数据出境安全评估：背景和要点

北京理工大学 洪延青

2022年9月

国内外背景

监管数据跨境流动的事由

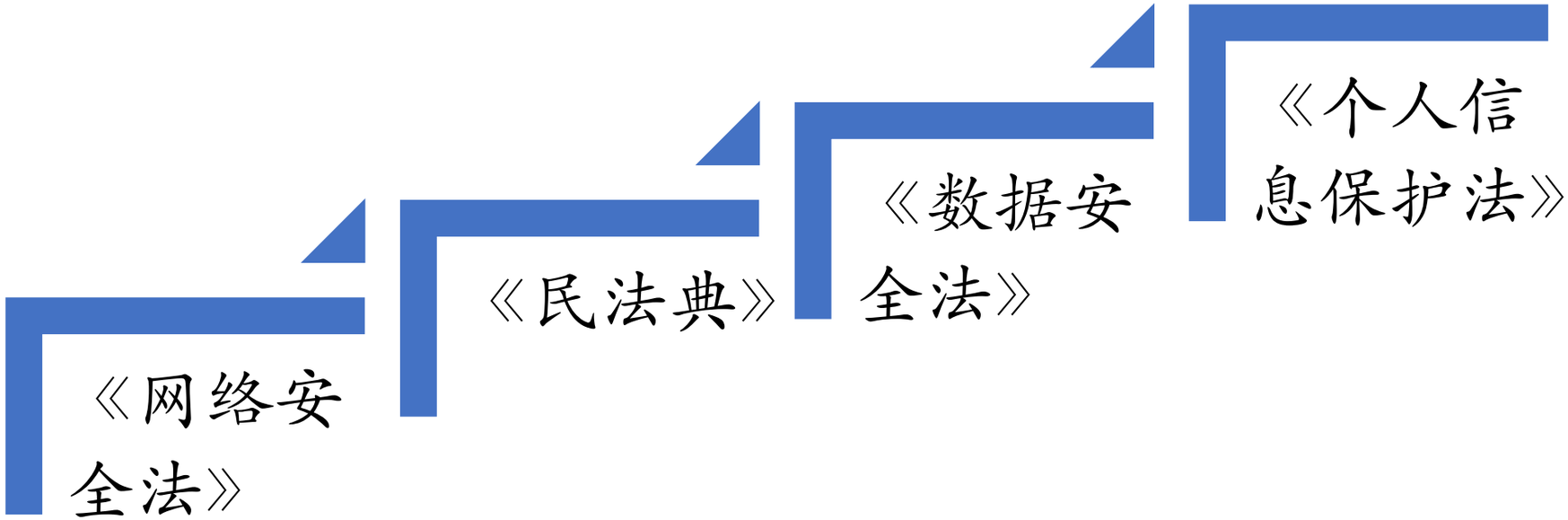
- 数据安全
- 保护个人
- 其他正当公共政策目标
- 国家安全

尚未有国家要求所有电子化数据都在本地化存储。多数国家选择在有限的范围内划定需本地化存储的数据，常见的有以下几类：

a. 个人数据（或个人信息）：这也是最常见的受本地化存储要求的数据类型。

b. 行业内的重要数据：如医疗健康行业（如澳大利亚）、银行业（如中国）、保险业（如中国）、征信业（如中国）、交通（如中国）、电子支付业（如土耳其）、地图数据（如韩国）、网络信息服务（如越南）等

2014年中央网信办成立



《国家安全法》

- 国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和**国家其他重大利益**相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力

《数据安全法》

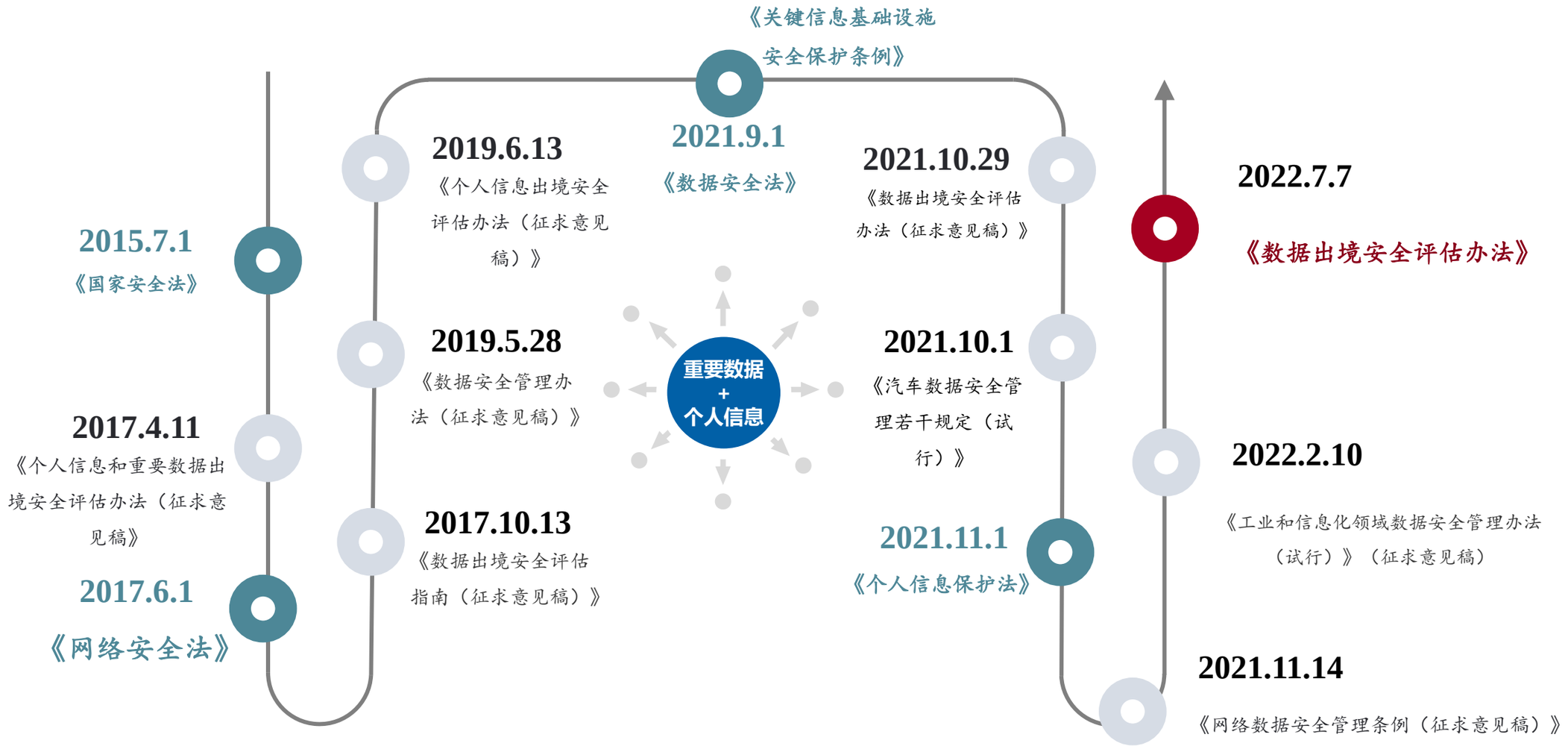
- 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。
- 数据安全，是指通过采取必要措施，确保数据处于**有效保护**和**合法利用**的状态，以及具备保障持续安全状态的能力。

《网络安全法》

- 网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，**使网络处于稳定可靠运行的状态**，以及保障**网络数据的完整性、保密性、可用性**的能力。

数据出境安全的监管背景

立法脉络



合规要点

定义

《数据出境安全评估指南（征求意见稿）》：“网络运营者通过网络等方式，将其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，通过**直接提供**或**开展业务**、**提供服务**、**产品**等方式提供给境外的机构、组织或个人的一次性活动或连续性活动。”

识别出境

- 数据未转移存储至本国以外的地方，但**被境外的机构、组织、个人访问查看的**（公开信息、网页访问除外）；
- **网络运营者集团内部数据由境内转移至境外**，涉及其在境内运营中收集和产生的个人信息和重要数据的。

数据出境安全的监管背景

主体不一致

境外接收者数据保护能力发生变化，可能造成数据泄露或滥用。

法律不一致

各国对数据保护的态度不同，数据跨境流动缺乏统一的标准，用户个人信息权益保障可能难以为继。

监管不一致

一旦发生数据安全事件，境外维权取证存在困难，执法权收到阻碍。

国家安全问题

数据跨境流动易引发数据安全风险，威胁国家主权与安全。

数据出境安全的监管背景 —— 《个人信息保护法》

监管思路

前提条件（必要条件1）

（一）依照本法第四十条的规定通过国家网信部门组织**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他条件。

必要条件2

- 告知
- 单独同意
- 个人信息保护影响评估
- 保障接受方标准

CIIO +处理个人信息达到国家网信部门规定数量的个人信息处理者

应当将在中国境内收集和产生的个人信息存储在境内

其他重要数据

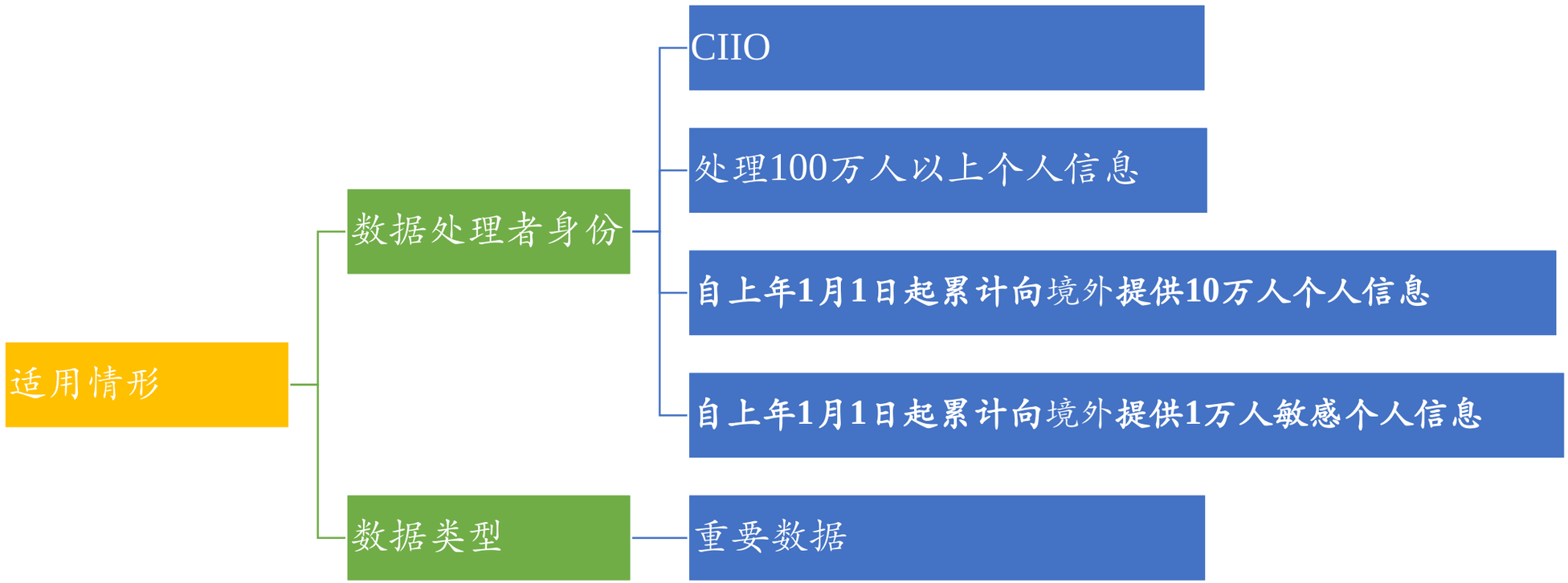
其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

→ 《数据出境安全评估办法》
《网络数据安全管理条例》

CIIO 在中华人民共和国境内运营中收集和产生的重要数据，适用《网络安全法》

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；法律、行政法规另有规定的，依照其规定。

数据出境安全的适用情形



个人信息和敏感个人信息

个人信息 Personal Information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

敏感个人信息 Sensitive Personal Information

敏感个人信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

“处理个人信息达到一百万人或累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息”

- ✓ 在向境外提供个人信息前需申报出境安全评估的个人信息处理者，其本身即掌握、存储、拥有，或者对多达一百万人的个人信息的处理握有事实上的控制权。
- ✓ 在个人信息处理者向境外提供的个人信息达到了涉及十万人以上的程度，或者对外提供的敏感个人信息达到了影响一万人以上的规模。

敏感个人信息示例

类别	典型示例和说明
特定身份	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证、港澳台通行证等
生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、面部识别特征、步态等
金融账户	金融账户及金融账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、证券账户、基金账户、保险账户、其他财富账户、公积金账户、公积金联名账号、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等
医疗健康	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
行踪轨迹	基于实时地理位置形成的个人行踪和行程信息，例如实时精准定位信息、GPS 车辆轨迹信息、出入境记录、住宿信息（定位到街道小区甚至更精确位置的数据）等
未成年人个人信息	14 岁以下（含）未成年人的个人信息
身份鉴别信息	用于验证主体是否具有访问或使用权限的信息，包括但不限于登录密码、支付密码、账户查询密码、交易密码、银行卡有效期、银行卡片验证码（CVN 和 CVN2）、口令、动态口令、口令保护答案、短信验证码、密码提示问题答案、随机令牌等
其他敏感个人信息	种族、性取向、婚史、宗教信仰、未公开的违法犯罪记录等

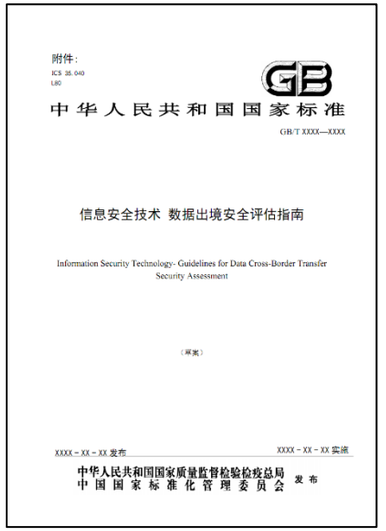
重要数据

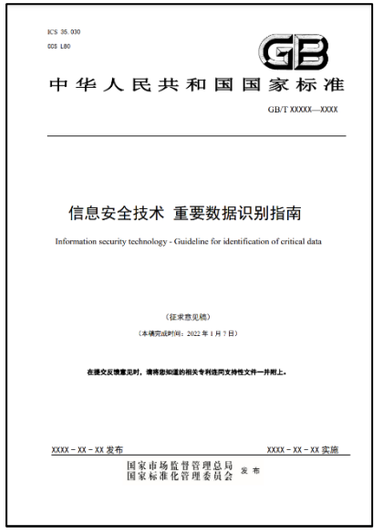
重要数据 Critical Data

以电子方式存在的，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

注：重要数据不包括国家秘密和个人信息，但基于海量个人信息形成的统计数据、衍生数据有可能属于重要数据。

虽然重要数据的具体范围还不明确，但根据目前已有的参考文件，“反映国家战略储备、应急动员能力，如战略物资产能、储备量属于**重要数据**；支撑关键基础设施运行或重点领域工业生产，如直接支撑关键基础设施所在行业、领域核心业务运行或重点领域工业生产的数据属于重要数据”。


附件：
ICS 35.040
L80
GB
中华人民共和国国家标准
GB/T XXXX—XXXX
信息安全技术 数据出境安全评估指南
Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment
（草案）
XXXX－XX－XX 发布
XXXX－XX－XX 实施
中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布


ICS 35.030
L80
GB
中华人民共和国国家标准
GB/T XXXXX—XXXX
信息安全技术 重要数据识别指南
Information security technology - Guideline for identification of critical data
（征求意见稿）
（本稿完成时间：2022 年 1 月 7 日）
在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。
XXXX－XX－XX 发布
XXXX－XX－XX 实施
国家市场监督管理总局
国家标准化管理委员会 发布

参考文件：

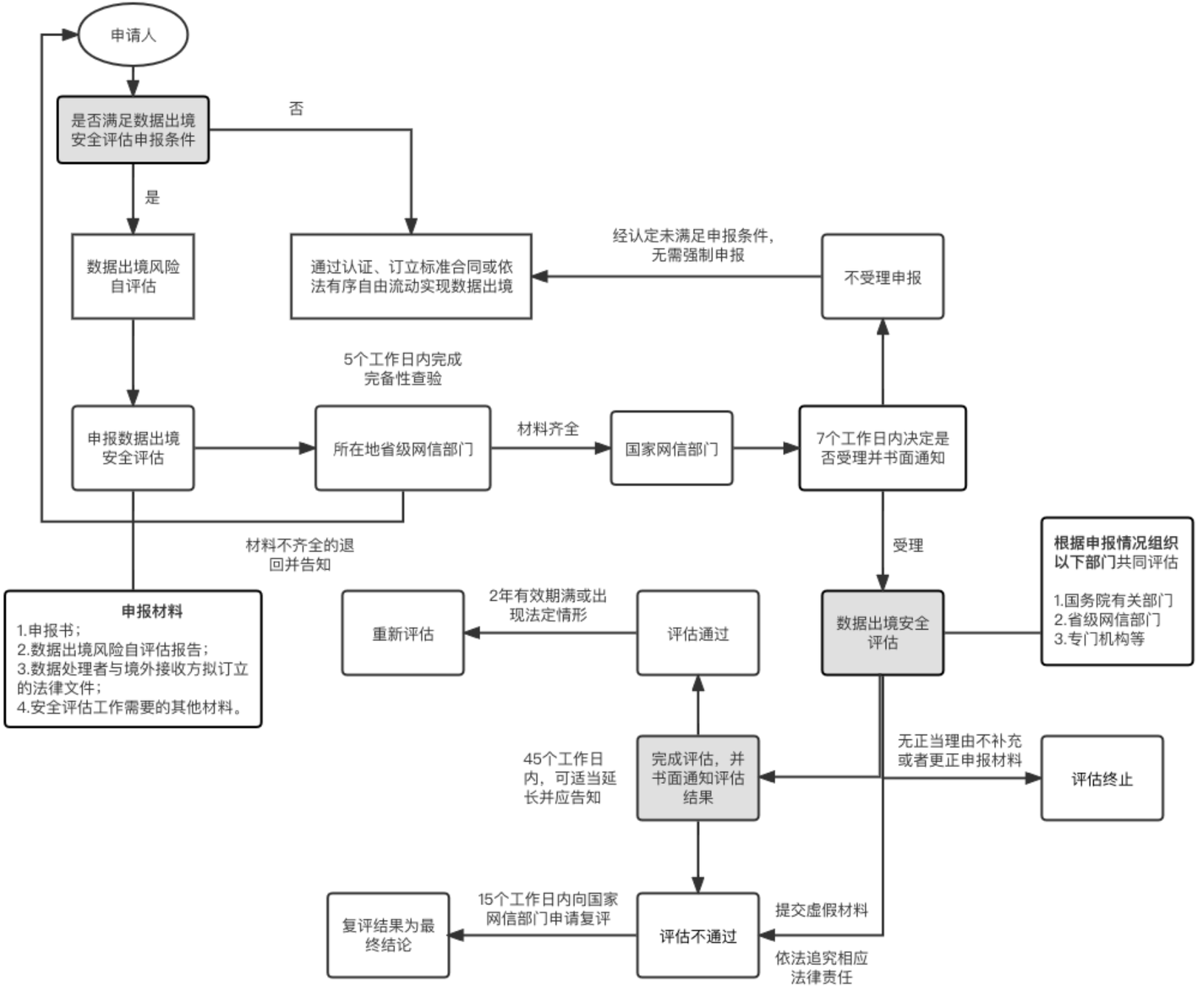
《信息安全技术 数据出境安全评估指南（征求意见稿）》附录A

《重要数据识别指南》

《信息安全技术 重要数据识别指南（征求意见稿）》（2021.9.23）

《信息安全技术 重要数据识别指南》（征求意见稿）（2022.1.13）

数据出境安全的评估流程



重点评估事项	需要关注的问题
（一）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、必要性	关注是否属于法律禁止事项；是否符合数据出境条约、协议规定；是否获取个人信息主体的授权；是否属于业务开展所必需；是否属于其他依法应当开展的情形等。
（二）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	建议出境方企业根据具体业务场景，针对数据的规模、范围、种类、敏感程度等特点采取相应的分级、分类管理，同时根据数据属性，结合出境方数据出境的技术和管理能力，分析研判数据出境发生安全事件的风险。
（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、能力等能否保障出境数据的安全	关注境外接收方内部管理和防护技术的可靠性，结合其既往安全管理水平，采取的具体保护措施评估安全保护能力，同时需关注外部因素影响，例如接收方所在国家或地区的政治法律环境等因素。在相应的法律文件明确接收方的责任义务，由其作出承诺。
（四）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	关注保障数据传输的保密性、完整性、真实性等问题的技术能力以及针对数据安全风险的响应能力，考察访问权限管理、数据源鉴别、存储介质等方面。实操上具备相应的技术工具防范DDOS、网络攻击、数据爬虫等异常行为。畅通的个人信息权益维护渠道。
（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务	《办法》第九条规定数据出境双方订立的法律文件中需明确约定数据安全保护责任义务，涵盖数据出境目的、方式、数据范围、保存期限、数据出境后再转移的约束、补救措施、争议解决方式等等。 2022年6月发布的《个人信息出境标准合同规定（征求意见稿）》作为出境的配套文件，也在第六条就条款设计规定了标准合同需要包括的主要内容。相关企业可以根据自身业务涉及到的数据类型对照两个文件开展自评估。
（六）其他可能影响数据出境安全的事项	例如中美两国因PCAOB审验在美中概股审计底稿等问题存有分歧。

**只有具备数据出境安全评估申报情形的数据处理者需在出境前进行数据出境自评估。*

自评估与国家网信评估内容高度一致

风险自评估事项	安全评估事项	说明
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、必要性	数据出境的目的、范围、方式等的合法性、正当性、必要性	前者较后者增加“境外接收方”处理目的等合法、正当、必要性
出境数据的规模、范围、种类、敏感程度	出境数据的规模、范围、种类、敏感程度	一致
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；	数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险	虽然前者与后者一致，但后者在表述上与其他所有安全评估事项构成“总分”关系
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；	N/A	前者需要重点评估接收方履约能力
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；	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；	一致
个人信息权益维护的渠道是否通畅等；	数据安全和个人信息权益是否能够得到充分有效保障	后者涵盖的范围比前者更广
与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务。	数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务。	一致
N/A	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。	仅在后者列出，评估部门的特有审核事项
N/A	遵守中国法律、行政法规、部门规章情况	仅在后者列出，评估部门的特有审核事项

数据出境安全评估制度落地指南

合同要求

01	目的方式范围	数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等
02	存储	数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施
03	再转移	对于境外接收方将出境数据再转移给其他组织、个人的约束性要求
04	安全补救措施	境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施
05	争议解决	违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式
06	应急处置	出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式

**法律文件经签署发生效力后，存在数据安全评估未通过进而无法履约的违约风险。我们认为谨慎的解决方案是将安全评估未通过情形与合同解除条款相结合，或者约定合同的生效条件为安全评估通过情形。*

评估有效期

- ✓ 数据处理者通过国家网信部门数据出境安全评估后，在**二年内**无需就同一接收者后续的多次或连续的传输类似数据申请重新评估。
- ✓ 有效期届满，需要继续开展原数据出境活动的，数据处理者应当在有效期届满**六十个工作日前**重新申报评估。

重新申报情形

- ✓ 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；
- ✓ 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；
- ✓ 出现影响出境数据安全的其他情形；
- ✓ 国家网信部门发现已经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。

行为	罚则		法律依据
	数据处理者	直接负责的主管人员和其他直接责任人员	
CIIO非法在境外存储数据或非法向境外提供数据	由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，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	对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款	《网安法》第六十六条
非法向境外提供重要数据	由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款	对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款	《数安法》第四十六条
	情节严重的，处一百万元以上一千万元以下罚款，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	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以上一百万元以下罚款	
非法向境外提供个人信息或向境外提供个人信息未履行个人信息保护义务	由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款	对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款	
	情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万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	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以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人	《个保法》第六十六条

感谢聆听