准合同办法》第 5 条、第 6 条及第 7 条分别规定了通过订立标准合同的方式向境外提供个人信息的步骤。

(一) 首先，个人信息处理者向境外提供个人信息前须开展个人信息保护影响评估，制作评估报告。其中重点评估内容如下：

- 1) 个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；
- 2) 出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；
- 3) 境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；
- 4) 个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
- 5) 境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；
- 6) 其他可能影响个人信息出境安全的事项。

(二) 其次，个人信息处理者须与境外接收方签订标准合同，其内容必须严格遵循《个人信息出境标准合同办法》所附合同文本【5】，国家网信部门可以调整该版本内容。该版本内容包括合同正文、附录一“个人信息出境说明”、附录二“双方约定的其他条款（如需要）”，合同双方当事人不得变更合同正文的内容，如双方拟约定与正文不同的内容的，可以记载在附录二。标准合同生效后即可开展个人信息出境活动。

(三) 再次，个人信息处理者应当在标准合同生效之日起 10 个工作日内持标准合同和个人

⁵<https://resources.pkulaw.cn/staticfiles/fagui/20230224/15/31/0/f392a25392ea107a4926b3994bcc3521.pdf>

信息保护影响评估报告向所在地省级网信部门备案。

(四) 最后，需要提醒的是，《个人信息出境标准合同办法》第 8 条规定，在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

- 1) 向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；
- 2) 境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；
- 3) 可能影响个人信息权益的其他情形。

三、适用对象

《个人信息出境标准合同办法》自今年 6 月 1 日起施行，但根据该办法第 13 条的规定，其适用的对象不仅限于施行后的个人信息出境活动，施行前的个人信息出境活动也将受到该办法的规制，且限定整改时限为该办法施行之日起 6 个月内完成。

四、法律责任

个人信息处理者如因任何组织或个人的举报（第 10 条）或者备案材料的真实性存在问题（第 7 条）等，而被省级以上网信部门发现个人信息出境活动存在较大风险或者发生个人信息安全事件的，将被要求约谈、整改，甚至承担行政乃至刑事责任。

如您对本内容有任何疑问，敬请联系：info@shiminlaw.com

本资料的著作权归世民律师事务所（以下简称“世民”）所有，请勿擅自引用、更改、转印或复印本资料。

本资料是仅供理解法律法规内容而制作的，不包括对于法律法规的解释、说明或解读等。

「個人情報越境移転標準契約弁法」簡易分析

2023 年 5 月 8 日

国家インターネット情報弁公室から 2023 年 2 月 24 日に「個人情報越境移転標準契約弁法」【⁶】が公布され、今年 6 月 1 日に施行されます。

個人情報越境移転標準契約の締結は、「中華人民共和国個人情報保護法」第 3 章「個人情報越境提供の規則」第 38 条【⁷】に規定される個人情報越境移転に準拠したルートの一つです。当該条項に列挙されている、国内の個人情報取扱者が国外に個人情報を提供可能なルートは次のとおりです。①安全評価の通過、②安全認証の申請、③国外受領者との標準契約締結、④法律、行政法規又は国のインターネット情報部門が規定するその他の方法。

現時点で、安全評価については「データ越境移転安全評価弁法」【⁸】が 2022 年 9 月 1 日に正式に施行、安全認証についても「サイバーセキュリティ標準実践ガイドライン-個人情報越境取扱活動安全認証規範 V2.0」【⁹】が 2022 年 12 月 16 日に公布され、今回の「個人情報越境移転標準契約弁法」の公布により、「個人情報保護法」に定める個人情報越境移転を遵守するルートすべてについて、具体的に取扱う際に従うべき根拠が整いました。

本稿が「個人情報越境移転標準契約弁法」に絞って簡易分析は以下のとおりです。

一、適用主体

「個人情報越境移転標準契約弁法」第 4 条には、個人情報取扱者は以下の条件を同時に満たす場合に限り、標準契約を締結した後に国外に個人情報を提供することを選択することができますと規定されています。①重要情報インフラ運営者に該当しないこと、②取り扱う個人情報 100 万人未満であること、③前年 1 月 1 日から累計して国外への個人情報の提供が 10 万人未満であること、④前年 1 月 1 日から国外への機微個人情報の提供が累計 1 万

⁶ 「個人情報越境移転標準契約弁法」（国家インターネット情報弁公室令第 13 号、2023 年 6 月 1 日施行）

⁷ 「個人情報保護法」（第 13 期全国人民代表大会常務委員会第 30 回会議にて可決、2021 年 11 月 1 日施行）

第 38 条 個人情報取扱者が業務等の必要性により、確かに中華人民共和国国外に個人情報を提供する必要が確にある場合、下記に掲げる条件の一つを備えていなければならない。

(1) 本法第 40 条の規定により国のインターネット情報部門を通じて組織される安全評価を通過すること。

(2) 国のインターネット情報部門の規定に従い、専門機関が行う個人情報保護認証を受けること。

(3) 国のインターネット情報部門が制定する標準契約に従い、国外受領者と契約を締結し、双方の権利と義務を約定すること。

(4) 法律、行政法規又は国のインターネット情報部門が規定するその他条件。

中華人民共和国国外への個人情報提供の条件等について中華人民共和国が締結又は参加する国際条約、協定に規定がある場合、当該規定に従い執行することができる。

個人情報取扱者は、必要な措置を講じ、国外受領者による個人情報の取扱活動が本法に規定する個人情報保護基準に達することを保障しなければならない。

⁸ 「データ越境移転安全評価弁法」（国家インターネット情報弁公室令第 11 号、2022 年 9 月 1 日施行）

⁹ <https://www.tc260.org.cn/front/postDetail.html?id=20221216161852>

人未満であること、⑤法律、行政法規又はその他国のインターネット情報部門が規定する越境移転の制限に該当しないこと（例えば、「国家健康医療ビッグデータ基準、安全及びサービス管理弁法（試行）」第 30 条など）。

また当該条項の第 3 項では、個人情報取扱者が数量分割等の手段を採用して越境移転安全評価を回避する行為を明確に禁止しています。

個人情報取扱者が上記の事由を同時に満たすことができない場合、標準契約の締結を放棄し、安全評価又は安全認証の形で国外に個人情報を提供しなければなりません。

二、適用手順

「個人情報越境移転標準契約弁法」第 5 条、第 6 条及び第 7 条では、標準契約の締結を通じた国外への個人情報の提供手順がそれぞれ規定されています。

（一） まず、個人情報取扱者は、国外に個人情報を提供する前に、個人情報保護影響評価を行い、評価報告書を作成しなければなりません。そのうち、重点的に評価する内容は以下の通りです。

- （1） 個人情報取扱者及び国外受領者による個人情報の取扱いの目的、範囲、方法等の適法性、正当性、必要性
- （2） 越境移転する個人情報の規模、範囲、種類、機微度合い、及び個人情報の越境移転が個人情報権益にもたらす可能性のあるリスク
- （3） 国外受領者が承諾する義務、並びに義務履行の管理及び技術的措置、能力等について越境移転する個人情報の安全を保障することができるか否か
- （4） 個人情報が越境移転後に改ざん、破壊、漏洩、紛失及び不法利用等に遭うリスク、個人情報権益を維持・保護する経路がスムーズである等
- （5） 国外受領者の所在国又は地域における個人情報保護政策及び法規が標準契約の履行に及ぼす影響
- （6） 個人情報の越境移転の安全性に影響を及ぼす可能性のあるその他事項。

（二） 次に、個人情報取扱者は国外受領者と標準契約を締結し、その内容は「個人情報越境移転標準契約弁法」に添付される契約文書【¹⁰】に厳格に準拠していなければならない。国のインターネット情報部門は当該バージョンの内容を調整することができます。当該バージョンの内容は、契約の本文、付属書一「個人情報越境移転説明」、付属書二「双方が約定したその他条項（必要な場合）」を含みます。契約の双方当事者は、契約本文の内容を変更してはなりません。双方が契約本文の内容と抵触しない場合において本文と異なる内容を約定する場合には、付属書二に記載することができます。標準契約の発効後に個人情報の国外越境移転活動を行うことができます。

（三） 続いて、個人情報取扱者は標準契約の発効日から 10 営業日以内に標準契約及び個

¹⁰

<https://resources.pkulaw.cn/staticfiles/fagui/20230224/15/31/0/f392a25392ea107a4926b3994bcc3521.pdf>

個人情報保護影響評価報告書を持参し、所在地の省級インターネット情報部門に届出なければなりません。

- (四) 最後に、注意を要する点として、「個人情報越境移転標準契約弁法」第 8 条の規定によると、標準契約の有効期間内に次の状況のいずれかが発生した場合、個人情報取扱者は、個人情報保護影響評価を再度行い、標準契約を補足又は再締結し、かつ、相応の届出手続を履行しなければなりません。

- (1) 国外への個人情報提供の目的、範囲、種類、機微度合い、方法、保存場所若しくは国外受領者による個人情報取扱の用途、方法に変化が生じた場合、又は個人情報の国外保存期間を延長した場合。
- (2) 国外受領者の所在する国又は地域の個人情報保護政策及び法規に変化が生じる等、個人情報の権益に影響を及ぼす可能性がある場合。
- (3) 個人情報の権益に影響を及ぼす可能性があるその他事由。

三、適用対象

「個人情報越境移転基準契約弁法」は今年 6 月 1 日に施行されますが、同弁法第 13 条の規定によると、その適用対象は施行後の個人情報越境移転活動に限らず、施行前の個人情報越境移転活動も同弁法の規制を受け、かつ、是正期限は同弁法施行日から 6 ヶ月内に完了するよう限られています。

四、法的責任

個人情報取扱者は、いかなる組織や個人の通報（第 10 条）又は届出資料の真実性に問題がある（第 7 条）等により、省級以上のインターネット情報部門によって個人情報の越境移転活動に大きなリスクがあることを発見された場合、又は個人情報のインシデントが発生した場合、事情聴取、是正、さらには行政ないし刑事責任を負うことを要求されことになります。

注：上記情報は公開されている各種公式情報に基づき収集整理した情報であり、一般的な参考情報として供することを目的としてのみ作成されたものです。上記情報に含まれる内容は政策および法律改正等の要因により、通知なしに変更される可能性があり、その正確性および確実性を保証するものではなく、弊所は上記情報の全部又は一部に起因するいかなる直接又は間接的な損失および損害に対して、いかなる責任も負いません。

上記情報に関するご不明点は、下記担当者までお問合せください。

日本窓口：
黒田（東京）

中国大陸窓口：
中野（大連）
坂口（上海）

info@shiminlaw.com

Brief Analysis of the Measures on the Standard Contract for the Outbound Transfer of Personal Information

8 May 2023

On 24 February 2023, the Cyberspace Administration of China (the “CAC”) published the *Measures on the Standard Contract for the Outbound Transfer of Personal Information* (the “Standard Contract Measures”) [¹¹], which shall come into force on 1 June 2023.

Concluding a standard contract for the outbound transfer of personal information is one of the legal approaches for the outbound transfer of personal information as provided in Article 38 [¹²] of Chapter 3 - Rules on Cross-Border Provision of Personal Information of the *Personal Information Protection Law of the People’s Republic of China* (the “PIPL”). Article 38 of the PIPL outlines the routes available to personal information processors for transferring personal information out of the People's Republic of China, including: (1) passing the security assessment by the CAC; (2) obtaining personal information protection certification; (3) entering into a Standard Contract with the overseas recipient; (4) fulfilling the requirements as stipulated in other laws or administrative regulations, or by the state cyberspace authorities.

Up to now, the *Measures on the Security Assessment of Outbound Data Transfer* [¹³] for the security

¹¹ **Measures on the Standard Contract for the Outbound Transfer of Personal Information** (Order No.13 of the Cyberspace Administration of China), effective on 1 June 2023.

¹² **Personal Information Protection Law of the People’s Republic of China** (Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress, effective on 1 November 2021).

Article 38 of the PIPL:

Where personal information processors truly need to provide personal information outside the borders of the People’s Republic of China for business or other such requirements, they shall meet one of the following conditions:

- (1) Passing a security assessment organized by the national cyberspace administration department according to Article 40 of this law;
- (2) Undergoing personal information protection certification conducted by a specialized body according to provisions by the national cyberspace administration department;
- (3) Concluding a contract with an overseas recipient in accordance with a standard contract formulated by the national cyberspace administrative department, agreeing on the rights and obligations of both sides;
- (4) Other conditions provided in laws or administrative regulations or by the national cyberspace administrative department.

Where treaties or international agreements that the People’s Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal information outside the borders of the People’s Republic of China, those provisions may be carried out.

Personal information processors shall adopt necessary measures to ensure that overseas recipients’ personal information handling activities reach the standard of personal information protection provided in this Law.

¹³ **Measures for Security Assessment of Outbound Data Transfer** (Announcement No.11 of the Cyberspace

assessment was officially implemented on 1 September 2022, and the *Practical Guidelines for Cybersecurity Standards – Specifications on Security Certification for Cross-Border Processing of Personal Information V2.0* [14] for security certification was issued on 16 December 2022. Along with the Standard Contract Measures, these documents provide the compliance basis for the outbound transfer of personal information under PIPL.

This article will provide a brief analysis of the Standard Contract Measures as follows:

1. Scope of Application

According to Article 4 of the Standard Contract Measures, any personal information processor transferring personal information overseas by entering into a Standard Contract shall meet all of the following conditions: (1) it is not a critical information infrastructure operator; (2) it processes the personal information of less than 1 million persons; (3) since 1 January of the preceding year, it has cumulatively provided the personal information of less than 100,000 persons overseas; (4) since 1 January of the preceding year, it has cumulatively provided the sensitive personal information of less than 10,000 persons overseas; and (5) it does not fall within the circumstances of restricting the outbound transfer of personal information prescribed by laws, administrative regulations or the national cyberspace administration department (for instance, Article 30 of the *Administrative Measures on National Health and Medical Care Big Data Standards, Security and Services (Trial)*, etc.).

At the same time, it is explicitly prohibited by paragraph 3 of this article that personal information processors shall not use quantity splitting or similar methods to escape the security assessment of outbound data transfer.

If a personal information processor does not satisfy any of the above conditions, it will have to give up the approach of entering into a Standard Contract and reply on other approaches of passing the security assessment or obtaining personal information protection certification to transfer personal information overseas.

2. General Process

The general process for a personal information processor to transfer personal information overseas by entering into a Standard Contract is as follows (Article 5, Article 6, and Article 7 of the Standard Contract Measures):

(五) Before the outbound transfer of personal information, the personal information processor shall conduct a Personal Information Protection Impact Assessment (the “PIPIA”) and produce a

Administration of China, it was effective on September 1, 2022)

¹⁴ <https://www.tc260.org.cn/front/postDetail.html?id=20221216161852>

PIPIA Report. The PIPIA shall mainly focus on the following matters:

- (1) the legality, legitimacy and necessity of the purpose, scope and method of the personal information processing by the personal information processor and the overseas recipient;
- (2) the scale, scope, type, and sensitivity of the personal information to be transferred overseas, and the risks that outbound transfer may pose to the rights and interests of the personal information;
- (3) the responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management and technical measures and capabilities of the overseas recipient to perform such responsibilities and obligations are sufficient to ensure the security of the personal information to be transferred overseas;
- (4) the risk of the personal information being tampered with, destroyed, disclosed, lost, or illegally used after it is transferred overseas, and whether the channels for protecting the rights and interests of the personal information are unobstructed;
- (5) the impact of personal information protection policies and regulations in the country or region where the overseas recipient is located on the performance of the Standard Contract; and
- (6) other matters that may affect the security of the personal information to be transferred overseas.

(六) The Standard Contract that is signed between the personal information processor and the overseas recipient (the “Parties”) shall strictly adhere to the template provided as the Appendix to the Standard Contract Measures [15], and the national cyberspace administration department may adjust this template accordingly. The full template includes the main body of the Standard Contract, the Appendix I – *Instructions on the Outbound Transfer of Personal Information* and the Appendix II – *Other Terms Agreed by the Parties (if necessary)*. The Parties shall not modify the main body of the contract. The Parties may agree on other terms in Appendix II, as long as they do not conflict with the main body of the contract. The outbound transfer of personal information can only be carried out after the Standard Contract takes effect.

(七) The personal information processor shall file for record the Standard Contract and the PIPIA report with the cyberspace administration department at the provincial level within 10 working days from the effective date of the Standard Contract.

(八) It should be noted, according to Article 8 of the Standard Contract Measures, if any of the following circumstances occurs during the validity period of the Standard Contract, the personal information processor shall conduct a new PIPIA, supplement or re-conclude the Standard Contract, and perform the corresponding filing procedures:

- (1) change in the purpose, scope, type, sensitivity, manner, and place of storage of the personal information transferred to the overseas recipient, or change in the use or manner of the

¹⁵ The full template can be found at <https://resources.pkulaw.cn/staticfiles/fagui/20230224/15/31/0/f392a25392ea107a4926b3994bcc3521.pdf>

- processing of the personal information by the overseas recipient, or the period of storage of personal information is extended;
- (2) change of the personal information protection policies and regulations of the country or region where the overseas recipient is located that may affect the rights and interests of personal information;
 - (3) other circumstances that may affect the rights and interests of personal information.

3. Effective Date and Transition Period

The Standard Contract Measures will come into effect on 1 June 2023, and they shall apply to (1) the outbound transfers of personal information that occur after the date; and (2) the outbound transfers of personal information that occur before the date, according to Article 13 of the Standard Contract Measures. The outbound transfers of personal information that occur before the date shall be rectified to comply with the Standard Contract Measures within 6 months from the date if there are any inconsistencies.

4. Legal Liabilities

If the personal information processor is reported any case by any organization or individual (Article 10) or the filing documents have any authenticity issues (Article 7) or other circumstances that the cybersecurity administration department at or above the provincial level finds relatively large risks in the outbound transfer of the personal information by the personal information processor or any personal information security incidents occur, the personal information processor will be required for the interview, rectification, administrative liabilities or even criminal liabilities.

If you have any questions about this article, please contact: info@shiminlaw.com

The copyright of the English translation of this document is property of Shimin Law Offices ("Shimin"). No part of this document may be reproduced, distributed, copied, modified or adapted without the prior written consent of Shimin. The purpose of this document is to serve as reference for understanding the meaning of Chinese laws and regulations. It is not intended to explain, interpret, or describe the laws and regulations themselves.