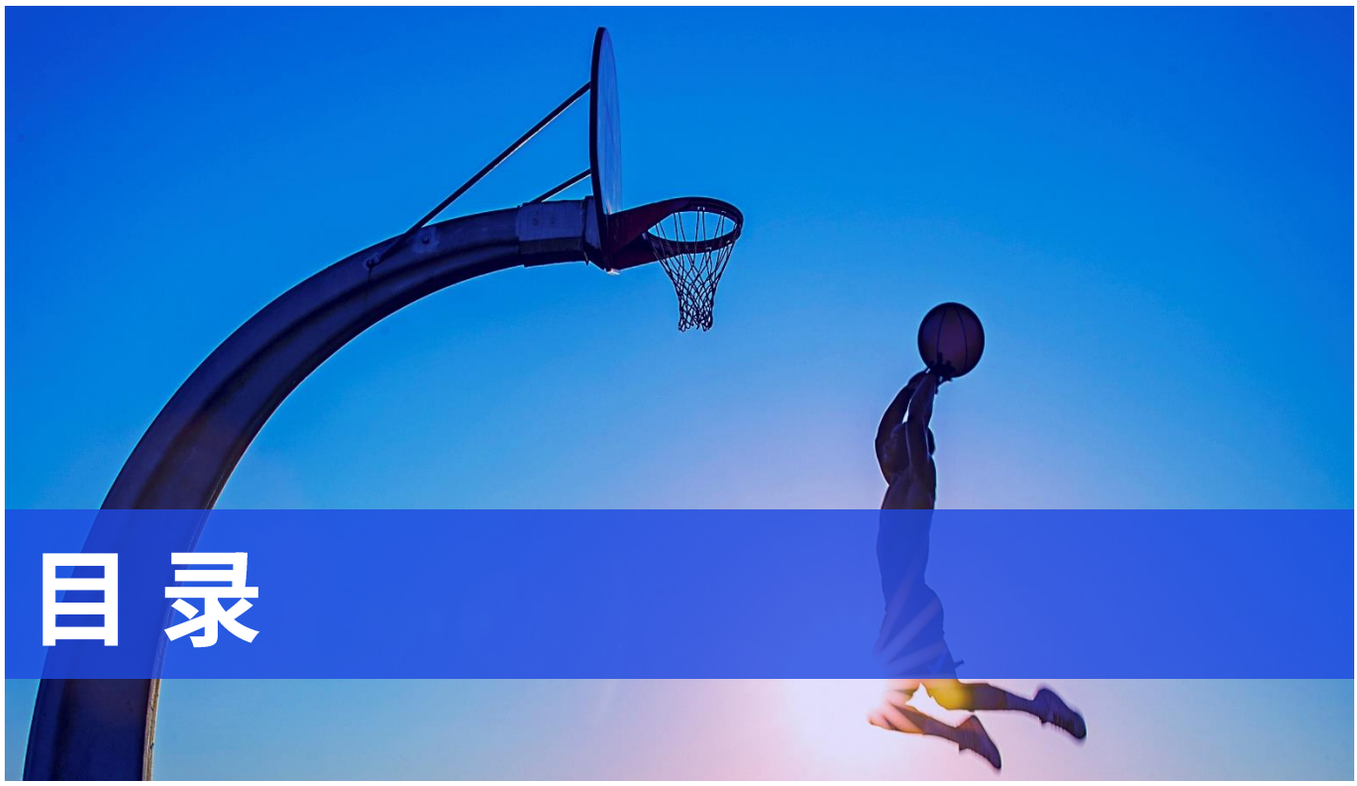
KPMG
毕马威

个人信息出境合规管理

——应对《个人信息出境标准合同办法》行动建议

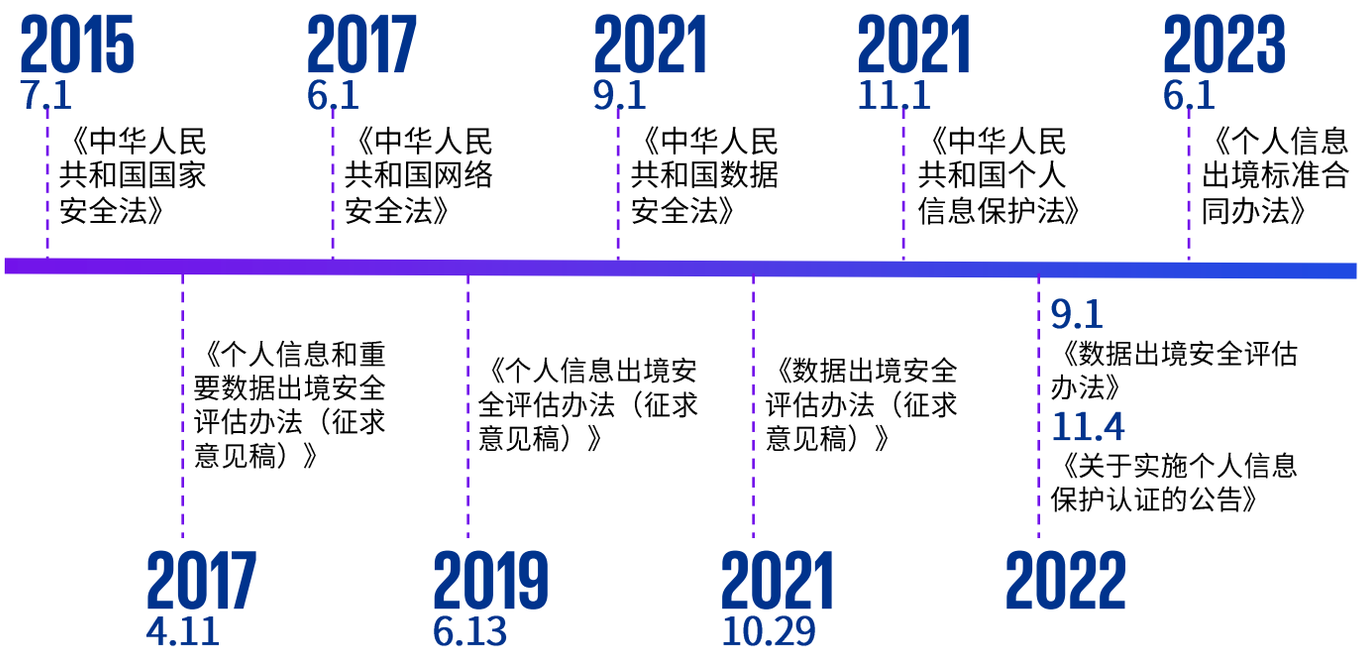
毕马威网络安全

2023年4月



目录

法律法规发展概览



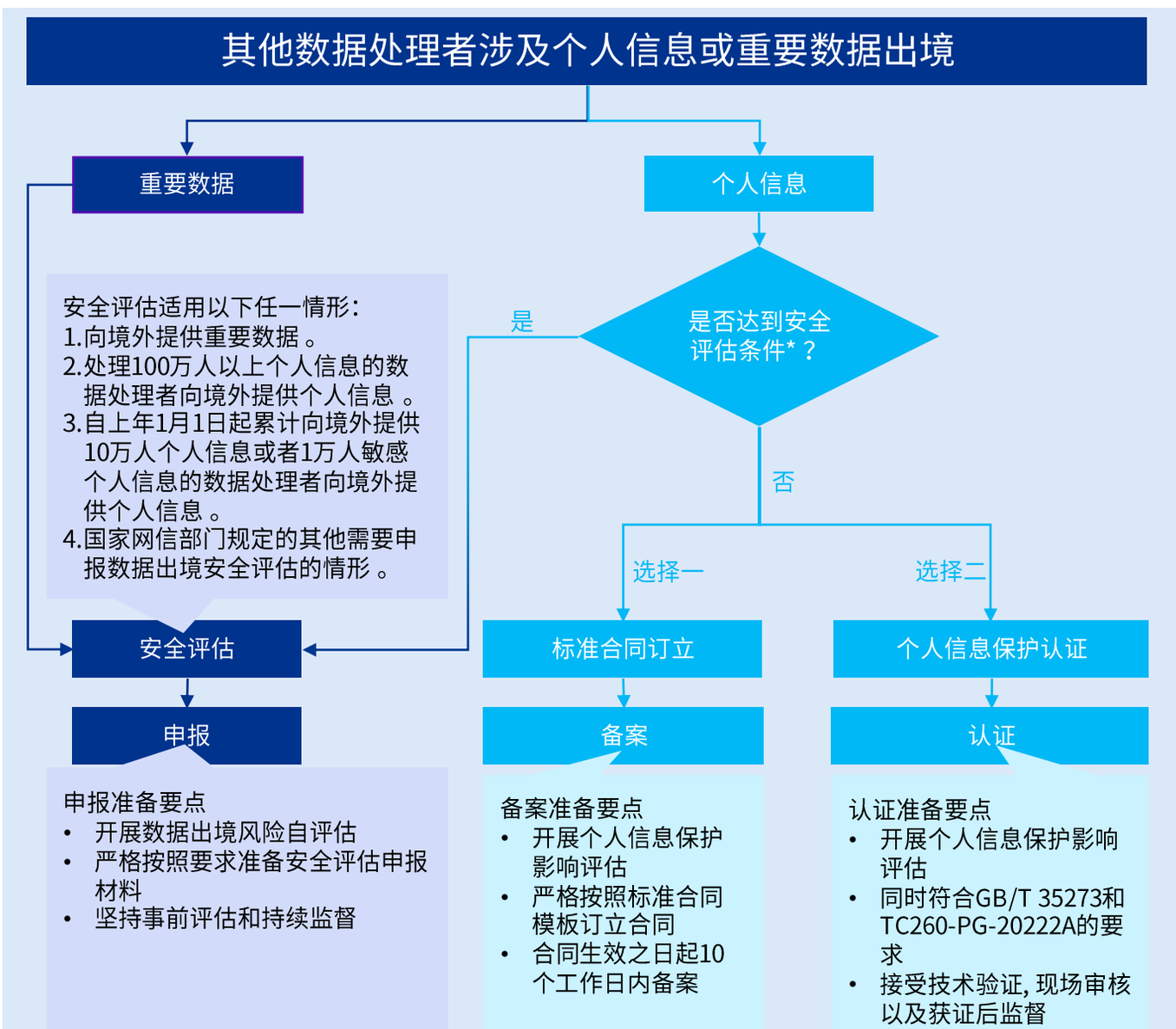
- 2022年7月7日，国家互联网信息办公室（“网信办”）发布《数据出境安全评估办法》（以下简称《出境评估办法》），自2022年9月1日起施行。《出境评估办法》规定了应当申报数据出境安全评估的情形并提出了数据出境安全评估的具体要求。
- 2022年11月4日，国家互联网信息办公室发布《关于实施个人信息保护认证的公告》(以下简称《公告》），自2022年11月4日起施行。《公告》明确了个人信息保护认证的实施细则，其中规定认证的依据为GB/T 35273《信息安全技术 个人信息安全规范》，对于开展跨境处理活动的个人信息处理者，还应当符合TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。
- 2023年2月24日，国家互联网信息办公室发布《个人信息出境标准合同办法》（以下简称《标准合同办法》）及其附件《个人信息出境标准合同》（以下简称《标准合同》），自2023年6月1日起施行。

合规路径总结

自发布《标准合同办法》以来，适用于个人信息跨境传输的三种路径已经明确：（一）通过国家网信部门组织的安全评估；（二）经专业机构进行个人信息保护认证；（三）与境外接收方订立标准合同。

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；

其他数据处理者应判断拟出境数据类型及规模，结合数据出境场景的实际情况，参照执行或选择适用的合规路径：



注：个人信息处理者不得采取数量拆分等手段，规避个人信息出境安全评估。符合《数据出境安全评估办法》第四条所述情形的个人信息处理者，仍需依法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。

主要内容

一、合同的不得冲突性

在订立标准合同或进行补充约定时，需注意 “不得冲突”的要求：

- 补充约定的条款不得与标准合同中的条款冲突。即标准合同中的条款优先于双方约定的其他条款。
- 其他法律文件不得与标准合同相冲突。即其他法律文件与本合同发生冲突，本合同的条款优先适用。

二、第三方受益人机制

- 涉及三方主体，即合同内容涉及的主体包括个人信息处理者（处理者）、境外接收方（接收方）和个人信息主体（个人）。
- 个人享有合同相应权利，即处理者与接收方作为合同相对方订立并履行协议，而个人作为第三方受益人，通过合同双方的约定被赋予了相应的权利。
- 个人权利的主张，即一旦发生个人信息权益侵害，个人既可以依据《个人信息保护法》向处理者主张权利，也可以按照标准合同的内容直接向合同任何一方或双方主张权利。

三、六个月的整改期限

- 在《标准合同办法》施行前已经开展的个人信息出境活动，不符合规定的，应当自《标准合同办法》施行之日起6个月内（即2023年11月30日）完成整改。

四、个人信息主体权利

- 个人被告知作为合同第三方受益人。处理者需向个人告知其与接收方通过标准合同约定个人为第三方受益人，如个人未在30日内明确拒绝，则有权根据标准合同向处理者和接收方的一方或双方主张并要求履行标准合同项下与个人权利相关的条款。
- 个人权利的保障。处理者和接收方在个人信息出境活动开展过程中需采取适当措施实现个人的合理请求。

参考：《个人信息出境标准合同办法》，国家互联网信息办公室

主要内容（续）

五、处理者/接收方的法律责任

构成连带责任（对外连带，对内按份）	个人有权请求任何一方或双方承担民事责任，任何一方承担的责任超过其应承担的责任份额时，有权向另一方追偿。
不构成连带责任	1、由违反保护义务的一方承担民事责任； 2、处理者可能承担行政、刑事等法律责任。
网信部门约谈	当省级以上网信部门发现出境活动存在较大风险或发生个人信息安全事件，可对处理者进行约谈。处理者应按要求整改，消除隐患。

六、个人信息处理者的主要义务

个人信息主体	1、仅限在实现目的所需最小范围内向境外提供个人信息； 2、履行告知义务； 3、获取个人的单独同意（基于同意向境外提供个人信息的）； 4、响应个人要求，向个人提供标准合同的副本。
境外接收方	1、检查境外接收方是否履行义务的管理和技术措施、能力； 2、提供相关法律规定和技术标准的副本。
监管机构	1、答复监管机构的询问； 2、提供对出境处理活动的合规审计； 3、对合同义务的履行承担举证责任。
内部管理	开展个人信息保护影响评估，并保存评估报告至少3年。

主要内容（续）

七、境外接收方的主要义务

个人信息主体	1、按照标准合同的约定处理个人信息； 2、响应个人要求提供标准合同的副本； 3、采取对个人权益影响最小的方式处理个人信息； 4、个人信息的保存期限为实现处理目的最短时间； 5、如涉及自动化决策，应遵循透明度和结果公平、公正原则； 6、及时采取应对安全事件的补救措施，并履行通知与记录义务； 7、提供已遵守标准合同义务所需的必要信息； 8、告知个人联系渠道； 9、响应个人行权请求。
个人信息处理者	1、按照与处理者的约定范围处理个人信息； 2、向处理者提供合规证明资料，允许处理者开展合规审计、查阅文件； 3、向处理者提供所有的必要信息。
监管机构	1、接受监管机构的监督管理； 2、服从监管机构采取的措施或决定； 3、提供已采取必要行动的书面证明。
内部管理	1、对开展的个人信息处理活动进行客观记录，保存记录至少3年； 2、采取技术和管理措施； 3、建立最小授权的访问控制权限； 4、发生安全事件后及时规范应对。
第三方（如涉及）	境外第三方提供个人信息： 1、业务需要； 2、履行告知义务并获得个人单独同意（基于个人同意处理的）； 3、与第三方达成书面协议，并响应个人要求提供协议副本。 转委托情形： 1、事先征得个人信息处理者同意； 2、处理目的、方式等不能超出合同约定； 3、对第三方的处理活动进行监督。

标准合同签署的关键流程

合同订立前

1、判断是否可通过订立标准合同的方式向境外提供个人信息

（1）“是否为关键信息基础设施运营”；

（2）“处理个人信息的数量”；

（3）“自上年1月1日起累计向境外提供个人信息和敏感个人信息的数量”

2、梳理存量数据出境业务

处理者应明确出境活动所涉及的详情，如：个人信息出境目的、范围、规模、方式、个人信息种类、境外接收方、出境后保存期限与地点、境外接收方是否进行转委托等事项。

3、开展个人信息保护影响评估（PIPIA）

个人信息订立标准合同前须开展个人信息保护影响评估。个人信息保护影响评估重点关注内容与评估流程的详情，请见本文后面《个人信息保护影响评估》介绍。

合同协商签约

1、完善合同文本

合同仍有部分内容需要自行补充，如联系方式、地址、个人信息出境说明等。

2、合同谈判与订立

标准合同的落地有以下挑战点：

（1）目前国家尚未发布标准合同的官方英文翻译；

（2）标准合同的制式条款不可修改。网信办对标准合同制式条款进行严苛限定，缔约双方需妥善协商商业部分的调整；

（3）合规要求。企业可能需要签署“海外版”的标准合同，或配合接收方履行海外法律要求的义务。企业应谨慎评估其签署的合同或履行的义务是否可能违反中国的法律要求。

合同订立后

1、履行备案手续

备案要求：处理者应在标准合同生效之日起10个工作日内向所在地省级网信部门备案。值得注意的是，备案手续的履行完毕不是标准合同生效的前提。

2、事后跟进监督

重新评估与补充合同。在标准合同有效期内出现下列情形之一的，处理者应当重新开展个人信息保护影响评估，补充或重新订立标准合同，并履行相应备案手续：

（1）个人信息出境情况发生变化；

（2）接收方所在地的个人信息保护法规政策发生变化等可能影响个人信息权益；

（3）可能影响个人信息权益的其他情形。

3、其他义务措施

（1）持续监督和评估境外接收方所在地的个人信息保护政策和法规变化；

（2）积极行使合同赋予对境外接收方的监督检查权利；

（3）对合同涵盖的处理活动进行合规审计；

（4）积极响应个人信息主体权利请求。

个人信息保护影响评估的法律依据

为什么要开展个人信息保护影响评估?

有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

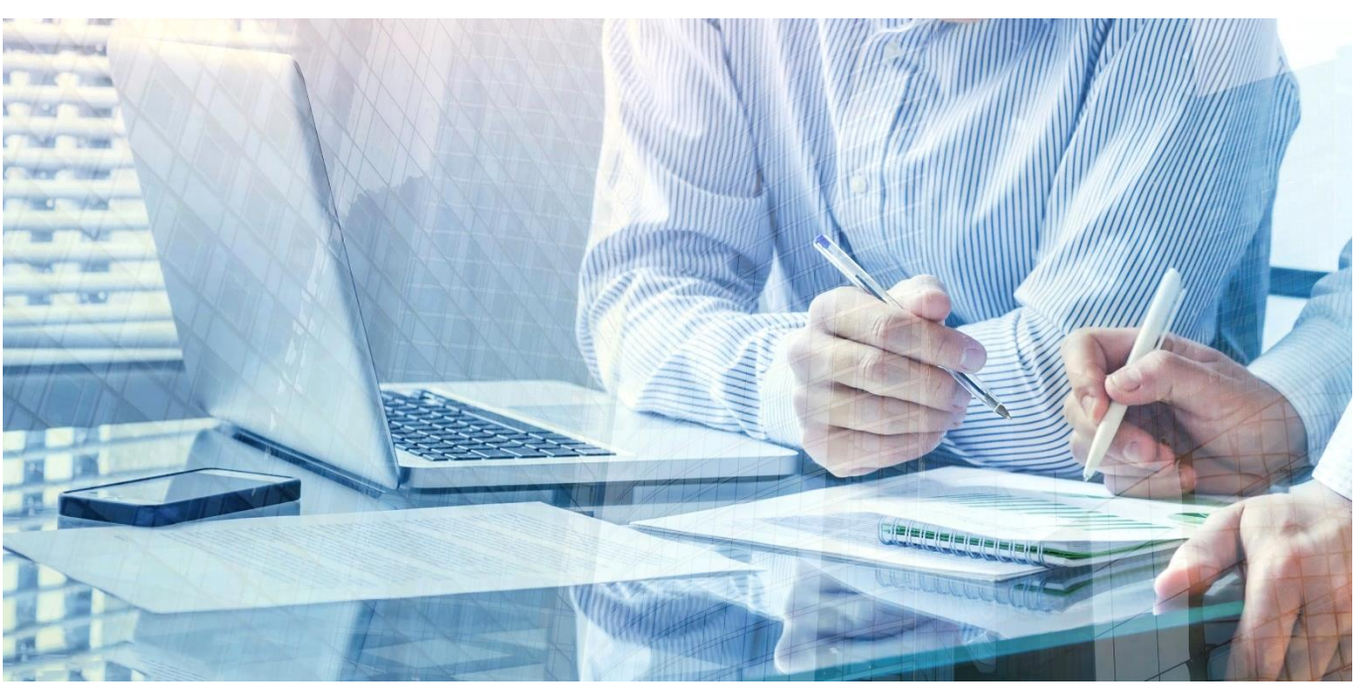
——中国人民共和国个人信息保护法 第五十五条

什么是个人信息保护影响评估?

根据《 GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南》，针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

在业务运营和共享服务中，个人信息保护影响评估将提供一个企业关于如何以及为什么使用、存储和共享个人信息的概况。

评估旨在发现处理个人信息所带来的风险，并采取相应的补救措施，以及满足个保法中的相关监管要求。



个人信息保护影响评估的法律依据（续）

此外，针对**标准合同订立**和**个人信息保护认证**这两条出境路径，下列法规还提出了更加详细的个人信息保护影响评估的要求：

个人信息保护认证

《关于实施个人信息保护认证的公告》，国家互联网信息办公室、国家市场监督管理总局

两个认证依据：个人信息处理者应当符合GB/T 35273《信息安全技术个人信息安全规范》的要求。对于开展跨境处理活动的个人信息处理者，还应当符合TC260-PG-20222A《个人信息跨境处理活动安全认证规范》的要求。

《个人信息跨境处理活动安全认证规范V2.0》，全国信息安全标准化技术委员会

第5.4条 个人信息处理者应对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估，并形成个人信息保护影响评估报告，评估报告至少保存3 年。评估报告应至少包括下列事项：

（一）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；

（二）跨境处理个人信息的规模、范围、类型、敏感程度、频率，个人信息跨境处理可能对个人信息权益带来的风险；

（三）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、能力等能否保障跨境处理个人信息的安全；

（四）个人信息跨境处理存在的泄露、损毁、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；

（五）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履行个人信息保护义务和保障个人信息权益的影响；

（六）其他可能影响个人信息跨境处理安全的事项。

标准合同订立

《个人信息出境标准合同办法》，国家互联网信息办公室

第五条 个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：

（一）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；

（二）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；

（三）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；

（四）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；

（五）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；

（六）其他可能影响个人信息出境安全的事项。

个人信息保护影响评估流程

1 场景

触发个人信息保护影响评估的常见条件：

1) 新上线的系统、应用、产品和服务
2) 业务运营或系统功能存在重大变化
3) 引进新的供应商
4) 现存供应商审查
5) 供应商合同续订或更新

…

2 识别

业务活动/约定/规划中包含个人信息的处理

个人信息

3 评估

对个人权益的影响

影响类别:

- 对数据主体自我决策权的影响
- 造成差别待遇
- 个人声誉受损或精神压力
- 个人财产损失

个人信息安全事件概率

评估域:

- 网络环境及技术措施
- 个人信息处理流程
- 参与者和相关第三方
- 安全形势和处理规模

4 评估结果

风险等级		概率			
		低	中	高	非常高
影响等级	严重	中	高	严重	严重
	高	中	中	高	严重
	中	低	中	中	高
	低	低	低	中	中

公司应考虑内部控制目标和风险偏好确定行动，例如避免/减轻/接受风险。

参考：《信息安全技术——个人信息安全影响评估指南》（GB/T 39335-2020），国家市场监督管理总局、国家标准化管理委员会

个人信息保护影响评估常见挑战与应对建议

在实施个人信息保护影响评估的过程中，常见的挑战与应对建议如下：

01 未充分对组织内的个人信息处理活动进行识别和范围界定

- **挑战：**目前部分企业尚未充分识别组织内的个人信息处理活动，不清楚哪些处理活动依法应开展个人信息保护影响评估。
- **应对建议：**应识别并建立完整的个人信息处理活动清单，并对适用个人信息保护影响评估的处理活动进行范围界定。

02 缺乏个人信息保护影响评估工具和流程

- **挑战：**部分企业尚未建立个人信息保护影响评估的工具和流程，未开展过个人信息保护影响评估。
- **应对建议：**应按照法规及相关国标的要求，制定个人信息保护影响评估工具和流程，并对适用的个人信息处理活动按照法律要求开展个人信息保护影响评估并存档。

03 与企业已有的数据保护影响评估流程难以整合

- **挑战：**目前部分跨国公司已建立基于《欧盟通用数据保护条例》等国外法规要求的数据保护影响评估的流程和工具，此类评估与个人信息保护影响评估既有相似之处又存在一定的差异。
- **应对建议：**应建立本地化的个人信息保护影响评估的工具与流程，并与企业已有的数据保护影响评估流程整合，在符合本地的合规要求的同时满足企业全球化统一运营的需求。

下一步行动建议

01 识别和评估

企业需根据自身业务情况决定出境路径类型，包括安全评估，标准合同或个人信息保护认证：

- 安全评估：企业达到安全评估的条件则**必须**进行安全评估申报。
- 标准合同：较为灵活，流程相对简单，但需要明确数据出境活动具体场景，配合实施个人信息保护影响评估工作。有效期依照合同约定。
- 个人信息保护认证：认证范围较广，但流程和内容相对复杂。需要个人信息处理者与境外接收方约定并遵守同一个人信息跨境处理规则，认证要求亦包含具有法律约束力的文件的签署和个人信息保护影响评估的开展。认证证书有效期为3年。

02 出境路径决策

- 根据识别到的受影响的应用程序和业务流程，梳理跨境数据传输场景，明确相应的境外接收方。
- 建立本地化个人信息保护影响评估流程和检查表，对明确的跨境数据传输场景/处理活动进行影响评估。
- 落实内部快速整改工作。

03 持续关注

- 持续监控企业内部的个人信息处理活动是否达到数据出境自评估的阈值，并根据《数据出境安全评估办法》要求着手准备自评估申报工作。
- 持续关注重要数据目录的正式发布，识别企业是否涉及重要数据的出境。
- 持续关注标准合同备案或个人信息保护认证的时效性，按时进行更新。

毕马威个人信息保护管理服务

毕马威可协助企业解决不同阶段个人信息保护议题：

盘资产 → 找差距 → 建体系 → 强运营 → 勤优化

盘资产	找差距	建体系	强运营	勤优化
个人信息分级管理及处理活动识别和梳理	个人信息保护评估和规划（治理、流程、技术）	个人信息保护管理制度体系建设	个人信息保护管理运营和合规落实	个人信息保护管理成熟度评估、定期风险评估和合规审计

个人信息保护影响评估设计和执行	个人信息安全工程设计和实施（权限管理、加密、去标识化等）	数据出境场景梳理、评估和管理框架流程建设	隐私政策及相关合同文件模板审阅和更新
移动应用/小程序隐私合规评估和整改	第三方个人信息保护管理机制优化和审计	个人信息保护管理对外合规活动运营支持	数据和系统本地化分析、规划与建设

毕马威自动化工具和平台

联系我们

石浩然

毕马威中国
网络安全和数据保护服务
合伙人
电话：+852 2143 8799
henry.shek@kpmg.com

张令琪

毕马威中国
网络安全和数据保护服务
合伙人
电话：+86 (21) 2212 3637
richard.zhang@kpmg.com

郝长伟

毕马威中国
网络安全和数据保护服务
合伙人
电话：+86 (10) 8508 5498
danny.hao@kpmg.com

黄芃芃

毕马威中国
网络安全和数据保护服务
合伙人
电话：+86 (21) 2212 2355
quin.huang@kpmg.com

张倪海

毕马威中国
网络安全和数据保护服务
合伙人
电话：+852 2847 5062
brian.cheung@kpmg.com

林海燕

毕马威中国
网络安全和数据保护服务
合伙人
电话：+852 2143 8803
lanis.lam@kpmg.com

李振

毕马威中国
网络安全和数据保护服务
总监
电话：+86 (10) 8508 5397
jz.li@kpmg.com

邬敏华

毕马威中国
网络安全和数据保护服务
总监
电话：+86 (21) 2212 3180
fm.wu@kpmg.com

周文韬

毕马威中国
网络安全和数据保护服务
总监
电话：+86 (21) 2212 3180
kevin.wt.zhou@kpmg.com

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站:
https://home.kpmg/cn/zh/home/about/offices.html

二零二三年四月出版