天達共和律師事務所
East & Concord Partners

数据出境的法律风险及控制

演讲人：天达共和律师事务所合伙人　冯超

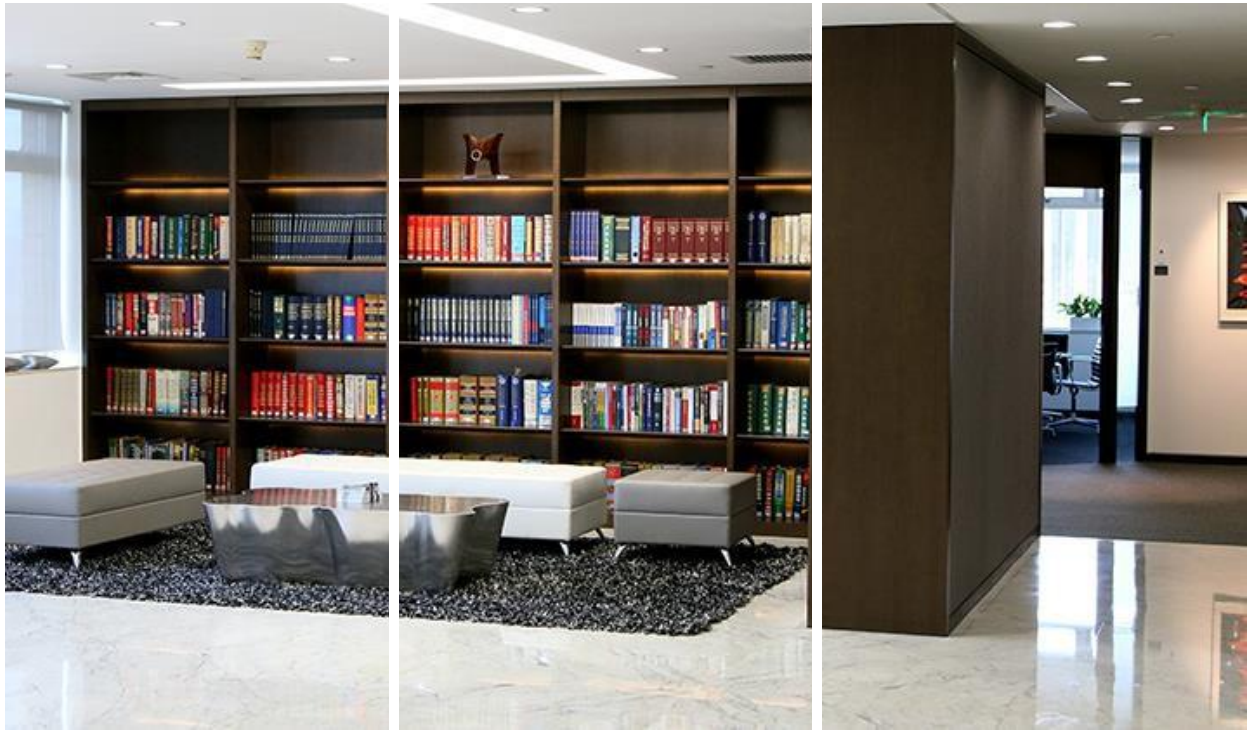
L-Council简介

L-Council为理购与协同共享企业服务（上海）股份有限公司旗下服务品牌。秉承“专业分享、价值创造”的企业使命，致力于成为国内优质的汇聚知名跨国企业及本土大型企业法务人员的会员制服务机构。**L-Council**以专业人群为依托，结合特定行业，精准聚焦法务经理人，旨在提供最佳实战经验分享及法律信息服务。在中国已有超过1000家会员企业，30，000多位企业法务同行使用和体验**L-Council**的超值分享服务。

CHINA LEGAL
Executive Council

L-Council 电话：021-62705678-1086
邮箱：cs1@lcouncil.com

目录



主要内容：

- 数据保护法律体系
- 数据出境的理解
- 数据出境的监管
- 数据出境的合规安排建议

数据保护的法律法规体系

法律（综合）

- 《**网络安全法**》（2017）

第三十七条：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**应当在境内储存。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

- 《**国家安全法**》

第十六条规定国家“保障公民的生命财产安全和其他合法权益” 个人信息具有数据和公民权益的双重属性；

第二十五条明确规定国家“实施网络和信息核心技术、关键基础设施和重要领域信息系统及数据安全可控”，重要数据即对应“**关键基础设施和重要领域信息系统及数据**”

- 《**数据安全法（草案）**》（2020）

第二条（域外管辖）“属地管辖”与“保护性管辖”相结合，即《数据安全法（草案）》适用于“中华人民共和国境内开展的数据活动”以及“中华人民共和国境外的组织、个人开展的损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的数据活动”。

第三条（调整对象）数据活动,是指数据的收集、存储、加工、使用、提供、交易、公开等行为。数据出境问题当然受其调整。从这部法案中也可以看出，数据跨境问题已逐渐上升到国家主权、数据主权、国家安全层面，监管部门对于企业的数据跨境流动也将可能形成更加严格的规制要求。

数据保护的法律法规体系

法律（刑事、行政）

《刑法》、《刑法修正案（九）》

侵犯公民个人信息罪、危害国家安全类犯罪和拒不履行信息网络安全管理义务罪

- 《保守国家秘密法》

第四十八条，任何“在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递**国家秘密**的”行为都应当受到行政处分；如果该传输行为情节严重的，可能触犯刑法的，则需要追究刑事责任。

数据保护的法律法规体系

法律（民商事）

- **《民法典》（2020）第六章**

第六章专门就**隐私权**和**个人信息**保护作出规定，尤其对个人信息处理者（个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。）在第一千零三十五条、一千零三十六条提出要求，其中就涉及到个人信息境外传输问题

- **《电子商务法》（2019）**

第二十六条规定“电子商务经营者从事跨境电子商务，应当遵守进出口监督管理的法律、行政法规和国家有关规定。”同时，第七十九条规定：电子商务经营者违反法律、行政法规有关**个人信息保护**的规定，或者不履行本法第三十条和有关法律、行政法规规定的网络安全保障义务的，依照《中华人民共和国网络安全法》等法律、行政法规的规定处罚。

- **《消费者权益保护法》（2014）**

第二十九条规定：经营者及其工作人员对收集的**消费者个人信息**必须严格保密，不得泄露、出售或者非法向他人提供。这意味着，经营者在数据出境过程中若涉及消费者个人信息的相关内容，需按照相关法律法规的程序进行。

数据保护的法律法规体系

行政法规

. 《人类遗传资源管理条例》

第四条：“国家对重要遗传家系和特定地区遗传资源实行申报登记制度，发现和持有重要遗传家系和特定地区遗传资源的单位或个人，应及时向有关部门报告。未经许可，任何单位和个人不得擅自采集、收集、买卖、出口、出境或以其他形式对外提供”。

第七条：“明确禁止外国组织、个人及其设立或实际控制的机构在我国境内采集、保藏、对外提供我国人类遗传资源”因此受到了行政处罚”

- 《中华人民共和国消费者权益保护法实施条例》

第二十二条：“经营者收集、使用消费者个人信息应当遵循**合法、必要、正当**的原则。”

数据保护的法律法规体系

部门规章

	部门	名臣	发布日
1	国家互联网信息办公室	《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称“安全评估办法（2017）”）	2017-4-11发布
2	国家互联网信息办公室	《个人信息出境安全评估办法（征求意见稿）》（以下简称“安全评估办法（2019）”）	2019-6-13发布
3	国家互联网信息办公室	《数据安全管理办法（征求意见稿）》（以下简称“数据管理办法”）	2019-5-28发布
4	国家互联网信息办公室	《网络安全审查办法》	2020-04-13 发布 2020-06-01正式生效

数据保护的法律法规体系

部门规章

- 《评估办法 2017 》

《网络安全法》中的责任主体由“关键信息基础设施运营者”=》“网络运营者”，重申数据本地化存储的要求，并提出因业务需要确需向境外提供个人信息和重要数据时的**安全评估**的流程、评估重点及具体要求

- 《评估办法 2019》、《数据管理办法 2019》

合理地审查向境外传输数据的情形，对于可能影响**国家安全、损害公共利益**，或者难以有效保障**个人信息**安全性的情况下，**禁止**相关的个人信息或重要数据向**境外传输**。

- 《网络安全审查办法 2020》

第二条“**关键信息基础设施运营者**采购**网络产品和服务**，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。”该办法是配套《网络安全法》就网络数据等产品与服务的采购等影响或可能影响国家安全的情形，构建了网络安全审查制度并对审查的具体机关、程序、内容等予以规定。其中涉及互联网等数据出境问题的，需按此规定进行安全审查。

第二十条：本办法中**关键信息基础设施运营者**是指经关键信息基础设施保护工作部门认定的运营者。

本办法所称**网络产品和服务**主要指核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。

数据保护的法律法规体系

国家标准

序号	部门	国家标准	标准号	日期
1	全国信息安全标准化技术委员会	**《信息安全技术数据出境安全评估指南（草案）》（“指南”）**		2017-5-27发布
		《信息安全技术数据出境安全评估指南（征求意见稿）》		2017-8-30发布
2	全国信息安全标准化技术委员会	《信息安全技术个人信息安全规范》（以下简称“安全规范”）	GB/T35273-2020	2020-3-06发布

数据保护的法律法规体系

- 《指南》对数据安全出境评估内容为“首先评估数据**出境目的**……在此基础上评估**数据出境安全风险**，将数据**出境及再转移后被泄露、毁损、篡改、滥用等风险**有效地降至最低限度”，同时扩充并完善数据出境定义，提出“**境内运营**”的判断标准。

- 除此之外，在其他的一些规范性文件中散件对**个人信息出境**问题的规定
  - 《互联网个人信息安全保护指南》5.3扩展要求之5.3.1云计算安 全扩展要求规定：a)应**确保个人信息**在云计算平台中**存储**于中 国**境内**，如需**出境**应遵循国家相关规定；
  - 《App违法违规收集使用个人信息自评估指南》：一、隐私政 策文本评估事项3:12.个人信息出境“如果存在个人信息出境情 况，隐私政策中应将**出境个人信息类型**逐项列出并**显著标识**（如字体加粗、标星号、下划线、斜体、颜色等）。”

数据保护的法律法规体系

其他：

- 《地图管理条例》第三十四条
- 《网络预约出租汽车经营服务管理暂行办法》第二十七条
- 《网络出版服务管理规定》第八条
- 国家卫生计生委发布的《人口健康信息管理办法(试行)》第十条
- 国务院发布的《征信业管理条例》第二十四条
- 《中国人民银行金融消费者权益保护实施办法》第三十条以及《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第六条。
- 《中国人民银行金融消费者权益保护实施办法（征求意见稿）》第三十四条
- 《私募投资基金服务业务管理办法（试行）》第四十八条
- 《关于加强在境外发行证券与上市相关保密和档案管理工作的规定》第六 条
- 《中华人民共和国对外合作开采海洋石油资源条例》第二十一条”；
- 《证券基金经营机构信息技术管理办法》第三十条规定：
- 《外商投资期货公司管理办法》第十五条规定
- 《邮件快件实名收寄管理办法》第十六条：
- 《国家健康医疗大数据标准、安全和服务管理办法（试行）》第三十条规定”

数据出境：基本概念

数据出境：

《安全评估办法（2017）》国家互联网信息办公室

第十七条，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**，**提供给境外**的**机构、组织、个人**。

《安全评估办法（2019）》第二条“**个人信息**出境”是指网络运营者**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。

《指南》规定数据出境是指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。《指南》进一步明确了数据出境包括以下情形：

- 向本国**境内**、但**不属于本国司法管辖**或**未在境内注册**的**主体**提供**个人信息和重要数据**；（接受主体）
- 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）；（接受主体）
- 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。（客体）
- 根据《指南》：**非在境内运营中收集和产生**的个人信息和重要数据经本国出境，**未经任何变动或加工处理**的，**不属于**数据出境。**非在境内运营中收集和产生**的个人信息和重要数据**在境内存储、加工处理**后**出境**，**不涉及境内运营中收集和产生**的个人信息和重要数据的，不属于数据处境。（客体：否；过境）

数据出境：主体

1、关键信息基础设施运营者

《网络安全法》第三十七条规定“**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”

1“关键信息基础设施”仅限于“**公共通信和信息服务、能源、交通、水 利、金融、公共服务、电子政务**等重要行业和领域，以及其他一旦遭到破坏、 丧失功能或者数据泄露，可能**严重危害国家安全、国计民生、公共利益**的关键 基础设施”。

2 “网络运营者”是指“网络的**所有者、管理者和网络服务提供者**”。

- 几乎所有的互联网运营商、网络新媒体企业以及利用互联网提供服务信息的传统企业（例如银行、保险公司等）都有可能被纳入。
- 《安全评估办法（2017）》还规定，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，这意味着数据出境限制进一步扩展到全社会范围。

数据出境：主体

1、关键信息基础设施运营者

《网络安全法》第三十七条规定“**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”

1“关键信息基础设施”仅限于“**公共通信和信息服务、能源、交通、水 利、金融、公共服务、电子政务**等重要行业和领域，以及其他一旦遭到破坏、 丧失功能或者数据泄露，可能**严重危害国家安全、国计民生、公共利益**的关键 基础设施”。

2 “网络运营者”是指“网络的**所有者、管理者和网络服务提供者**”。

- 几乎所有的互联网运营商、网络新媒体企业以及利用互联网提供服务信息的传统企业（例如银行、保险公司等）都有可能被纳入。
- 《安全评估办法（2017）》还规定，**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，这意味着**数据出境限制**进一步扩展到全社会范围。

数据出境：客体

1.1、个人信息

- 《民法典》第1034条：“自然人的个人信息受法律保护；个人信息是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特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定”。

- 《网络安全法》：个人信息是指以电子或者其他方式记录的能够单独或者电子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。

- 两高司法解释：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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

数据出境：客体

1.1、个人信息示例

个人信息的类型	举 例
个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	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，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货 币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

数据出境：客体

1.2、**个人敏感信息**

- 《指南》：在个人信息基础上，还进一步明确了**个人敏感信息**，即指一旦泄露、披露或滥用可能危害人身和财产安全、损害个人名誉和身心健康 、导致歧视性待遇等的个人信息。通常情况下，身份证号、银行卡号、健 康记录、生物识别等属于个人敏感信息。

- 《安全评估办法（2019）》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个人信息。

- 《信息安全技术个人信息安全规范》规定个人敏感信息是指：一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。个人敏感信息包括身份证件号码、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

数据出境：客体

1.2、个人敏感信息示例

个人敏感信息	举 例
个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	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
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

数据出境：客体

2、重要数据

- 《安全评估办法（2017）》：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。

- 《安全评估办法（2019）》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个人信息。

- 《信息安全技术个人信息安全规范》规定个人敏感信息是指：一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。个人敏感信息包括身份证件号 码 、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息 、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

- 判断属于重要数据路径

《指南》附录A（规范性附录）为重要数据识别指南，将各个行业、业务中重要数据的具体类型、数量、范围等进行了规定。

数据出境的监管

- 境内存储原则
- 授权原则
- 合法性原则
- 必要性原则
- 正当性原则
- 最小化原则

数据出境的监管：境内存储原则

- 《网络安全法》第37条规定，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应当在境内存储。

- 《安全评估办法（2017）》 第2条规定，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，应当在境内存储。

应对：知名科技公司相继在中国建立数据中心以存储国内用户的个人信息。如苹果中国（贵安）数据中心、亚马逊西云数据中心等。

数据出境的监管：境内存储原则

规定	条款
《人口健康信息管理办法（试行）》	不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器。人口健康信息，是指依据国家法律法规和工作职责，各级各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息。
《中国人民银行金融消费者权益保护实施办法》	在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。
《网络预约出租汽车经营服务管理暂行办法》	网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于2年，除法律法规另有规定外，上述信息和数据不得外流。

数据出境的监管：授权原则

- **个人信息**：个人信息主体的同意；
  - 《民法典》1035条：合法、正当、必要原则，不得过度处理，并符合下列条件：（一）征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外；（二）公开处理信息的规则；（三）明示处理信息的目的、方式和范围；（四）不违反法律、行政法规的规定和双方的约定。

  - 《指南》**明示同意**：个人信息主体通过书面声明，对其个人信息出境做出明确授权的行为。

  - 《指南》**默示同意**：个人信息主体通过做出肯定性行为

拨打国际及漫游电话、发送国际电子邮件、进行国际即时通信、通过互联网进行**跨境交易**以及其他个人主动行为，以及将合法向社会**公开披露**的个人信息出境等，**视为**个人信息主体已经**同意**。

数据出境的监管：授权原则

重要数据：出境时需要获得国家相关部门的批准。

《安全评估办法（征求意见稿）》第九条

个人信息和重要数据出境明确规定，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1000 GB；

（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、安全防护等信息；

（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社会公共利益，行业主管或监管部门认为应该评估。

数据出境的监管：授权原则

《评估办法》第八条：数据出境安全评估应重点评估以下内容：

（一）数据出境的必要性；

（二）涉及情况，包括的数量、范围、类型、敏感程度，以及主体是否同意其出境等；

（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；

（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；

（五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；

（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；

（七）其他需要评估的重要事项。

数据出境的**监管：授权原则**

第十一条　存在以下情况之一的，数据不得出境：

（一）**个人信息**出境**未经**个人信息主体**同意**，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。

数据出境的**监管：授权原则**

第十一条　存在以下情况之一的，数据不得出境：

（一）**个人信息**出境**未经**个人信息主体**同意**，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。

数据出境的监管：必要性原则

《网络安全法》第三十七条 “确需向境外提供的”

《指南》第八条

数据出境安全评估应重点评估以下内容：

（一）数据出境的必要性；

《指南》规定的必要性包括以下任一种或几种情况： 1）履行合同义务所必需的；

2 同一机构、组织内部开展业务所必需的；

3 我国政府部门履行公务所必需的；

4履行我国政府或其他国家和地区、国际组织签署的条约、协议所必需的；

5 其他维护网络空间主权和国家安全、经济发展、社会公共利益和保护公民合法利益需要的。

数据出境的**监管：正当性原则**

- 《全国人大常委会关于加强网络信息保护的决定》(2012) 网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则；

- 《指南》规定的正当性包括以下情形：

1）个人信息主体已**同意**的（虽未经个人信息主体同意但是危及公民生命财产安全等紧急情况除外）； 2）不违反相关主管部门规定。

- 《安全评估办法（2019）》第二条明确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。存在可能影响国家安全、损害社会公 共利益或者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，则不允许出境。

数据出境的监管：最小化原则

- **最小化原则**：防止数据出境行为发起方以超出其开展业务所必 需的数量、频率将数据传输出境，从而造成安全风险。

- **具体要求**：
  - 向境外传输的个人信息应与出境目的相关的业务功能有**直接关联**（直接关联是指没有该信息的参与，相应功能无法实现）
  - 向境外自动传输的个人信息**频率**应是与数据出境目的相关的业务功能所**必需**的频率；
  - 向境外传输的个人信息**数量**应是与数据出境目的相关的业务功能所**必需**的数量。

数据出境的监管主体

- 《数据安全法（草案）》

第六条：中央国家安全领导机构负责数据安全工作的决策和统筹协调

第七条规定工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等主管部门承担本行业、本领域数据安全监管职责；公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责；国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

- 《网络安全审查办法》

第四条：中央网络安全和信息化委员会领导下，**国家互联网信息办公室**会同国家发改委、工信部、公安部、国安部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局建立国家网络安全审查工作机制。网络安全审查办公室设在**国家互联网信息办公室**，负责制定网络安全审查相关制度规范，组织网络安全审查。

数据出境的**监管主体**

- 《数据管理办法》第五条

在中央网络安全和信息化委员会领导下，国家网信部门统筹协调、指导监督个人信息和重要数据安全保护工作；地（市）及以上网信部门依据职责指导监督本行政区内个人信息和重要数据安全保护工作。

- 《安全评估办法（2017）》第五条

国家网信部门统筹协调数据出境安全评估工作，指导行业主管或监管部门组织开展数据出境安全评估；第六条**行业主管或监管部门**负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。

- 《安全评估办法（2019）》第三条

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。

数据出境的**监管审批**

- **出境前**

1. 合法数据审查：数据提供方应当提供符合法律规定的数据出境，《安全评估办法（2017）》第十一条规定,存在以下情况之一的,数据不得出境:
   - 个人信息出境未经个人信息主体同意,或可能侵害个人利益;
   - 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;
   - 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。

数据出境的监管审批

出境前

2、**数据安全评估**

- 《安全评估办法（2017）》：数据安全评估将成为数据出境合规中不可或缺的一环
- 数据安全评估程序包括两类
  - 网络运营者自行组织的安全评估
  - 由行业主管或监管部门组织安全评估。

3、**数据脱敏：**数据提供方需要对某些敏感数据通过脱敏规则进行变形脱敏处理，防止隐私敏感数据在未经脱敏的情况下泄露。

- **重要数据**在出境前，网络运营者应对其采取数据脱敏处理等措施，并对数据脱敏处理的效果进行验证，使其不能被还原为原始数据。脱敏处理后的重要数据能适度降低出境带来的安全风险。
- 网络运营者可在满足业务需求的前提下，对拟出境的**个人信息**采取去标识化等数据脱敏处理措施，并应**与可用于恢复标识的信息分别存储**采取技术和管理措施**单独存储去标识化后个人信息**。经技术处理后的个人信息能有效降低数据出境安全风险。

数据出境的监管审批

出境前

关键要素	影响等级	修正要素		
敏感程度		数量	范围	技术处理情况
个人敏感信息为主	3	一年内涉及出境的个人信息累计大于主管部门规定的大量个人信息时影响等级可增加1。	如果出境个人信息超出满足出境目的最小集，则影响等级可增加1。	**使用技术措施对涉及出境的个人信息进行去标识化处理能有效防止识别出个人的，影响等级可减去1。**
包含少量个人敏感信息（如个人敏感信息占个人信息中的比例小于50%）	2			
仅为个人信息不包含个人敏感信息	1			

数据出境的**监管审批**

出境前

- 签订合同（接收方义务的约定）

与出境数据接收者签订合同，**合同条款**应当包括：

1　　数据**接收方**进行**数据处理的目的、方式**和采取的**安全措施**；

2　　数据**接收方配合**对数据出境活动进行**审查**的**义务**；

3　　数据**接受方**对出境数据的**使用范围**；

4　　数据**接收方使用、留存**数据的**期限**及**超出约定期限**后数据接收方应对数据**采取的合理措施**如：删除、销毁等。

合同签订后，如果数据接收方出现**违约**行为，数据提供方可依据合同约定追究数据接收方的**违约责任**，有利于减轻企业应对数据出境后的数据安全监管压力。

数据出境的**监管审批**

出境后

- **出境记录**

建立信息出境记录并至少保存**5年**，记录应当包括：

1　　向境外提供数据的**日期**时间。

2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。

3　　向境外提供的数据的**类型及数量、敏感程度**。

4　　国家网信部门规定的其他内容。

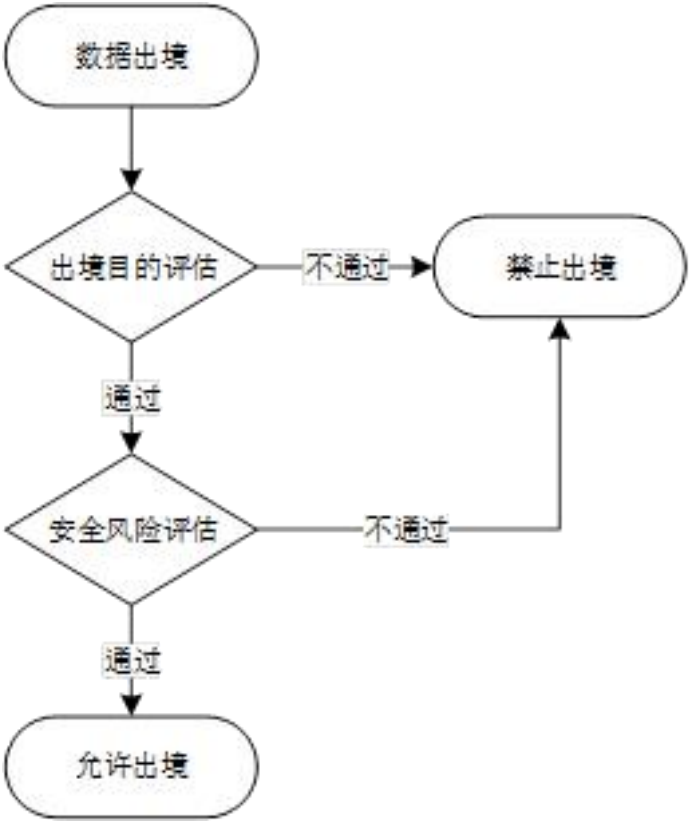
- **专人管理**

指定专职人员从事数据出境安全管理工作，负责数据出境转移的审计、合规管理、评估报告的编写与提交、配合主管部门监督检查、处理有关纠纷等工作。

数据出境的监管审批

出境后

安全评估总流程



数据出境的监管审批

安全评估机构

- 《安全评估办法（2017）》第五条：“国家网信部门统筹协调数据出境安全评估工作，指导行业主管或者监管部门组织开展数据出境安全评估”，第六条规定“行业主管或监管部门负责本行业数据出境安全评 估工作，定期组织开展本行业数据出境安全检查”。《安全评估办法（2019）》第三条规定个人信息出境前，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。

- 单一部门：如银行、保险企业，其行业主管或者监管部门较为明显

- 多部门监管的企业（如互联网企业）、以及综合利用多个类型的个人 信息和重要数据的企业（如大数据挖掘型企业）或者机构，其可能面 临多个行业主管或者监管部门的安全检查，而辨别这类企业或机构究 竟属于哪些行业主管或监管部门归口管理，是一个考验监管部门对相关行业的理解能力和执法能力的问题。对此，《安全评估办法（2017）》规定，行业主管或监管部门不明确的，由国家网信部门组织评估。

- 同时，对不能出境的数据认定上，网信部门、公安部门、安全部门等 有关部门可以行使否决权。

数据出境的监管审批

安全评估申报材料《安全评估办法（2019）》

- **申报材料：**个人信息出境需要提交的材料部分。

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；

（四）国家网信部门要求提供的其他材料。

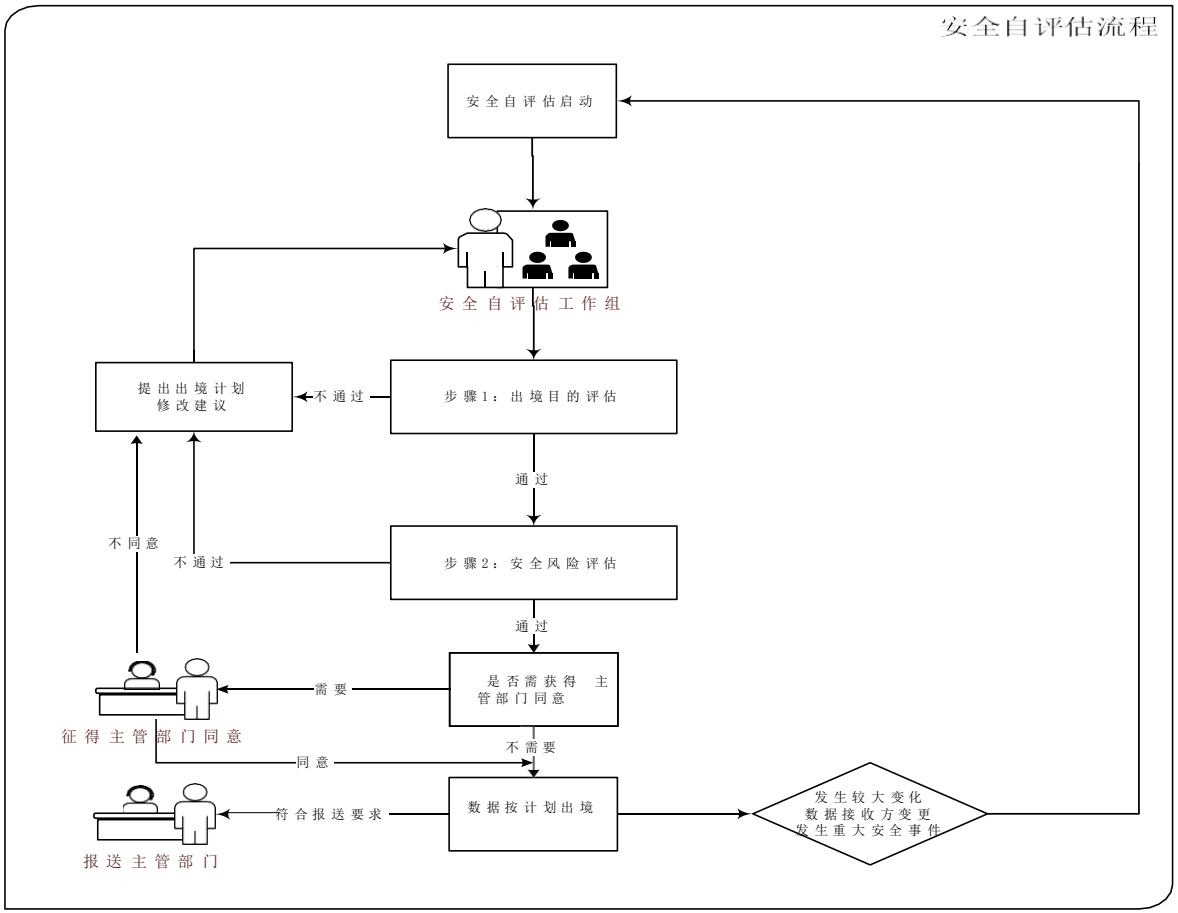
- 个人信息出境合同：主要参考了GDPR中的标准合同条款的思路，即通过对合同权利义务的安排，将网络运营者及境外接收者均纳入规制对象的范围，以弥补个人信息出境后的保护不足。后续会就合同权利义务安排的要点进行分析。EDPB《GDPR标准合同条款》（简称SCC,根据GDPR第28条）

- 安全风险及保障措施分析报告

数据出境的监管审批

安全评估程序

- 网络运营者自行评估：每年至少一次，并应当及时将评估情况报行业主管部门或者监管部门。所有涉及到数据出境的网络运营者，也就是说只要涉及到数据出境的组织都需要进行安全自评估，而不分所处行业、自身规模与业务类型。



数据出境的监管审批

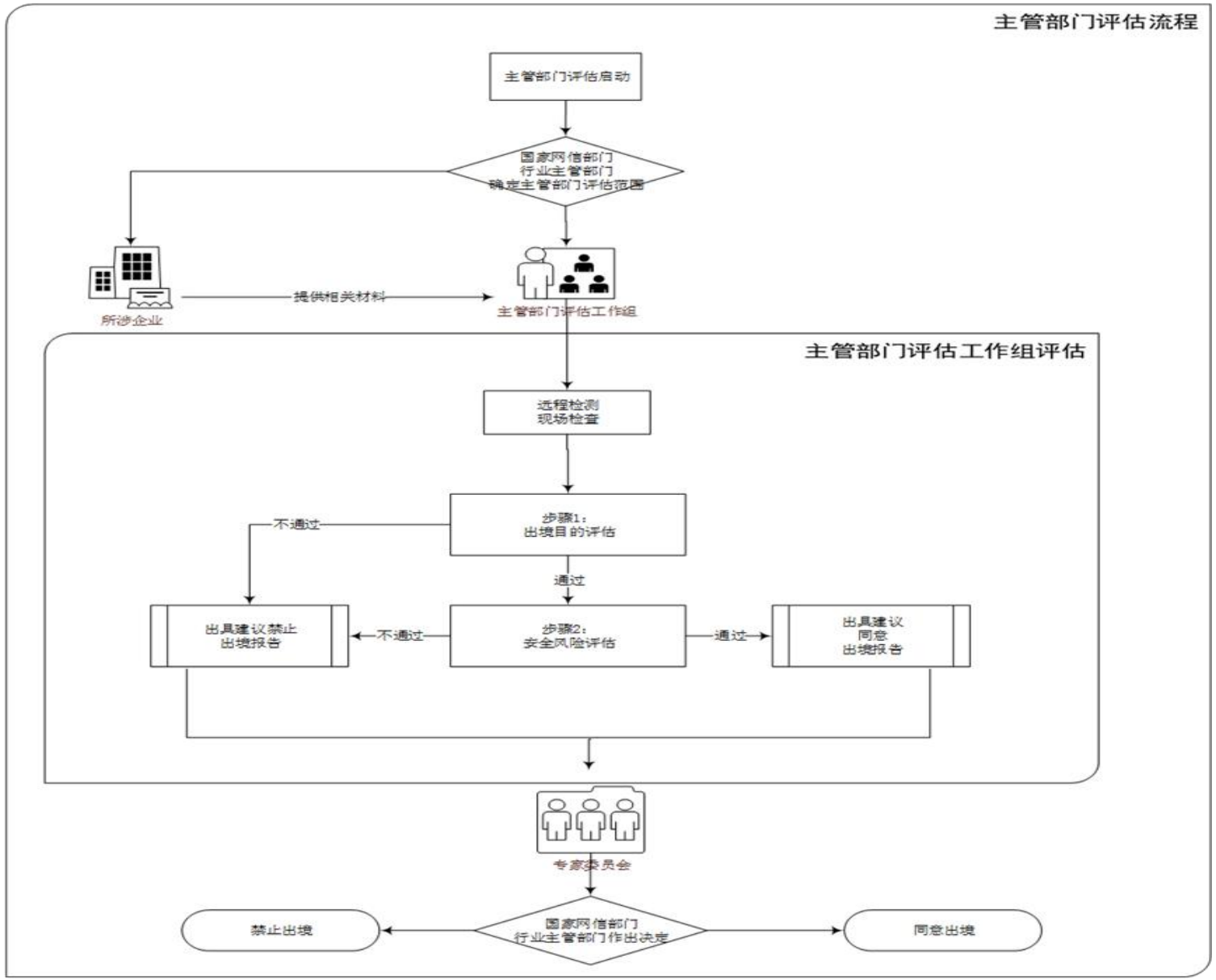
- 监管机构安全评估

《安全评估办法（2017）》第九条: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：

  - 含有或累计含有50万人以上的个人信息；
  - 数据量超过1000GB；
  - 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；
  - 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；
  - 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；
  - 其他可能影响国家安全和社会公共利益，行业主管或监管部门认为应该评估。

- 行业主管或监管部门不明确的，由国家网信部门组织评估。

数据出境的监管审批


主管部门评估流程
主管部门评估启动
国家网信部门
行业主管部门
确定主管部门评估范围
所涉企业
提供相关材料
主管部门评估工作组
主管部门评估工作组评估
远程检测
现场检查
步骤1：
出境目的评估
不通过
通过
出具建议禁止
出境报告
不通过
步骤2：
安全风险评估
通过
出具建议
同意
出境报告
专家委员会
禁止出境
国家网信部门
行业主管部门作出决定
同意出境

数据出境的**监管审批**

- 《安全评估办法（2017）》第十二条： 年度评估和二次评估的内容
- 年度评估要求“根据业务发展和网络运营情况，每年至少进行一次安全评估”
- 二次评估要求“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时，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”。

数据出境的监管审批

- 安全评估内容：出境目的、安全风险
- **出境目的**：数据出境计划中出境目的应同时满足合法性、正当性和必要性的要求：

合法性：

1　不属于法律法规明令禁止的；

2不属于国家网信部门、公安部门、安全部门等有关部门认定不能出境的。 **正当性：**

3个人信息主体已同意的。虽未经个人信息主体同意但是危及公民生命财产 安全等紧急情况除外；

4　不违反相关主管部门规定的。

必要性：

1　履行合同义务所必需的；

2　同一机构、组织内部开展业务所必需的；

3　我国政府部门履行公务所必需的；

4　履行我国政府与其他国家和地区、国际组织签署的条约、协议所必需的；

5其他维护网络空间主权和国家安全、经济发展、社会公共利益和保护公民 合法利益需要的。

数据出境的**监管审批**

- 安全评估内容
- **安全风险**

评估数据出境计划的安全风险，应综合考虑出境数据的属性和数据出境发生安全事件的可能性及影响程度：

数据属性：

1个人信息的属性，包括类型、数量、范围、敏感程度和技术处 理情况等；

2　重要数据的属性，包括类型、数量、范围和技术处理情况等；

3当数据出境同时包含个人信息和重要数据时，应同时满足上述 两条评估要求。

数据出境发生安全事件的可能性及影响程度：1） 发送方数据出境的技术和管理能力；

2　数据接收方的安全保护能力、采取的措施；

3　数据接收方所在国家或区域的政治法律环境。

数据出境的监管审批

安全评估内容

（3）评估内容中的特殊内容

- 网络运营者自行评估

《安全评估办法（2017）》，除了上述内容外，自行评估重点关注了数据出境及在转移后被泄露、毁损、篡改、滥用等风险以及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。

网络运营者自行组织评估的要点与监管部门进行的安全评估程序略有不同，在第十二条要求**网络运营者每年都须对数据出境至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。而由行业主管或监管部门组织的安全评估，应当于**60个工作日内完成，及时向网络运营者反馈情况**并报国家网信部门。

- 个人信息出境安全评估

《安全评估办法（2019）》就个人信息出境安全评估重点做了特别规定：

- 是否符合国家有关法律法规和政策规定；
- 合同条款是否能够充分保障个人信息主体合法权益；
- 合同能否得到有效执行；
- 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；
- 网络运营者获得个人信息是否合法、正当；
- 其他应当评估的内容。

数据出境的监管审批

- 数据出境网络运营者与境外相关主体的义务

相比于重要数据的出境，**个人信息出境**在相关主体义务方面有更加明确的规定：

- 网络运营者：根据《安全评估办法（2019）》，个人信息出境合同应明确规定网络运营者（个人信息发送方）承担以下义务。

告知义务	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。
提供合同副本义务	应个人信息主体的请求，提供本合同的副本。
先行赔付义务	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。

数据出境的监管审批

- 境外数据接收者

合同中的境外接收者义务：根据《安全评估办法（2019）》，个人信息出境合同应明确规定境外接受者承担以下责任和义务，跨国公司的境外母公司在接收中国境内的个人信息时应引起注意。

保障信息主体对其个人信息的访问、更正及删除权利的义务	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；
所在国家和地区法律环境发生重大变化时的报告 义务	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，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，并通过网络运营者报告网络运营者所在地省级网信部门。
个人信息出境合同终止后的义务	除非境外接收者已经销毁了接收到的个人信息或作了匿名化处理，即使个人信息出境合同终止，也不能免除接收者承担涉及个人信息主体合法权益的义务。

数据出境的监管审批

- 对境外机构的域外适用
- 《安全评估办法（2019）》第20条规定，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。一般认为，该条规定意味着《安全评估办法（2019）》可能会适用于不在我国境内但为我国用户提供服务的机构。

数据出境的监管审批

违法数据出境法律责任

- 个人信息未获授权
  - 民事责任：根据《民法典》人格权编关于个人信息保护的规定，个人信息受到侵害时，受害人有权依照《民法典》和其他法律的规定，请求行为人承担停止侵害、排除妨碍、消除危险、消除影响、恢复名誉、赔礼道歉的民事责任。此外，根据《安全评估办法（2019）》，在个人信息出境合同中，个人信息主体是涉及个人信息主体权益的受益人。个人信息主体合法权益受到损害时，可以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。
  - 刑事责任：侵犯公民个人隐私/公民个人信息罪

网络运营者未经用户允许，而将用户个人信息提供给境外人员或者机构，轻则受到民法规范，承担侵犯隐私的民事责任，如赔礼道歉、消除影响以及赔偿损失。如果运营者提供数据出境后还谋取利益，情节严重造成较为严重的社会后果，可能构成侵犯公民个人信息罪，《刑法》第二百五十三条规定了“侵犯公民个人信息罪”，具体包括“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的”。

数据出境的监管审批

- 重要数据未获批准
  - 行政处罚
  - 网络运营者未经国家相关部门批准擅自将数据信息提供给境外机构组织的，将受到行政处罚。根据《网络安全法》第六十六条：关键信息基础设施的运营者违法在境外存储网络数据，或者向境外提供网络数据的，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。

数据出境的监管审批

- 危害国家安全类犯罪

网络运营者若未经国家相关部门批准擅自将重要信息提供给境外机构、组织，可能构成我国《刑法》分则第一章中危害国家安全类的犯罪，如第一百一十一条“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”。

- 拒不履行信息网络安全管理义务罪

《刑法修正案（九）》已针对网络服务提供者专门增设了一个罪名，即拒不履行信息网络安全管理义务罪。作为网络服务提供者的企业，若不依法履行相关的信息网络安全管理义务，企业本身及相关负责人员就可能因消极的不作为而承担刑事责任。《刑法》第二百八十六条之一规定：“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：（一）致使违法信息大量传播的；（二）致使用户信息泄露，造成严重后果的；（三）致使刑事案件证据灭失，情节严重的；（四）有其他严重情节的。

数据出境的**监管审批**

数据出境合规安排建议

1. 建立境内数据中心

企业进行个人信息或数据出境均需报请安全评估，无论是选择安全自评估还是主管部门评估，都应尽早建立数据出境的内控政策以及出境安全的评估机制。从长远来看，搭建系统的数据保护和管理体系，建立符合企业发展需要的独立数据评估机制是网络运营者们的必由之路。对于出境并非唯一选择项的业务场景，可以考虑本地化收集、本地化存储的解决方案，尽可能在中国建立地区数据中心,在中国处理源自于中国的个人信息和数据，可以极大减少成本和风险。

数据出境的**监管审批**

数据出境合规安排建议

2、积极应对出境安全评估，开展个人信息和重要数据出境自查

- 如果出于商业或技术上的原因, 信息和数据必须出境的, 企业可以根据上述规定的要求, 自我评估是否满足信息出境的安全要求。
- 以个人信息出境为例，《安全评估办法（2019）》规定网络运营者申报个人信息出境安全评估时，需要向网信部门提交个人信息出境安全风险及安全保障措施分析报告，该报告应包含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。
  - **信息数据资产尽职调查**
  - **梳理企业数据资产**
  - **对企业信息处理行为是否合规、网络安全能力及安全保障措施、数据出境计划等开展内部自查**
  - **制作自查报告或数据出境评估报告。**

数据出境的监管审批

主要流程	相应工作内容
设立自评估工作组	工作组主要包含法务、政策、安全、技术、管理相关专业人员。可以根据需要，邀请外部专家和律师加入工作组。
制定数据出境计划	计划的内容包括但不限于： a) 涉及个人信息情况，包括个人信息的类型、数量、范围和敏感程度等； b) 涉及的信息系统情况； c) 个人信息发送方的安全保护能力； d) 个人信息境外接收者的安全保护能力及其所在的国家或地区的法律基本情况； e) 出境持续时间、个人信息出境后是否会再向第三方传输等。
安全自评估要点及方法	评估要点：包括获得个人信息是否合法、正当；出境计划的安全风险；个人信息发送方的安全保护能力；个人信息接收者的安全保护能力；个人信息接收者所在国家或区域的法律环境等。 评估方法：首先，评估个人信息出境对个人权益的影响等级，并根据信息发送方和境外接收者安全保障能力、以及接收者所在地法律，判定安全事件可能性等级；其次，从个人权益受影响程度及安全事件可能性两个层面开展安全风险综合评估综合评价，按照“极高”、“高”、“中”和“低”四个等级对整体安全风险进行评估。
形成安全自评估报告	网络运营者在完成数据出境安全自评估后，应形成安全自评估报告。安全自评估报告内容应包括但不限于：安全自评估对象基本情况、安全自评估组织实施情况、安全自评估结果、数据出境安全风险点、检查修正建议。

数据出境的监管审批

数据出境合规安排建议

2、积极应对出境安全评估，开展个人信息和重要数据出境自查

仔细审核关于信息出境的合同, 确保以尽可能符合《合同法》的方式具备《安全评估办法（2019）》所要求的必备条款，一方面提高自身的出境合规标准，另一方面避免在接收者违反合同约定、侵害个人信息主体权利时由企业承担过重的先行赔付责任。

数据出境的监管审批

- 数据出境合规安排建议

3、实施数据筛查，对涉及个人信息和重要数据的出境文件进行特殊加工

- 向境外政府部门、母公司、司法机构、客户公司等提供包含个人信息的文件资料。对此，跨国公司应持保守、谨慎的态度，在个人信息出境前，通过获取外部专家的协助对相关文件进行筛查，
- 如果经筛查发现相关资料涉及个人信息，一般应通过特殊加工（Redaction）等措施进行排除，防止这些信息被传输至境外带来不必要的风险。

数据出境的监管审批

- 数据出境合规安排建议

4、与监管部门进行紧密沟通和配合

评估监管机构的设定机制为各自行业监管，而非统一机构，在评估中可能容易造成尺度不一等对企业不利的情况发生。且就目前阶段而言，行业监管机构在数据评估上缺乏相关经验，因此，对于适用法定机构评估情形的企业在发生跨境数据或信息传输前，需要与对应监管机构进行紧密的沟通和配合，对可能的数据出境行为先行报备，以减少数据传输的合规成本和风险。

谢谢大家！

冯超

Charles_feng@east-concord.com; fchao7847@Hotmail.com

+86 13910336970

天达共和律师事务所 合伙人 律师

北京市朝阳区东三环北路8号亮马河大厦写字楼1座20层 邮编100004