LATHAM&WATKINS
瑞生国际律师事务所

客户通讯
评论

瑞生数据隐私和安全业务

2022年8月9日 | 第2998号

Read this Client Alert in English

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

中国国家互联网信息办公室发布了关于数据出境的系列规定，包括中国个人信息出境标准合同草案，以及个人信息保护认证和数据出境安全评估的有关监管指引和规定。

要点：

- **安全评估：**自2022年9月1日起，《个人信息保护法》项下的个人信息处理者（**数据处理者**）有下列情形之一的，必须向国家互联网信息办公室（**网信办**）申报安全评估：(i) 数据处理者向境外提供重要数据；(ii) 关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；或 (iii) 自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息。

- **认证：**数据处理者可经网信部门指定机构取得个人信息保护认证。根据《认证规范》，认证适用于：(i) 集团内数据传输，类似于《通用数据保护条例》（GDPR）中的“有约束力公司规则”（Binding Corporate Rules）；及 (ii) 受《个人信息保护法》域外效力/长臂管辖的境外数据处理者进行的数据传输。

- **中国标准合同草案：**网信办已发布了一版中国标准合同草案，即，个人信息出境合同（类似于GDPR项下的欧盟标准合同条款），并公开征求意见。中国标准合同意在用于个人信息跨境传输，但须申报安全评估的数据出境情况除外。

中华人民共和国（仅就《个人信息保护法》而言，**中国**指中国大陆境内）的有关监管部门已发布了根据《个人信息保护法》进行数据出境的三种路径的具体规定：

- 2022年6月24日，国家信息安全标准化技术委员会（**信安标委**）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》（**《认证规范》**）（见中文版本）。

- 2022年6月30日，网信办发布了《个人信息出境标准合同（草案）》（**中国标准合同**），以及《个人信息出境标准合同规定（征求意见稿）》（**《规定草案》**），在一个月内公开征求意见，截止时间为2022年7月29日（见中文版本）。

- 2022年7月7日，网信办在三版征求意见稿后发布了《数据出境安全评估办法》的正式版本，将于2022年9月1日生效（见中文版本）（**《评估办法》**）。

就如何根据《个人信息保护法》规定进行数据出境，尽管实践中仍存在诸多尚待澄清的问题，上述规定一定程度上为数据处理者明确了中国监管部门的具体要求。本客户通讯将梳理三种数据出境机制以及数据处理者应如何采用各种数据出境机制。

背景

数据出境机制

《个人信息保护法》第38条规定了数据处理者将个人信息提供至中国境外的三种路径（**数据出境机制**）：

1. 在个人信息出境前，通过国家网信部门组织的安全评估（**安全评估**）；
2. 取得网信部门指定的专业机构的个人信息保护认证（**认证**）；或者
3. 在个人信息出境前，按照中国标准合同，与境外接收方订立合同。

其他数据出境要求

除需采用上述任意一种数据出境机制以外，如此前《个人信息保护法》的客户通讯中提到的，数据处理者在将个人信息提供至中国境外前还需满足以下要求：

- **必要安全措施：**采取必要措施，确保境外数据接收方的个人信息处理活动满足《个人信息保护法》规定的标准；
- **告知及单独同意：**将境外数据接收方的联系信息、处理目的和方式、个人信息种类及向境外数据接收方行使其个人信息权利以及取得其单独同意的程序，告知个人信息主体；及
- **个人信息保护影响评估（Protection Impact Assessment）：**事前进行个人信息保护影响评估，评估报告和处理情况记录应至少保留三年。

境外上市网络安全审查

此外，数据出境活动还可能涉及到2021年12月28日颁布的《网络安全审查办法（2021）》。该办法经修订后进一步要求掌握100万用户个人信息且寻求在境外上市的网络平台运营商向网信部门申报网络安全审查，不论其是否将任何数据（或个人信息）提供至境外。更多信息，参见瑞生关于网络安全审查的客户通讯。

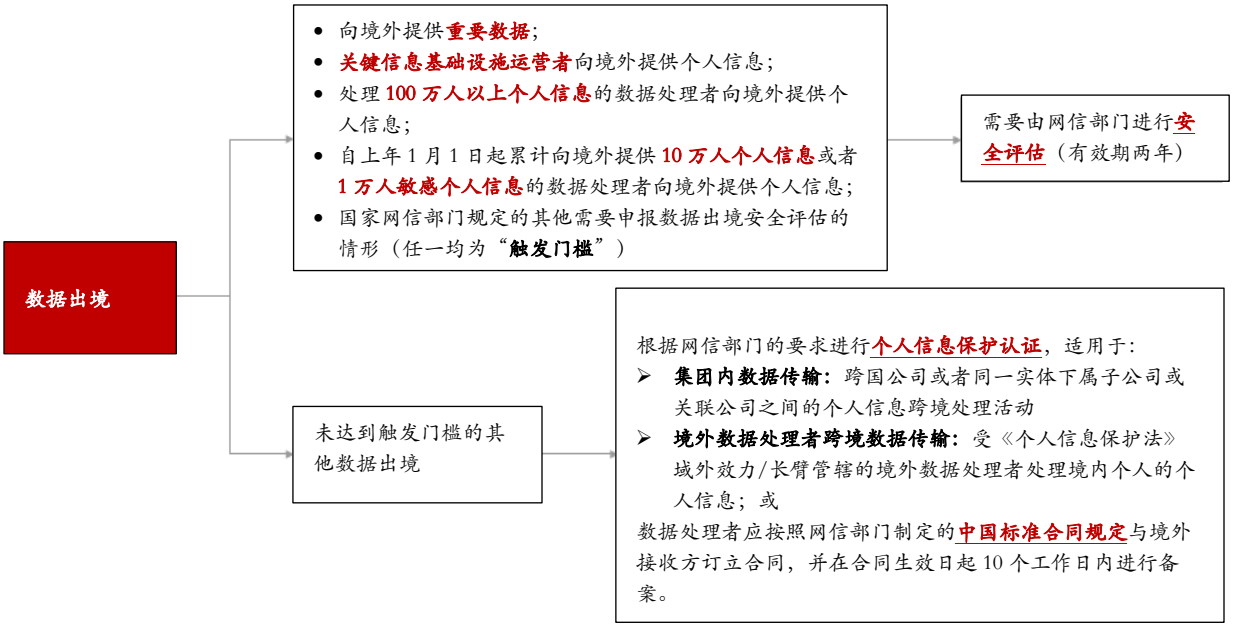
下文将详细讨论三种数据出境机制。

机制一：安全评估

适用范围

《评估办法》旨在明确《个人信息保护法》项下的安全评估的具体适用范围和程序。《评估办法》明确规定，向境外提供数据，有下列情形之一的，数据处理者必须事前申报安全评估，不得采用其他数据出境机制（**触发门槛**）：

- 向境外提供**重要数据**（《评估办法》项下定义的“重要数据”，是指“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”）；
- 关键信息基础设施运营者[1]向境外提供个人信息；
- 处理**100万人**以上个人信息的数据处理者向境外提供个人信息；
- 自上年1月1日起累计向境外提供**10万人个人信息**或者**1万人敏感个人信息**的数据处理者向境外提供个人信息；或者
- 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（该款赋予了网信部门未来进一步扩大需强制进行安全评估的数据出境范围的解释权）。



（《个人信息保护法》第38条项下数据出境的必要条件）

如上所述，《评估办法》强制要求数据处理者在数据出境达到触发门槛之一时，应事前向网信部门申报安全评估。

安全评估的程序及时间

自评估

在申报安全评估前，数据处理者须开展数据出境相关风险的自评估。自评估必须考虑以下事项：

- 数据出境和境外接收方处理数据的目的、范围、方式等的**合法性、正当性和必要性**；

- 出境数据的**规模、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；
- **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；
- **数据**出境中和出境后**遭到篡改**、破坏、泄露、丢失、转移或者被非法获取、非法利用等**的风险**，个人信息权益维护的渠道是否通畅等；
- 与境外接收方拟订立的数据出境相关**法律文件**是否充分约定了数据安全保护责任义务；及
- 其他可能影响数据出境安全的事项。

自评估后，作为正式安全评估的一部分，网信部门将进一步评估以下事项：

- 境外接收方所在国家或者地区的数据安全保护政策法规和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、行政法规的规定和强制性国家标准的要求；
- 数据安全和个人信息权益是否能够得到充分有效保障；及
- 数据处理者遵守中国法律、行政法规、部门规章的情况。

（上述全部事项，称为**数据出境评估事项**）

这些评估事项与数据处理者在进行个人信息保护影响评估（采用中国标准合同的要求之一）中关注的事项基本类似。要求对数据出境风险进行自评估并非中国特有的要求，实际上该规定类似于GDPR中在向第三国转移个人数据前应进行“传输影响评估”（Transfer Impact Assessment）的相关规定。

申报流程

省级审查：自评估后，数据处理者应向省级网信部门提交安全评估材料，包括申报书、自评估报告、与境外接收方拟订立的法律文件，以及安全评估工作需要的其他材料。省级网信部门应当自收到申报材料之日起5个工作日内完成完备性查验。值得注意的是，《评估办法》并未规定“与境外接收方拟订立的法律文件”是否必须采用中国标准合同，因此数据处理者可能与境外接收方自由订立合同，而不一定需严格采用中国标准合同。

国家级审查：如省级网信部门认为申报材料齐全，则其应将申报材料报送国家网信部门，国家网信部门应当自收到申报材料之日起7个工作日内，确定是否受理安全评估申请。如网信部门受理申报，其将正式启动安全评估，综合国务院有关部门、省级网信部门以及专门机构等的意见，进行实质审查，并在45个工作日内出具书面决定。如网信部门发现提交的申报材料不符合要求或者涉及复杂情况，因而需要进一步补充或更正的，可以延长审批时间并书面告知数据处理者。安全评估的时间通常为三个月，网信部门可酌情延长，即，安全评估自申报之日至收到最终评估结果，需5 + 7 + 45 + n 个工作日。

安全评估结果

评估结果应当书面通知数据处理者，且该结果有效期为两年（自评估结果出具之日起计算）。这意味着数据处理者必须每两年完成相同申报。有效期届满后，如需继续开展数据出境活动，数据处理者应当在两年有效期届满的60个工作日前重新申报评估。

数据处理者对评估结果有异议的，可以在收到评估结果15个工作日内向国家网信部门申请复评，复评结果为最终结论。

如发生任何可能影响数据出境评估事项以及整体数据出境风险的变化，数据处理者需要重新申报安全评估。被影响的评估事项包括向境外提供数据的目的和范围、境外国家或地区的数据保护政策以及数据处理者与境外接收方拟订立的法律文件的变更，以及影响出境数据安全的其他任何情况。

国家网信部门发现已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，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。

过渡期

数据处理者有6个月的过渡期（即至2023年3月1日），可对2022年9月1日前开展的数据出境活动进行整改，使之符合《评估办法》的相关规定。

有待澄清的问题

安全评估程序的要求已较为明确（尽管程序相对复杂且审批时间较长），但现实中仍存在很多不确定性。例如，如何计算触发门槛，特别是如何计算出境数据的数量以及哪些变化需重新提交安全评估。同样的问题也存在于下文即将提到的中国标准合同中。

机制二：个人信息保护认证

2022年6月24日，信安标委发布了《技术规范》，对实施个人信息保护认证作出了指引并明确了其适用范围。

需要提示的是，《认证规范》并非法律法规、行政规章或国家标准，而仅是技术委员会出具的指引，因此其不具有法律效力。但监管部门未来可能根据该规范制定具有法律约束力的强制性国家标准。

适用范围

认证机制类似于GDPR项下的“有约束力公司规则”（Binding Corporate Rules），是数据控制者和处理者在同一集团经营者或企业之间跨境传输个人数据可采用的机制之一。

《认证规范》明确了在两种情况下可采用认证机制：

- **集团内数据传输：**跨国公司或者同一实体下属子公司或关联公司之间的个人信息跨境处理活动；及
- **境外数据处理者跨境数据传输：**受《个人信息保护法》域外效力/长臂管辖的境外数据处理者处理境内个人的个人信息。

第二种情况下，直接收集中国境内个人信息的境外数据处理者可采用认证机制进行数据出境。《认证规范》还规定，“个人信息跨境处理活动认证属于国家推荐的自愿性认证，鼓励符合条件的个人信息处理者

和境外接收方在跨境处理个人信息时自愿申请个人信息跨境处理活动认证”。该规定似乎表明，认证机制并非数据处理者向境外传输个人信息的唯一路径；中国标准合同可能是数据出境的第二种路径，尽管这一点在《认证规范》和《规定草案》中没有得到确认。

为避免疑义，如果数据处理者达到安全评估的触发门槛，则其必须申报安全评估，而不得通过认证方式进行数据出境。

根据《认证规范》，就集团内的数据传输，中国实体（即境内关联公司）应负责取得认证并承担法律责任，不过《认证规范》中没有明确说明中国实体的责任是否仅限于以认证方式进行的数据出境。《认证规范》同时规定，对于境外数据处理者的跨境数据传输，其境内专门机构或指定代表应负责取得认证，并对以认证进行的数据出境活动承担法律责任。同样，《认证规范》中也没有明确说明境内专门机构或指定代表的责任是否仅限于以认证方式进行的数据出境。《个人信息保护法》对境外数据处理者的法律责任并没有特别规定，《认证规范》则要求境内代表应对境外数据处理者采用认证机制时的数据出境活动承担法律责任，该规定似乎未体现在《个人信息保护法》范围中。

认证要求

《认证规范》对参与个人信息跨境处理的数据处理者和境外接收方（合称**参与者**）提出了五项要求。

1. **有法律约束力的协议：**参与者必须订立有法律约束力的协议，至少载明以下内容：

   - 涉及个人信息跨境处理活动的相关参与者
   - 跨境处理个人信息的目的以及个人信息的类别、范围
   - 个人信息主体权益的保护措施
   - 境外接收方承诺并遵守中国统一的个人信息跨境处理规则，确保个人信息保护水平不低于中国个人信息保护相关法律、行政法规规定的标准，以及接受认证机构监督和相关中国法律管辖的义务
   - 承担法律责任的中国境内组织
   - 遵守法律、行政法规规定的其他义务

   与中国标准合同草案中载明的义务相比，上述要求相对简单且宽泛（更多是原则性的要求），数据处理者在决定是否采用认证机制还是中国标准合同进行数据出境时可综合考虑该因素。

2. **组织管理：**参与者须指定个人信息保护负责人并建立个人信息保护机构，负责确保其遵守个人信息保护义务。《个人信息保护法》仅对处理个人信息达到国家网信部门规定数量的数据处理者施加了此等义务，但《认证规范》明确对数据处理者和境外接收方均施加了该义务，这一要求相比《个人信息保护法》第52条更为严格。

3. **处理规则：**参与者必须遵守统一的个人信息跨境处理规则，包括处理个人信息的范围、目的、方式、保存时间、需要中转的国家或者地区，保障个人信息主体权利的措施，以及个人信息安全事件的处置规则。

4. **个人信息保护影响评估：**参与者必须开展个人信息保护影响评估并评估以下事项：(i) 向境外提供个人信息是否符合法律、行政法规；(ii) 对个人信息主体权益产生的影响，特别是境外国家和地区的法律环境、网络安全环境等对个人信息主体权益的影响；及 (iii) 其他维护个人信息权益所必需的事项。该要求与《个人信息保护法》项下数据处理者在数据出境前必须进行个人信息保护影响评估

的要求一致。《个人信息保护法》并未详细规定个人信息保护影响评估必须包括的事项，《认证规范》也只是简要提及评估要求。《评估办法》与《规定草案》则相对详细地阐明了在自评估和个人信息保护影响评估中分别应当关注的事项，且自评估载明的评估事项与《规定草案》中个人信息保护影响评估的评估事项完全一致。因此，如果数据处理者选择认证机制，保守考虑，应在进行个人信息保护影响评估时更全面地涵盖《评估办法》中要求的所有数据出境评估事项。

5. **个人信息主体权益：**《认证规范》要求指定个人信息主体为数据处理者与境外接收方之间有法律约束力的第三方受益人。个人信息主体还有权要求数据处理者与境外接收方提供法律文本中涉及个人信息主体权益部分的副本。该要求类似于中国标准合同草案中个人信息主体可以要求数据处理者和境外接收方提供中国标准合同副本。

有待澄清的问题

尽管《认证规范》就认证机制作出了较为详细的规定，但实践中仍存在许多不确定性。目前尚不明确具体的指定认证机构，取得认证的具体流程，在认证有效期内因达到触发门槛转换为强制安全评估的流程，以及认证的有效期等。

机制三：中国标准合同

2022年6月30日，网信办最终发布了期待已久的中国标准合同，与《规定草案》一起公开征求意见，截至2022年7月29日。中国标准合同草案中的一些条款与GDPR的标准合同条款（**欧盟标准合同条款**）类似，特别是“控制者到处理者”的条款。然而，中国标准合同草案采取了与欧盟标准合同条款截然不同的方式，后者以四种模式对应不同的处理安排。相反，《规定草案》采用了一站式的方法，未区分“控制者到控制者”和“控制者到处理者”的数据传输。因此，除了达到触发门槛必须进行安全评估的情况外，《规定草案》可能将适用于所有不同情况下的数据出境。由于数据处理者的义务通常与数据控制者的义务不同，这在实践中如何操作尚未明确。

适用范围

只有满足以下全部条件（**标准合同规定门槛**）时，即，数据出境并未达到任何触发门槛（在达到触发门槛时，则需进行强制安全评估），方可采用中国标准合同进行数据出境：

- 数据处理者并非关键信息基础设施运营者；
- 数据处理者处理的个人信息不满100万人；
- 数据处理者自上一年1月1日起累计向境外提供未达到10万人个人信息；并且
- 数据处理者自上一年1月1日起累计向境外提供未达到1万人敏感个人信息。

鉴于标准合同规定门槛对于确定数据处理者能否选择中国标准合同进行数据出境尤为重要，我们期待未来有关部门能够发布该门槛计算方法的详细规定。遗憾地是，目前该规定尚未明确，并且与《评估办法》类似，关于个人信息数据总量的计算，例如应以单一实体还是集团公司为准，仍不明晰。对于数据处理者在中国标准合同的有效期内达到触发门槛从而触发安全评估的情况，《规定草案》也未规定相关的转换机制。

中国标准合同下的义务

根据《规定草案》，中国标准合同必须包括以下内容:

- 数据处理者和境外接收方的基本信息，包括但不限于名称、地址、联系人姓名、联系方式等;
- 个人信息出境的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点等;
- 数据处理者和境外接收方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;
- 境外接收方所在国家或者地区的个人信息保护政策法规对遵守中国标准合同的影响;
- 个人信息主体的权利，以及保障个人信息主体权利的途径和方式；及
- 救济、合同解除、违约责任、争议解决等。

《规定草案》强调了采用中国标准合同的其他必要条件，与《个人信息保护法》下的其他数据出境相同，数据处理者必须进行个人信息保护影响评估。该评估应关注数据出境风险相关的若干事项。这些规定也与强制安全评估前的自评估要求基本类似。个人信息保护影响评估类似于GDPR项下的“传输影响评估”（Transfer Impact Assessment）。尚未明确的是，个人信息保护影响评估是否也需要当地律师的法律意见，以确认数据出境至目标司法区不存在风险。根据《个人信息保护法》，个人信息保护影响评估相关记录必须保留至少三年。

备案要求及程序

数据处理者应在与境外接收方订立中国标准合同之日，即合同生效日起10个工作日内，向所在地省级网信部门备案，备案材料包括中国标准合同和已完成的个人信息保护影响评估报告。根据《规定草案》，该备案程序可能属于形式或程序性申报，而非实质审查，但这一点有待网信部门确认。

对于日常经营需要持续跨境提供个人信息的数据处理者来说，10日内的备案规定可能对其日常经营带来一定的负担。值得注意的是，尽管《个人信息保护法》第38条未明确要求需要就标准合同需进行备案，但根据《规定草案》，未遵守备案规定可能导致违反《个人信息保护法》。该备案要求可能与《个人信息保护法》的相关规定存在一定的出入。

如果在已签署的中国标准合同的有效期内发生以下可能影响数据出境的变化，数据处理者须重新签订中国标准合同并重新备案:

- 向境外提供个人信息的目的、范围、类型、敏感程度、数量、方式、保存期限、存储地点和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;
- 境外接收方所在国家或者地区的个人信息保护政策法规发生变化等可能影响个人信息权益的；或
- 可能影响个人信息权益的其他情况。

《规定草案》并未载明是否还需重新进行个人信息保护影响评估并重新备案，并且，导致需要重新备案的“变化”的范围界定和触发条件亦不明确。例如，在界定出境个人信息“数量”是否发生变化时，应根据所涉及的个人信息主体人数还是出境信息数量进行计算?

有待澄清的问题

中国标准合同草案中一些有待澄清的部分重要问题如下：

- **适用范围：**尽管许多利益相关方可能认为根据《个人信息保护法》的域外效力，《个人信息保护法》第38条和中国标准合同也应适用于境外数据处理者，但《规定草案》仅规定了数据处理者与境外接收方签订合同向境外提供个人信息时应当签署中国标准合同。《规定草案》并未确认中国标准合同是否适用于境外数据处理者直接收集中国境内个人的个人信息并将其提供给境外接收方的情况。根据《规定草案》，中国标准合同仅适用于数据处理者和境外接收方之间的数据出境活动，因此，代表境外数据处理者处理个人信息的“受托方”可否采用中国标准合同来实现数据出境目前存在不确定性。此外，由于中国标准合同并不区分“控制者到控制者”以及“控制者到处理者”的情况，考虑两种情况下数据出境安排的性质和各方义务存在根本区别，在前一场景下如何采用中国标准合同有待澄清。

- **内容、格式和语言：**《规定草案》载明，数据处理者与境外接收方必须签订中国标准合同（其中包括空白的附录二，以便于双方加入约定的其他条款）。但是，《规定草案》并未进一步明确，在遵守《个人信息保护法》第38(3)条的前提下，双方能否修改中国标准合同，以及，如可以修改，可以在多大程度上变更标准合同条款。例如，双方是否可以将中国标准合同项下的义务纳入到自己的标准协议中；还是说中国标准合同应完全按照其现有形式签署？双方能否将中国标准合同作为附件纳入主协议中？如涉及到境外接收方，数据处理者和境外接收方之间的合同很可能是英文的，并且在发生冲突的情况下，会存在以英文版本为准的语言优先条款。然而，中国标准合同只有中文版本，网信办是否会考虑到国际数据传输的情形发布中国标准合同的官方英文版本目前尚不明确。在这种情况下，数据处理者能否约定以合同的英文版本为准？

- **适用法和争议解决：**《规定草案》载明，中国标准合同的适用法必须为中国法。此外，争议解决方式仅能是在中国法院进行诉讼或由特定中国仲裁机构或其他《承认及执行外国仲裁裁决公约》成员的仲裁机构管理仲裁。如果境外数据处理者与境外接收方签订中国标准合同，能否优先适用外国法律，例如数据处理者本国的法律，仍存在疑问。例如，欧盟标准合同条款则允许双方在特定情形下可以选择欧盟成员国以外的其他国家法律作为欧盟标准合同的适用法。

- **法律冲突：**根据《规定草案》，数据处理者与境外接收方之间的其他合同不得与中国标准合同冲突。这就产生了一个问题：如果中国标准合同与其他国家或地区的法律（如许多跨国企业需遵守和采用的GDPR和欧盟标准合同条款）之间存在冲突，应如何解决？

- **实施时间：**为新开展的数据出境活动签订中国标准合同的实施时间要求尚不明确。网信部门也没有明确规定，签订中国标准合同的要求是否会追溯到已开展的数据出境活动，以及，如追溯，与境外接收方修订合同的宽限期有多长。例如，《评估办法》提供了六个月的过渡期以使数据处理者符合安全评估要求。

处罚

如果数据出境活动没有采用适当的数据出境机制，数据处理者及其相关负责人可能会受到相关数据法律（即《网络安全法》、《数据安全法》和/或《个人信息保护法》）的处罚。根据《评估办法》，这些不同法律项下规定的处罚条款可能同时适用。鉴于《评估办法》即将于2022年9月1日生效，数据出境活动属于触发门槛范围内的数据处理者如未申报安全评估，将面临现实的处罚风险。以下是中国各数据法律项下有关处罚条款的汇总。

法律	处罚（针对企业）	处罚（针对管理人员）
《网络安全法》（第66条）	• **关键信息基础设施的运营者**未按要求进行安全评估的，由有关主管部门责令改正，给予警告，没收违法所得，和/或处**五万元（约7,400美元）以上五十万元（约74,000美元）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	• 直接责任人员处一万元（约1,480美元）以上十万元（约14,800美元）以下罚款
《数据安全法》（第45、46条）	• 数据处理者向境外提供**重要数据**未申报强制安全评估的，由有关主管部门责令改正，给予警告，**可以**并处**十万元（约14,800美元）以上一百万元（约148,000美元）以下**罚款 • 情节严重的，处**一百万元（约148,000美元）以上一千万元（约1,480,000美元）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 • 违反**国家核心数据**管理制度的，由有关主管部门处**二百万元以（约296,000美元）上一千万元（约1,480,000美元）以下**罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任	• 对直接负责的主管人员和其他直接责任人员处一万元（约1,480美元）以上十万元（约14,800美元）以下罚款 • 情节严重的，对直接负责的主管人员和其他直接责任人员处十万元（约14,800美元）以上一百万元（约148,000美元）以下罚款
《个人信息保护法》（第66条）	• 数据处理者违法处理**个人信息**的，由相关部门责令改正，给予警告，没收违法所得，对数据处理者，责令暂停或终止提供服务 • 拒不改正的，并处**一百万元（约148,000美元）**以下罚款 • 有前款违法行为，情节严重的，由相关部门责令改正，没收违法所得，并处**五千万元（约7,400,000美元）**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	• 拒不改正的，对直接负责的主管人员和其他直接责任人员处一万元（约1,480美元）以上十万元（约14,800美元）以下罚款 • 情节严重的，对直接负责的主管人员和其他直接责任人员处十万元（约14,800美元）以上一百万元（约148,000美元）以下罚款

要点

鉴于《评估办法》即将生效，受《个人信息保护法》约束的数据处理者应评估其数据出境活动是否会——或很快会——达到任一触发门槛。如达到，数据处理者将需要申报安全评估。《评估办法》为数据处理者提供了6个月的过渡期，以使其数据出境活动符合《评估办法》的要求。

尽管数据处理者可采用的三种数据出境机制现已存在总体框架，但仍需网信部门作出进一步的澄清，例如每种机制的具体适用范围以及满足每项机制项下具体要求应采取的措施。预计今年后半段个别行业还将发布一些针对特定行业的具体数据出境规定（例如中国工业和信息化部和中国证券监督管理委员会），这些规定可能会对在特定行业经营的数据处理者的数据出境施加进一步的义务。

网信办近期发布的一系列监管规定，几乎都聚焦于数据出境，这表明数据出境是中国数据监管关注的重点。尽管有待后续对具体规定的进一步澄清和补充，最新的监管规定有助于企业继续完善其合规机制以符合《个人信息保护法》和相关法律规定。

关于本客户通讯，如有任何问题，请联系以下作者或阁下通常咨询的瑞生律师：

徐辉
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@lw.com
+852.2912.2500
香港

本客户通讯在瑞生北京办公室李芷莹的协助下完成。

尾注

1 关键信息基础设施运营者的概念在2021年9月1日生效的《关键信息基础设施安全保护条例》中进一步阐述（更多信息，请阅读瑞生客户通讯）。该条例规定行业主管部门有权根据企业的业务性质和规模，通过通知指定企业为关键信息基础设施运营者，例如，其设施和信息系统是否对重要行业和部门至关重要，包括公共通信和信息服务、能源、交通、水利、金融、公共服务和电子政务；或者当其数据被破坏、禁用或泄露，可能对国家安全、人民生活和公共利益构成严重威胁的其他行业和部门。关键信息基础设施运营者的确定最终要由行业监管部门来酌情决定。这些部门将根据鉴定规则，分别在其管辖的部门或领域安排关键信息基础设施的鉴定，并将鉴定结果及时通知运营商。也就是说，如果公司的任何网络设施或信息系统被认定为关键信息基础设施，公司将收到监管部门的明确的认定结果通知，在此基础上，公司将能够确认其是否为关键信息基础设施运营者。