LATHAM&WATKINS
瑞生国际律师事务所

客户通讯
评论

瑞生国际律师事务所隐私及网络业务组 2023年2月28日 | 第3076号

中国明确个人信息保护认证制度

中国国家市场监督管理总局（市场监管总局）与国家互联网信息办公室（网信办）联合发布了关于数据跨境转移认证制度的新规则，概述了个人信息处理者须符合的标准。

要点：

- **扩大后的适用范围：**《认证规范V2.0》明确说明认证实施程序适用于个人信息跨境转移到中国境外的*所有*情况。在《认证规范》上一个版本中，认证实施程序似乎仅适用于集团内数据转移和境外个人信息处理者的个人信息转移等两项活动。

- **认证实施程序的框架：**《认证规则》概述了认证实施程序的三个主要阶段：即(i) 技术验证，(ii) 现场审核，以及(iii) 获证后监督。认证机构相当可能会出台进一步的实际操作规则和指引。

- **CCRC被委任为首个认证机构**：中国网络安全审查技术与认证中心（CCRC）已在其网页中公告，其已被网信办指定为《个人信息保护法》项下的认证中心之一，将通过其营运的在线门户网站受理认证申请。在拟备本客户通讯之时，CCRC为可发出认证的唯一指定机构。

背景

《认证规则》

2022年11月18日，中国国家市场监督管理总局（市场监管总局）与国家互联网信息办公室（网信办）联合发布了《关于实施个人信息保护认证的公告》，该公告中附有《个人信息保护认证实施规则》（《认证规则》）（见中文版本）。《认证规则》明确说明个人信息保护认证（认证）的适用范围及取得有关认证的程序，以促进《个人信息保护法》（PIPL）项下的数据跨境传输活动。

要点重述：转移数据到中国境外的三大方法

《个人信息保护法》规定了个人信息处理者将个人信息转移至中华人民共和国（中国）境外的三个机制：

1. **安全评估：**在进行数据出境前，通过网信办组织的安全评估（安全评估）。个人信息处理者在到达《数据出境安全评估办法》（《安全评估办法》）列明的任一门槛时，必须进行评估；

2. **认证：**取得网信办指定的认证机构给予的认证；或

3. **中国标准合同规定：**按照网信办公布的标准合同规定（中国标准合同规定），与境外数据接收方订立合同。中国标准合同规定目前仍处于草案阶段，具体内容载于网信办于2022年6月30日公布的《个人信息出境标准合同规定（征求意见稿）》内。

有关上述三个机制的摘要说明，请参阅瑞生之前发出的客户通讯。

与欧盟的《通用数据保护条例》（GDPR）之比较

本客户通讯集中讨论认证机制，该机制类似欧盟的《通用数据保护条例》（EU GDPR）中有约束力的公司规则（有约束力公司规则）和相关的认证体系。欧盟的《通用数据保护条例》中的认证体系类似《个人信息保护法》项下的认证要求，因为两个认证实施程序均涉及由经认可的第三方认证机构给予认证，这也是机构可证明其个人数据处理活动符合欧盟的《通用数据保护条例》和《个人信息保护法》中各自的数据保护要求（包括跨境数据转移要求）的方法。欧盟的《通用数据保护条例》第46(2)条具体规定，认证体系为用于支持将个人数据转移到欧洲经济区以外的第三国家的方法。但在实践方面，到目前为止仍未有任何数据转移认证机制获得批准；较常见的做法就是依赖标准合同规定或有约束力公司规则。

有约束力公司规则与《个人信息保护法》中规定的认证要求相类似，因为两个机制均旨在实现集团公司与关联方之间的集团内数据转移（尽管网信办已明确说明认证机制的适用范围更广，不只限于集团内数据转移，同时也适用于各种形式的跨境数据转移）。此外，两个机制均以机构依据自身的数据保护政策和惯例进行认证为基础。在有约束力公司规则与认证要求两者之间，其主要区别在于有约束力公司规则的认证机构为监督机关，负责执行《个人信息保护法》项下的认证要求的则是经认可的第三方认证机构，而不是监管机关。

最后，欧盟的《通用数据保护条例》中的有约束力公司规则和认证体系以及《个人信息保护法》中的认证要求均为自愿程序。假如个人信息处理者不欲取得《个人信息保护法》项下的认证或依赖欧盟的《通用数据保护条例》中的认证体系或有约束力公司规则，其可以依赖其他数据转移机制（例如，在《个人信息保护法》项下的中国标准合同规定或欧盟的《通用数据保护条例》项下的欧盟标准合同规定）。因此，认证、有约束力公司规则和欧盟的《通用数据保护条例》中的认证体系（理论上虽然存在但目前仍未实施）只不过是各组织为了促进跨境数据转移而分别在《个人信息保护法》和欧盟的《通用数据保护条例》项下可采取的少数机制之一（标准合同规定除外）。

认证范围和要求

适用范围

《认证规则》适用于个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等的各类型处理活动。为了取得跨境数据转移的认证，个人信息处理者必须符合以下的标准，尽管该等标准仅为推荐性国家标准及技术委员会的指引：

- *《信息安全技术　　个人信息安全规范》（GB/T 35273-2020）*，是由市场监管总局及国家标准化管理委员会发布的推荐性国家标准（见官方英文译本）。

- *《个人信息跨境处理活动安全认证规范》（TC260-PG-20222A）*。2022年12月16日，全国信息安全标准化技术委员会（TC 260）发布了《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（第二版）》（《认证规范V2.0》）（见中文版本）。《认证规范V2.0》取代并替代了在2022年6月24日发布的《认证规范（第一版）》（《认证规范V1.0》）。如在跨境数据转移以外的情况下需要进行认证，个人信息处理者不需要遵循《认证规范V2.0》或其较后版本的规定。

与市场监管总局和网信办发布的具有法律约束力的《认证规则》不同，上述规范不具有法律效力。但是，《认证规则》明确提到《信息安全技术　个人信息安全规范》（GB/T 35273-2020）的最新版本和《认证规范V2.0》的最新版本作为认证依据，要求个人信息处理者遵循相关规定以便将个人信息转移至中国境外。此项提述似乎间接地提升了*GB/T 35273-2020*和《认证规范V2.0》的法律地位。

《认证规范V2.0》大幅扩大认证的适用范围，以涵盖任何及所有个人信息跨境转移的活动。相比之下，《认证规范V1.0》注明仅可在两种情况下采用认证机制：即集团内数据转移和境外个人信息处理者跨境数据转移。

认证申请人的要求

此外，《认证规范V2.0》明确了哪些人士有资格可在认证机制中申请认证：

1. **不包括分支机构和代表处：**申请认证的人士必须为取得合法的法人资格，正常经营且具有良好的信誉、商誉的中国实体。虽然仍未就"正常经营且具有良好信誉、商誉"给予定义，但中国国内的分支机构和代表处没有资格申请取得认证。

2. **当地代表申请跨境数据转移：**《认证规范V2.0》对两种情况进行区分并说明在每一种情况下哪些人士可提出认证申请。就集团内数据转移而言，必须由中国实体（即境内子公司）申请认证；就境外个人信息处理者的跨境数据转移而言，根据《个人信息保护法》第53条的规定，必须由境外个人信息处理者在中国境内委派的当地代表申请认证。

认证的最新要求

《认证规范V2.0》对参与个人信息的跨境处理的个人信息处理者和境外接收方（两者合称参与者）的认证要求进行了更新。关于与《认证规范V1.0》所载的要求进行之比较，请参阅瑞生之前发出的当中载有《认证规范V1.0》的要求的客户通讯。

1. **具有法律约束力的文件：**与《认证规范V1.0》相比，《认证规范V2.0》进一步规定参与者之间签订的具有法律约束力的文件所需包含的内容。参与者之间签订的具有法律约束力的文件必须至少明确下列内容：

   - 涉及跨境数据转移的相关参与者，包括其名称、地址、联系人姓名、联系方式等；
   - 跨境数据转移的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点等；
   - 参与者保护个人信息的责任与义务，以及为防范个人信息出境可能带来安全风险所采取的技术和管理措施等；
   - 数据主体的权利，以及保障数据主体权利的途径和方式；
   - 救济、合同解除、违约责任、争议解决等；
   - 境外接收方承诺并应遵守数据处理规则，确保数据保护水平符合中国个人信息保护相关法律、行政法规规定的标准；

- 境外接收方接受认证机构的持续监督，以及中国个人信息保护相关法律、行政法规管辖；
- 参与者的中国境内实体必须承担承诺法律责任并履行个人信息保护义务；
- 参与者各自承诺对侵害个人信息权益行为承担民事法律责任，并明确约定参与者应承担的民事法律责任；及
- 遵守适用法律法规规定的其他义务。

《认证规范V2.0》提高了具有法律约束力的文件中规定的义务，将这些要求与强制性安全评估前的自评估要求以及中国标准合同规定草案中的条文保持一致。

2. **组织管理：**参与者须指定数据保护负责人（DPO）并建立数据保护部门，负责确保遵守个人信息保护义务。与瑞生之前发出的客户通讯所述的要点类似，这一要求相比《个人信息保护法》第52条要更深入，因为该条规定仅对达到上述若干门槛的个人信息处理者施加了这项数据保护负责人的义务。

   《认证规范V2.0》要求数据保护负责人和数据保护部门承担其他职责。数据保护负责人必须具备个人信息保护专业知识和相关管理工作经历，由相关组织的决策层成员担任（但问题是哪些工作岗位属于决策阶层）。个人信息保护部门必须：

   - 履行个人信息保护义务；
   - 防止未经授权的访问以及个人信息泄露、篡改、丢失等；
   - 定期对个人信息处理的情况进行合规审计；及
   - 接受认证机构的持续监督，包括答复询问、配合检查等；该等认证机构由《认证规则》指定以进行获证后监督。

1. **处理规则：**《认证规范V2.0》强调，参与者均应共同遵守同一处理规则，其中至少包括处理信息的范围、目的、方式、保留期、转移个人数据需要中转的国家或者地区、保障数据主体权利的措施，以及数据安全事件的响应政策。

2. **个人信息保护影响评估（PIA）：**《认证规范V2.0》加入了个人信息处理者在开展个人信息保护影响评估时须考量的因素，这与其他两个机制（即安全评估和中国标准合同规定）中规定进行个人信息保护影响评估的要求一致。《认证规范V2.0》重申，个人信息处理者应当发出个人信息保护影响评估报告，且至少保存三年。此要求与《个人信息保护法》项下的要求类似。

3. **数据主体权利：**《认证规范V2.0》阐述了有关组织必须确保数据主体享有《个人信息保护法》下的权益的规定。尤其值得注意的是，《认证规范V2.0》还进一步要求：(i) 境外接收方不得将所接收的个人信息提供给第三方，但符合中国相关法律进行的披露除外，及(ii) 若发生个人信息泄露的情况，数据主体可要求个人信息处理者作出处理，或直接向境外护具接收方提出请求。

认证实施程序

认证实施程序分为三个阶段：(i) 技术验证；(ii) 现场审核；及 (iii) 获证后监督。该三个阶段可细分为五个步骤，而申请认证的人士必须完成有关步骤方可取得认证。

1. **准备工作及取得委托：**申请认证的人士向认证机构提交“认证委托文件”，包括申请认证人士的基本材料、认证委托书（委托指定代理人核实申请认证人士（即个人信息处理者）的身份），以及认证机构规定的其他相关证明文件（《认证规范V2.0》没有对“证明”文件给予定义）。如认证机构受理该认证申请的整套文件，应根据所涉个人信息的类型和数量、个人信息处理活动范围、技术验证机构信息等制定认证方案，并将该认证方案通知申请认证的人士。

2. **技术验证：**技术验证机构（可能是与认证机构截然不同的组织）根据认证方案实施技术验证，并向认证机构和认证申请人出具技术验证报告。

3. **现场审核：**认证机构实施现场审核，并向申请认证的人士出具现场审核报告。

4. **认证结果评价和批准：**认证机构根据认证申请、技术验证报告、现场审核报告和其他相关资料信息作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，会给予申请认证的人士另一次机会，要求限期整改；整改后仍不符合的，以书面形式通知申请认证人士终止认证。

5. **获证后监督：**认证机构应当在认证的三年有效期内，对获得认证的个人信息处理者进行持续监督，并“采取适当措施”，确保该等个人信息处理者持续符合认证要求。认证机构应确定监督频次，同时有权在个人信息处理者不再符合认证要求时对认证证书予以暂停或撤销。此外，获得认证的个人信息处理者可于认证有效期内申请认证证书暂停、注销。

《认证规则》没有对每个阶段或步骤的时限作出规定，但授权认证机构自行对须遵循的认证实施程序的合理时限做出决定。在认证机制全面运作一段时间之前，完成整个认证实施程序的时限仍属未知之数。

认证机构：CCRC

CCRC是一个在网络安全和数据安全认证及检查领域中最重要的政府附属机构之一，它同时负责开展各类型由政府主导的其它重要审查，其中包括网络安全审查、数据安全管理认证以及应用程序安全认证。CCRC为市场监管总局直属正司局级事业单位。

CCRC似乎是经网信办指定的负责处理并审查认证申请的认证机构；在拟备本客户通讯之时，获得这项任命的看来只有CCRC这一机构。这项任命的消息是经由CCRC网站上推出的一个名为“个人信息保护认证”的网页披露的，与此同时亦新增了一个名为“个人信息保护认证管理系统”的在线门户网站，让申请认证的人士在线上登记账户并提交认证申请。至于网信办是否已指定/将于日后指定任何其它机构进行认证，这一点目前仍未清楚。

尤其值得注意的是，CCRC发布了一份空白的申请表格，当中披露了其在认证实施程序中须考量的一些因素。该申请表格列明该认证申请的整套文件所需包含的一系列文件：

- 申请认证的人士的身份证明文件（营业执照）及个人信息处理者的办公场所的详情（包括证明该场所的法律地位的证明文件，如房租合同等）；
- 自评价表（至今未有任何具体说明或指引）及相关证据材料；
- 如具体涉及任何跨境数据转移，业务流程及描述；
- 如涉及跨境数据转移，个人信息处理者和其它实体二者的组织机构图或每个部门的相关职能表述文件；及

- 涉及的个人信息清单及该等信息的等级，例如个人信息是否为敏感个人信息。如为跨境数据转移，申请认证的人士必须注明境外接收方和目的地国家。

- 其它补充文件。

除上文所述者外，申请认证的人士还必须声明其在过去12个月内未发生任何重大个人信息安全事件。经研究上述规定均未有反映在《个人信息保护法》、《实施细则》、国家标准或技术委员会指引等规定内，因此，这似乎是CCRC新增的一项特定要求。

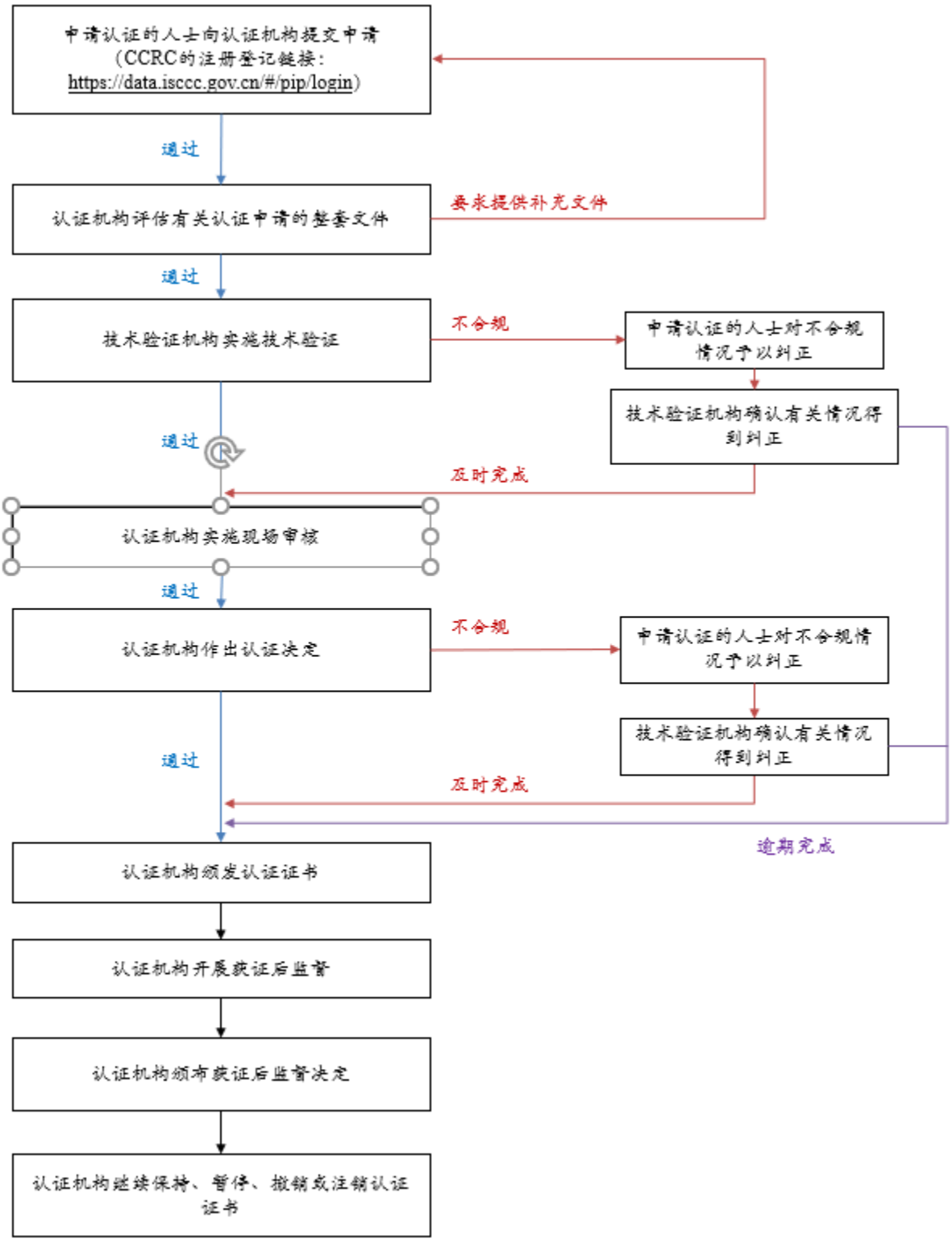
还有，申请认证的人士必须选择涉及的个人信息的量级，即个人信息主体量级是否为100万、1,000万或1亿。如涉及跨境数据转移，申请认证的人士必须选择自上年1月1日起累计向中国境外转移个人信息的量级，即涉及的信息量为(i) 10万人个人信息，及/或(ii) 1万人敏感个人信息。

认证效力/有效期

认证有效期为三年，申请认证的人士应在认证的三年有效期届满前六个月内提出认证续期的申请。于认证的有效期内，若获得认证的个人信息处理者名称、注册地址，或认证要求的合规情况、认证范围等发生变化时，将须提出变更初始认证申请的要求。然后，认证机构应考虑是否有需要重新进行技术验证和/或现场审核，以及是否可以批准变更。

认证机构须对外公布认证证书颁发、变更、暂停、注销和撤销等相关信息。

以下为阐述整个认证申请程序的流程图：


申请认证的人士向认证机构提交申请
（CCRC的注册登记链接：
https://data.isccc.gov.cn/#/pip/login）
通过
认证机构评估有关认证申请的整套文件
要求提供补充文件
通过
技术验证机构实施技术验证
不合规
申请认证的人士对不合规情况予以纠正
技术验证机构确认有关情况得到纠正
通过
及时完成
认证机构实施现场审核
通过
认证机构作出认证决定
不合规
申请认证的人士对不合规情况予以纠正
技术验证机构确认有关情况得到纠正
通过
及时完成
逾期完成
认证机构颁发认证证书
认证机构开展获证后监督
认证机构颁布获证后监督决定
认证机构继续保持、暂停、撤销或注销认证证书

认证证书和认证标志

《认证规则》规定了两个不同的认证标志：(i) 一般用于个人信息的收集、使用及处理的但**不含**跨境数据转移的认证标志；及(ii) 跨境数据转移专用的认证标志。认证证书和认证标志均可在广告或其他宣传活动中使用，前提是展示该等认证证书或认证标志的的方式不可产生误导。至于为何个人信息处理者会申请第一种不包含跨境数据转移的认证，官方未有就此加以说明。或许该认证可以作为个人信息处理者获得"批准的标记"或对其所具备资历的认定，因为该个人信息处理者总体上通过了认证实施程序。在以下的样本标记中，ABCD代表特定认证机构（例如，CCRC）的名称：

不包含跨境数据转移的认证标记

跨境数据转移专用的认证标记

要点

对于定期转移个人信息到中国境外但仍未达到《安全评估办法》中须触发强制安全评估的门槛的个人信息处理者来说，认证机制可能是实现跨境数据转移的合适工具。由于目前已明确说明认证适用于所有跨境数据转移的情况，对认证机制的接受程度很可能会因而提高。然而，中国标准合同规定的认证会否在实践中因促进跨境数据转移而越来越受欢迎，这一点仍有待观察。

尽管外界对《认证规范V2.0》就认证机制作出了进一步的详细规定表示欢迎，但在个人信息处理者可在实践中成功依赖这个机制之前仍存在许多不确定因素。例如，网信办至今仍未处理如下的关键问题：除了CCRC之外，网信办是否还会陆续指定其它认证机构？如何在实践中进行获证后监管？个人信息处理者在认证的有效期内达到了《安全评估办法》规定的相关门槛时如何可以切换为安全评估申请？随着认证机制现正全面运作且CCRC被指定为认证机构，日后将很可能有更多的个人信息处理者提交认证申请，而CCRC将针对认证实施程序发布进一步的实际操作指引。

最后，随着中国当局开始加强其在《网络安全法》、《数据安全法》和《个人信息保护法》下的执法活动，他们相当可能会以本文所述的《认证规范》、国家标准及技术委员会指引作为个人信息处理者宜采用的建议最佳常规，好让个人信息处理者符合新法律的要求。

如对本客户通讯有任何疑问，请联系下列作者之一或您通常咨询的瑞生律师：

徐辉（Hui Xu）
hui.xu@lw.com
+86.10.5965.7006
北京

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
香港

李晓霖（Bianca Lee）
bianca.lee@lw.com
+852.2912.2500
香港

本客户通讯在瑞生北京办事处的李芷莹协助下编制。

阁下可能感兴趣的其他文章：

中国发布个人信息出境标准合同草案并明确数据出境机制

中国发布网络平台运营商境外上市网络安全审查新规（英文版）

中国首次出台综合性个人信息保护法律（英文版）

中国的新数据安全法（英文版）

中国发布新法规保护关键信息基础设施（英文版）