



公司及并购法律评述  
2019年6月

**上海**  
上海市银城中路68号  
时代金融中心16楼和19楼  
邮编: 200120  
电话: +86 21 3135 8666  
传真: +86 21 3135 8600

**北京**  
北京市建国门北大街8号  
华润大厦4楼  
邮编: 100005  
电话: +86 10 8519 2266  
传真: +86 10 8519 2929

**香港**  
香港中环皇后大道中5号  
衡怡大厦27楼  
电话: +852 2592 1978  
传真: +852 2868 0883

**伦敦**  
1F, 3 More London Riverside  
London SE1 2RE  
United Kingdom  
T: +44 (0)20 3283 4337  
D: +44 (0)20 3283 4323

[www.llinkslaw.com](http://www.llinkslaw.com)

**SHANGHAI**  
16F/19F, ONE LUJIAZUI  
68 Yin Cheng Road Middle  
Shanghai 200120 P.R.China  
T: +86 21 3135 8666  
F: +86 21 3135 8600

**BEIJING**  
4F, China Resources Building  
8 Jianguomenbei Avenue  
Beijing 100005 P.R.China  
T: +86 10 8519 2266  
F: +86 10 8519 2929

**HONG KONG**  
27F, Henley Building  
5 Queen's Road Central  
Central, Hong Kong  
T: +852 2592 1978  
F: +852 2868 0883

**LONDON**  
1F, 3 More London Riverside  
London SE1 2RE  
United Kingdom  
T: +44 (0)20 3283 4337  
D: +44 (0)20 3283 4323

[master@llinkslaw.com](mailto:master@llinkslaw.com)

## 从“雾里观花”到“柳暗花明” ——评《个人信息出境安全评估办法(征求意见稿)》

作者: 潘永建 | 黄文捷

6月13日,国家互联网信息办公室(“网信办”)发布了《个人信息出境安全评估办法(征求意见稿)》(“征求意见稿”),向社会公众征求意见。在征求意见稿发布之前,国家网信办于2017年4月公布的《个人信息和重要数据出境安全评估办法(征求意见稿)》(“2017版征求意见稿”)中首次专门对个人信息和重要数据出境的安全评估作出规定,但征求意见稿较2017版征求意见稿从监管部门到监管思路都发生了重要变化,并且对于个人信息出境安全评估的具体内容作出了详细规定。本文中,通力网安数据服务团队结合长期实践及持续关注,从主管部门、评估义务主体与客体、提供者与接收者合同、评估要求和违规责任等角度对征求意见稿进行解读,并附上征求意见稿与2017版征求意见稿中个人信息部分的详细对比,供客户与同行参考指正。

### 1. 主管部门

2017版征求意见稿规定,数据出境安全评估工作由国家网信部门进行统筹协调,由行业主管、监管部门组织开展具体工作。一般理解,此处提及的行业

For more Llinks publications, please contact:

**Roy Guo:** +86 21 3135 8756  
[Publication@llinkslaw.com](mailto:Publication@llinkslaw.com)

如您需要了解我们的出版物,  
请与下列人员联系:

**郭建良:** +86 21 3135 8756  
[Publication@llinkslaw.com](mailto:Publication@llinkslaw.com)

**通力律师事务所**  
[www.llinkslaw.com](http://www.llinkslaw.com)

**免责声明:** 本出版物仅代表作者本人观点,不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

## 从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

主管、监管部门应为交通、教育等与特定行业有关的政府部门。而在征求意见稿中，组织开展数据出境安全评估工作的部门改为省级网信部门。省级网信部门在个人信息出境安全评估工作中的主要职责包括：组织专家进行安全评估、对网络运营者的数据出境安全进行检查、接收网络运营者对于数据出境安全情况的报告等。国家网信办则负责受理网络运营者的申诉、接收省级网信部门出具的安全评估情况结论。

## 2. 安全评估义务主体与客体

### a) 义务主体

按照征求意见稿的规定，直接或间接承担个人信息出境安全评估义务的主体包括网络运营者、个人信息接收者与境外机构。

#### i. 网络运营者

《网络安全法》(“网安法”)将个人信息和重要数据出境安全评估义务主体限定为关键信息基础设施运营者(CIIO)。2017 版征求意见稿在网安法的基础上，将这一义务主体扩大到所有的网络运营者。之后，在非正式公开的内部讨论稿中又将义务主体限缩为 CIIO。而此次征求意见稿沿袭了 2017 版征求意见稿对于安全评估义务主体的规定，要求所有网络运营者应当承担个人信息出境评估义务。

《立法法》规定，没有法律或者国务院的行政法规、决定、命令的依据，部门规章不得设定减损公民、法人和其他组织权利或者增加其义务的规范，不得增加本部门的权力或者减少本部门的法定职责。虽然网安法并未要求除 CIIO 以外的网络运营者就个人信息出境进行安全评估，但 2017 版征求意见稿援引另一部上位法《国家安全法》将义务主体扩大至网络运营者。此次征求意见稿在仅引用《网络安全法》的情况下将个人信息出境评估的义务主体扩大到所有网络运营者，其法理依据有待商榷。

#### ii. 个人信息接收者

在个人信息出境情境下，个人信息接收者本应是安全评估义务的重要主体。但由于接收者位于境外，对其进行直接规制存在法理和实践困难。鉴于此，征求意见稿通过约束数据提供者与数据接收者订立的数据出境合同条款之方式，间接创设数据接收者的责任和义务，对数据出境安全进行规范。

## 从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

### iii. 境外机构

征求意见稿规定，境外机构收集境内用户个人信息并出境的，应在境内通过法定代表人或机构履行网络运营者的责任和义务。

### b) 义务客体

征求意见稿将其所规范的出境的个人信息定义为“以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息”。这一定义与网安法以及 2017 版征求意见稿中个人信息的定义一致，而没有采用相关司法解释及《信息安全技术 个人信息安全规范》等更为宽泛的定义，即未直接包括个人活动的信息。

## 3. 个人信息提供者与接收者签订的合同

与 GDPR 通过标准格式合同条款(standard contract clause, SCC)进行监管的思路相似，征求意见稿规定，网络运营者在申报个人信息出境安全评估时，应当提交其与接收者签订的合同。合同条款是安全评估的重点内容之一。网络运营者还应当将合同履行情况向网信部门汇报。

征求意见稿从以下四个方面对合同条款进行了规定，确定了合同的必备条款：合同基本条款、个人信息提供者的义务、个人信息接收者的义务以及个人信息接收者的再次传输。

### a) 合同基本条款

征求意见稿规定合同应当说明信息出境的目的、类型、保存时限；明确个人信息主体是合同中涉及个人信息主体权益的条款的受益人；网络运营者或接收者应当就个人信息主体受到的损害进行赔偿，除非证明没有责任；信息接收者难以履行合同时应当终止合同或重新进行安全评估。

### b) 个人信息提供者的义务

合同应当约定个人信息提供者的如下义务：对个人信息主体进行告知个人信息出境情况；应个人信息主体的要求提供合同副本；在个人信息主体无法从接收者处获得赔偿时对其进行先行赔付。

### c) 个人信息接收者的义务

合同应当约定个人信息接收者应履行的义务有：对个人信息主体提供访问、更正、删除个人信息的途径；按照合同约定适用和保存个人信息；由于法律环境的变化影响合同履行时及时通知

## 从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

提供者。

### d) 个人信息接收者的再次传输

对于接收者的再次传输行为，征求意见稿规定：网络运营者应当将传输情况通知个人信息主体；涉及个人敏感信息的，应当经个人信息主体同意；不涉及个人敏感信息的，无需征得个人信息主体同意，但个人信息主体可以请求停止传输；个人信息主体合法权益因再次传输受到损害的，网络运营者承担先行赔付责任。

以上必备合同条款从个人信息主体的知情权和同意权的角度对个人信息主体的合法权益多所着墨。必备条款亦通过网络运营者的连带责任保障个人信息主体权益，即个人信息主体的合法权益受到损害的，网络运营者将与接收者或接收个人信息的第三方向个人信息主体承担连带责任。值得商榷的是，征求意见稿规定，合同还应明确“个人信息主体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。”若这一规定旨在实现个人信息主体权益遭受损害情形下的举证责任倒置，因法律尚未明确将个人信息侵权案件作为“谁主张，谁举证”原则例外，这一规定目的的实现可能存在法律障碍。

通过合同监管的方式实现对信息接收者进行监管的效果可能有限。由于合同的效力是相对的，若信息提供者未经评估即向境外传输个人信息，不符合征求意见稿规定的合同在提供者和接收者之间仍然有效；即便合同条款符合征求意见稿的规定，若合同约定的接收者的违约责任较轻，或接收者违约后提供者或个人信息主体由于司法程序上的障碍无法有效获得赔偿，接收者仍然能以较低成本违约。

## 4. 安全评估的具体要求

### a) 义务的触发

2017 版征求意见稿规定网络运营者应当在数据出境前自行组织评估，在涉及影响国家安全和公共利益的数据出境的情形下(例如含有或累计含有 50 万人以上的个人信息或包含人口健康信息等情形)应当报请行业主管部门组织安全评估。

与此不同，征求意见稿规定了网络运营者不设前提条件的强制报请安全评估的义务。为减轻网络运营者的申报负担，征求意见稿规定向同一接收者多次或连续提供个人信息无需重复评估。毋庸置疑，这一规定对有定期数据传输需求的跨国公司当属利好消息。但是，尽管接收者相同，每隔 2 年或者个人信息出境目的、类型和境外保存时间发生变化时，由于数据出境的风险将随之发生较大变化，仍应重新申报评估。

## 从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

### b) 分析报告

网络运营者在向网信部门申报个人信息出境安全评估时，除应当提供申报书、与接收者订立的合同外，还应当提供个人信息出境安全风险及安全保障措施分析报告。网络运营者应当对报告的真实性、准确性负责。

分析报告的主要内容包括：(1)网络运营者和接收者的背景、规模、业务、财务、信誉、网络安全能力等。(2)个人信息出境计划，包括持续时间、涉及的个人信息主体数量、向境外提供的个人信息规模、个人信息出境后是否会再向第三方传输等。(3)个人信息出境风险分析和保障个人信息安全和个人信息主体合法权益的措施。

### c) 实施评估

#### i. 从自主评估到申报评估

如前所述，相比 2017 版征求意见稿，征求意见稿对于网络运营者数据出境安全评估的要求从自主评估为原则变为申报评估为原则，无疑提高了网络运营者的合规要求。

#### ii. 评估内容

在具体的安全评估过程中，网信部门将组织专家或技术力量围绕网络运营者提交的申报书、网络运营者与接收者签订的合同、个人信息出境安全风险及安全保障措施分析报告等材料进行安全评估。

安全评估的重点内容为(1)是否符合国家有关法律法规和政策规定；(2)合同条款是否能够充分保障个人信息主体合法权益；(3)合同能否得到有效执行；(4)网络运营者或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件；(5)网络运营者获得个人信息是否合法、正当；(6)其他应当评估的内容。可以看出，接收者的安全保障能力以及个人信息主体的合法权益保障是安全评估的重中之重。

#### iii. 评估期限

2017 版征求意见稿规定，行业主管或监管部门组织的安全评估应当于六十个工作日内完成。征求意见稿则将网信部门组织的安全评估期限缩短为十五个工作日，这将大大提高评估效率，避免耗时的评估工作影响网络运营者的商业安排。

## 从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

### d) 不得出境的情形

征求意见稿规定，出现下列情形的，网信部门可以要求网络运营者终止或暂停数据出境：(1)网络运营者或接收者发生较大数据泄露、数据滥用等事件；(2)个人信息主体不能或者难以维护个人合法权益；(3)网络运营者或接收者无力保障个人信息安全。网络运营者或接收者是否曾经发生过较为严重的数据安全事件属于其数据安全保障能力的衡量维度之一。发生过数据安全事件的，数据出境被禁止的可能性也更大。对于个人信息安全保障能力的判断可以参考《信息安全技术 数据出境安全评估指南(征求意见稿)》。

### e) 记录、汇报和检查

为实现对数据出境的后续监管，征求意见稿还提出了保存个人信息出境记录的要求，且要求网络运营者对记录至少保存 5 年。个人信息出境记录的内容主要包括信息出境的时间、接收者的身份以及出境信息的类型、数量和敏感程度。

除此之外，网络运营者应当每年度向网信部门汇报个人信息出境情况以及合同履行情况。网信部门还将定期组织对以上情况进行检查。

## 5. 违规责任

征求意见稿规定：“网络运营者违反本办法规定向境外提供个人信息的，依照有关法律法规进行处理”。这一规定十分笼统，为了解庞杂的《网络安全法》体系相关法律责任规定，读者可参见通力网安数据服务团队编著的《<网络安全法>实务 30 问》中相关实务文章，例如《<网络安全法>体系下企业的责任与义务概览》《浅析网络运营者刑事责任》等。

## 6. 结语

征求意见稿对个人信息出境安全评估作出了详尽规定，设定了企业强制安全评估义务，其要求之高前所未有的。对于有个人信息出境需求的网络运营者而言，应尽早采取合规措施，确保个人信息主体的合法权益、提前审查个人信息接收者的安全保障能力、对出境数据情况进行全流程的追踪。

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

附件

《个人信息和重要数据出境安全评估办法(征求意见稿)》与《个人信息出境安全评估办法(征求意见稿)》之比较

序号	主题	《个人信息和重要数据出境安全评估办法(征求意见稿)》	《个人信息出境安全评估办法(征求意见稿)》	主要变化
已有规定				
1.	立法宗旨	<b>第一条</b> 为保障个人信息和重要数据安全,维护网络空间主权和国家安全、社会公共利益,保护公民、法人和其他组织的合法权益,根据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规,制定本办法。	<b>第一条</b> 为保障数据跨境流动中的个人信息安全,根据《中华人民共和国网络安全法》等相关法律法规,制定本办法。	更新已有规定 删除了“依据《国安法》制定本办法”
2.	原则	<b>第二条</b> 网络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,应当按照本办法进行安全评估。  <b>第三条</b> 数据出境安全评估应遵循公正、客观、有效的原则,保障个人信息和重要数据安全,促进网络信息依法有序自由流动。	<b>第二条</b> 网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息(以下称个人信息出境),应当按照本办法进行安全评估。经安全评估认定个人信息出境可能影响国家安全、损害公共利益,或者难以有效保障个人信息安全的,不得出境。  国家关于个人信息出境另有规定的,从其规定。	更新已有规定 删除了“境内运营中收集的个人信息应当在境内存储”的要求
3.	个人信息主体同意	<b>第四条</b> 个人信息出境,应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区,并经其同意。未成年人个人信息出境须经其监护人同意。	N/A	删除已有规定 不再要求个人信息出境应当经个人信息主体同意
4.	主管机构	<b>第五条</b> 国家网信部门统筹协调数据出境安全评估工作,指导行业主管或	<b>第十条</b> 省级网信部门应当定期组织检查运营者的个人信息出境记录等个	更新已有规定

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

		<p>监管部门组织开展数据出境安全评估。</p> <p><b>第六条</b> 行业主管或监管部门负责本行业数据出境安全评估工作，<b>定期组织开展本行业数据出境安全检查。</b></p>	<p>个人信息出境情况，重点检查合同规定义务的履行情况、是否存在违反国家规定或损害个人信息主体合法权益的行为等。</p> <p>发现损害个人信息主体合法权益、数据泄露安全事件等情况时，应当及时要求网络运营者整改，通过网络运营者督促接收者整改。</p>	
5.	安全评估要求	<p><b>第七条</b> 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。</p> <p><b>第九条</b> 出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估： (一)含有或累计含有 50 万人以上的个人信息； (二)数据量超过 1000GB； (三)包含核设施、化学生物、国防军工、人口健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等； (四)包含关键信息基础设施的系统漏洞、安全防护等网络安全信息； (五)关键信息基础设施运营者向境外提供个人信息和重要数据； (六)其他可能影响国家安全和公共利益，行业主管或监管部门认为应该评估。</p> <p>行业主管或监管部门不明确的，由国家网信部门组织评估。</p> <p><b>第十二条</b> 网络运营者应根据业务发展和网络运营情况，<b>每年对数据出境至</b></p>	<p><b>第三条</b> 个人信息出境前，网络运营者应当向所在地省级网信部门申报个人信息出境安全评估。 向不同的接收者提供个人信息应当分别申报安全评估，向同一接收者多次或连续提供个人信息无需多次评估。</p> <p>每 2 年或者个人信息出境目的、类型和境外保存时间发生变化时应当重新评估。</p>	<p>更新已有规定 “网络运营者自行组织安全评估为原则”转变为 “向网信部门申报安全评估为原则”</p>

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

		<p>少进行一次安全评估,及时将评估情况报行业主管或监管部门。</p> <p>当数据接收方出现变更,数据出境目的、范围、数量、类型等发生较大变化,数据接收方或出境数据发生重大安全事件时,应及时重新进行安全评估。</p>		
6.	重点评估内容	<p><b>第八条</b></p> <p>数据出境安全评估应重点评估以下内容:</p> <p>(一)数据出境的必要性;</p> <p>(二)涉及个人信息情况,包括个人信息的数量、范围、类型、敏感程度,以及个人信息主体是否同意其个人信息出境等;</p> <p>(三)涉及重要数据情况,包括重要数据的数量、范围、类型及其敏感程度等;</p> <p>(四)数据接收方的安全保护措施、能力和水平,以及所在国家和地区的网络安全环境等;</p> <p>(五)数据出境及再转移后被泄露、毁损、篡改、滥用等风险;</p> <p>(六)数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险;</p> <p>(七)其他需要评估的重要事项。</p>	<p><b>第六条</b></p> <p>个人信息出境安全评估重点评估以下内容:</p> <p>(一)是否符合国家有关法律、法规和政策规定。</p> <p>(二)合同条款是否能够充分保障个人信息主体合法权益。</p> <p>(三)合同能否得到有效执行。</p> <p>(四)网络运营者或接收者是否有损害个人信息主体合法权益的历史、是否发生过重大网络安全事件。</p> <p>(五)网络运营者获得个人信息是否合法、正当。</p> <p>(六)其他应当评估的内容。</p>	<p>更新已有规定</p> <p>出境安全评估的重点转变为网络运营者或接收者对个人信息的保障能力</p>
7.	安全评估期限	<p><b>第十条</b></p> <p>行业主管或监管部门组织的安全评估,应当于<b>六十个工作日内</b>完成,及时向网络运营者反馈安全评估情况,并报国家网信部门。</p>	<p><b>第五条</b></p> <p>省级网信部门在收到个人信息出境安全评估申报材料并核查其完备性后,应当组织专家或技术力量进行安全评估。安全评估应当在<b>15个工作日内</b>完成,情况复杂的可以适当延长。</p>	<p>更新已有规定</p> <p>将网信部门进行安全评估的期限由60个工作日缩短为15个工作日</p>
8.	上报安全评估情况	<p><b>第十条</b></p> <p>行业主管或监管部门组织的安全评估,应当于六十个工作日内完成,及时向网络运营者反馈安全</p>	<p><b>第七条</b></p> <p>省级网信部门在将个人信息出境安全评估结论通报网络运营者的同时,将<b>个人信息出境安全评估情</b></p>	<p>重申已有规定</p>

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

		评估情况,并报 <b>国家网信部门</b> 。	<b>况报国家网信部门</b> 。  网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的,可以向国家网信部门提出申诉。	
9.	个人信息不得/暂停出境的情形	<b>第十一条</b> 存在以下情况之一的,数据不得出境: (一)个人信息出境未经 <b>个人信息主体同意</b> ,或可能侵害个人利益; (二)数据出境给国家政治、经济、科技、国防等安全带来风险,可能影响国家安全、损害社会公共利益; (三)其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。	<b>第二条</b> 网络运营者向境外提供在中华人民共和国境内运营中收集的个人信息(以下称个人信息出境),应当按照本办法进行安全评估。 <b>经安全评估认定个人信息出境可能影响国家安全、损害公共利益,或者难以有效保障个人信息安全的,不得出境</b> 。  国家关于个人信息出境另有规定的,从其规定。  <b>第十一条</b> 出现以下情况之一时,网信部门可以要求网络运营者 <b>暂停</b> 或终止向境外提供个人信息: (一)网络运营者或接收者发生较大数据泄露、数据滥用等事件。 (二)个人信息主体 <b>不能或者难以维护个人合法权益</b> 。 (三)网络运营者或接收者 <b>无力保障个人信息安全</b> 。	更新已有规定
10.	举报	<b>第十三条</b> 对违反相关法律法规和本办法向境外提供数据的行为,任何个人和组织有权向国家网信部门、公安部门等有关部门举报。	<b>第十二条</b> 任何个人和组织有权对违反本办法规定向境外提供个人信息的行为,向省级以上网信部门或者相关部门举报。	重申已有规定
11.	违法责任	<b>第十四条</b> 违反本办法规定的,依照有关法律法规进行处罚。	<b>第十八条</b> 网络运营者违反本办法规定向境外提供个人信息的,依照有关法律法规进行处理。	重申已有规定
12.	国际条约	<b>第十五条</b> 我国政府与其他国家、地区签署	<b>第十九条</b> 我国参与的或者与其他国家和地	重申已有规定

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

		的关于数据出境的协议，按照协议的规定执行。  涉及国家秘密信息的按照相关规定执行。	区、国际组织缔结的条约、协议等对个人信息出境有明确规定的，适用其规定，我国声明保留的条款除外。	
13.	参照执行	<b>第十六条</b> 其他个人和组织在中华人民共和国境内收集和产生的个人信息和重要数据出境的安全评估工作参照本办法执行。	N/A	删除已有规定
14.	定义	<b>第十七条</b> 本办法下列用语的含义： 网络运营者，是指网络的所有者、管理者和网络服务提供者。 数据出境，是指网络运营者将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，提供给位于境外的机构、组织、个人。 个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。 重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。	<b>第二十一条</b> 本办法下列用语的含义： (一)网络运营者，是指网络的所有者、管理者和网络服务提供者。 (二)个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。 (三)个人敏感信息，是指一旦被泄露、窃取、篡改、非法使用可能危害个人信息主体人身、财产安全，或导致个人信息主体名誉、身心健康受到损害等的个人信息。	重申已有规定
<b>新规定</b>				
15.	安全评估申报材料	N/A	<b>第四条</b> 网络运营者申报个人信息出境安全评估应当提供以下材料，并对材料的真实性、准确性负责： (一)申报书。 (二)网络运营者与接收者签订的合同。 (三)个人信息出境安全风险及安全保障措施分析报告。	新规定

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

			(四)国家网信部门要求提供的其他材料。	
16.	申诉	N/A	<p><b>第七条</b></p> <p>省级网信部门在将个人信息出境安全评估结论通报网络运营者的同时,将个人信息出境安全评估情况报国家网信部门。</p> <p>网络运营者对省级网信部门的个人信息出境安全评估结论存在异议的,可以向国家网信部门提出<b>申诉</b>。</p>	新规定
17.	保存个人信息出境记录	N/A	<p><b>第八条</b></p> <p>网络运营者应当建立个人信息出境记录并且<b>至少保存 5 年</b>,记录包括:</p> <p>(一)向境外提供个人信息的日期时间。</p> <p>(二)接收者的身份,包括但不限于接收者的名称、地址、联系方式等。</p> <p>(三)向境外提供的个人信息的类型及数量、敏感程度。</p> <p>(四)国家网信部门规定的其他内容</p>	新规定
18.	个人信息出境等情况报告	N/A	<p><b>第九条</b></p> <p>网络运营者应当每年 12 月 31 日前<b>将本年度个人信息出境情况、合同履行情况等报所在地省级网信部门</b>。</p> <p>发生<b>较大数据安全事件</b>时,应及时报所在地省级网信部门。</p>	新规定
19.	合同条款	N/A	<p><b>第十三条</b></p> <p>网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件(统称合同),应当明确:</p> <p>(一)个人信息出境的目的、类型、保存时限。</p> <p>(二)个人信息主体是合同中涉及个人信息主体权益的条款的受益人。</p> <p>(三)个人信息主体合法权益受到损</p>	新规定

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

			<p>害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。</p> <p>(四)接收者所在国家法律环境发生变化导致合同难以履行时，应当终止合同，或者重新进行安全评估。</p> <p>(五)合同的终止不能免除合同中涉及个人信息主体合法权益有关条款规定的网络运营者和接收者的责任和义务，除非接收者已经销毁了接收到的个人信息或作了匿名化处理。</p> <p>(六)双方约定的其他内容。</p> <p><b>第十四条</b></p> <p>合同应当明确网络运营者承担以下责任和义务：</p> <p>(一)以电子邮件、即时通信、信函、传真等方式告知个人信息主体网络运营者和接收者的基本情况，以及向境外提供个人信息的目的、类型和保存时间。</p> <p>(二)应个人信息主体的请求，提供本合同的副本。</p> <p>(三)应请求向接收者转达个人信息主体诉求，包括向接收者索赔；个人信息主体不能从接收者获得赔偿时，先行赔付。</p> <p><b>第十五条</b></p> <p>合同应当明确接收者承担以下责任和义务：</p> <p>(一)为个人信息主体提供访问其个人信息的途径，个人信息主体要求更正或者删除其个人信息时，应在合理的代价和时限内予以响应、更正或者删除。</p> <p>(二)按照合同约定的目的使用个人信息，个人信息的境外保存期限不</p>	
--	--	--	---	--

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

			<p>得超出合同约定的时限。</p> <p>(三)确认签署合同及履行合同义务不会违背接收者所在国家的法律要求，<b>当接收者所在国家和地区法律环境发生变化可能影响合同执行时，应当及时通知网络运营者，</b>并通过网络运营者报告网络运营者所在地省级网信部门。</p> <p><b>第十六条</b> 合同应当明确接收者不得<b>将接收到的个人信息传输给第三方</b>，除非满足以下条件： (一)网络运营者已经通过电子邮件、即时通信、信函、传真等方式将个人信息传输给第三方的目的、第三方的身份和国别，以及传输的个人信息类型、第三方保留时限等<b>通知个人信息主体</b>。 (二)接收者承诺在<b>个人信息主体请求停止</b>向第三方传输时，停止传输并要求第三方销毁已经接收到的个人信息。 (三)<b>涉及到个人敏感信息时，已征得个人信息主体同意</b>。 (四)因向第三方传输个人信息对个人信息主体合法权益带来损害时，<b>网络运营者同意先行承担赔付责任</b>。</p>	
20.	安全风险及安全保障措施分析报告	N/A	<p><b>第十七条</b> 网络运营者关于个人信息出境安全风险及安全保障措施分析报告应当至少包括： (一)网络运营者和接收者的背景、规模、业务、财务、信誉、网络安全能力等。 (二)个人信息出境计划，包括持续时间、涉及的个人信息主体数量、向境外提供的个人信息规模、个人信息出境后是否会再向第三方传</p>	新规定

**免责声明：**本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

			输等。 (三)个人信息出境风险分析和保障个人信息安全和个人信息主体合法权益的措施。	
21.	境外机构收集境内个人信息	N/A	<b>第二十条</b> 境外机构经营活动中，通过互联网等收集境内用户个人信息，应当在境内通过法定代表人或者机构履行本办法中网络运营者的责任和义务。	新规定

从“雾里观花”到“柳暗花明”——评《个人信息出境安全评估办法(征求意见稿)》

如需进一步信息，请联系：

<b>作者</b>	
<b>潘永建</b> 电话: +86 21 3135 8701 david.pan@linkslaw.com	
<b>上海</b>	
<b>俞卫锋</b> 电话: +86 21 3135 8686 david.yu@linkslaw.com	<b>刘贇春</b> 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
<b>余 铭</b> 电话: +86 21 3135 8770 selenashe@linkslaw.com	<b>娄斐弘</b> 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
<b>钱大立</b> 电话: +86 21 3135 8676 dali.qian@linkslaw.com	<b>孔焕志</b> 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
<b>吴 炜</b> 电话: +86 21 6043 3711 david.wu@linkslaw.com	<b>潘永建</b> 电话: +86 21 3135 8701 david.pan@linkslaw.com
<b>姜 琳</b> 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
<b>北 京</b>	
<b>俞卫锋</b> 电话: +86 10 8519 2266 david.yu@linkslaw.com	<b>刘贇春</b> 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
<b>杨玉华</b> 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
<b>香 港(与方緯谷律师事务所联营)</b>	
<b>俞卫锋</b> 电话: +86 21 3135 8686 david.yu@linkslaw.com	<b>吕 红</b> 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
<b>伦 敦</b>	
<b>杨玉华</b> 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 通力律师事务所 2019

**免责声明：**本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。