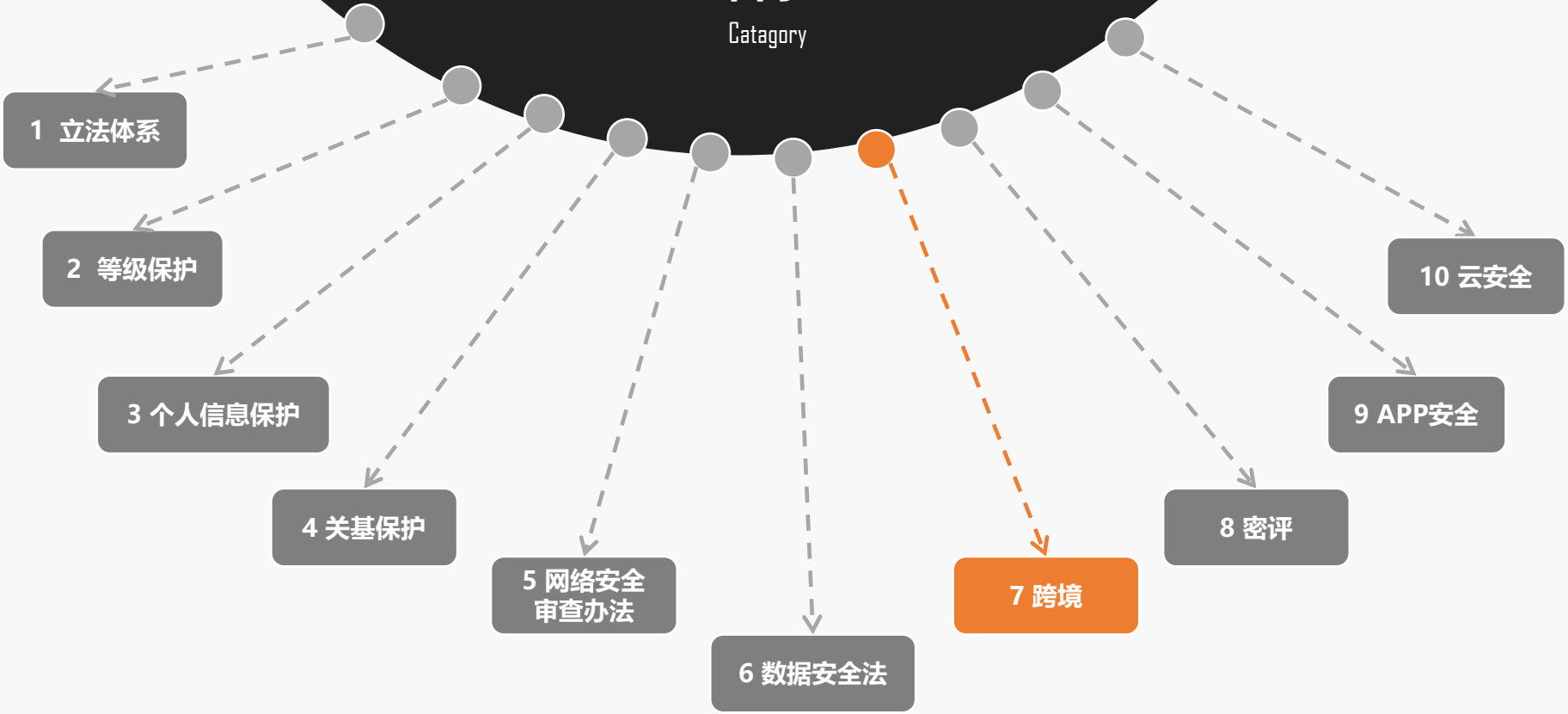
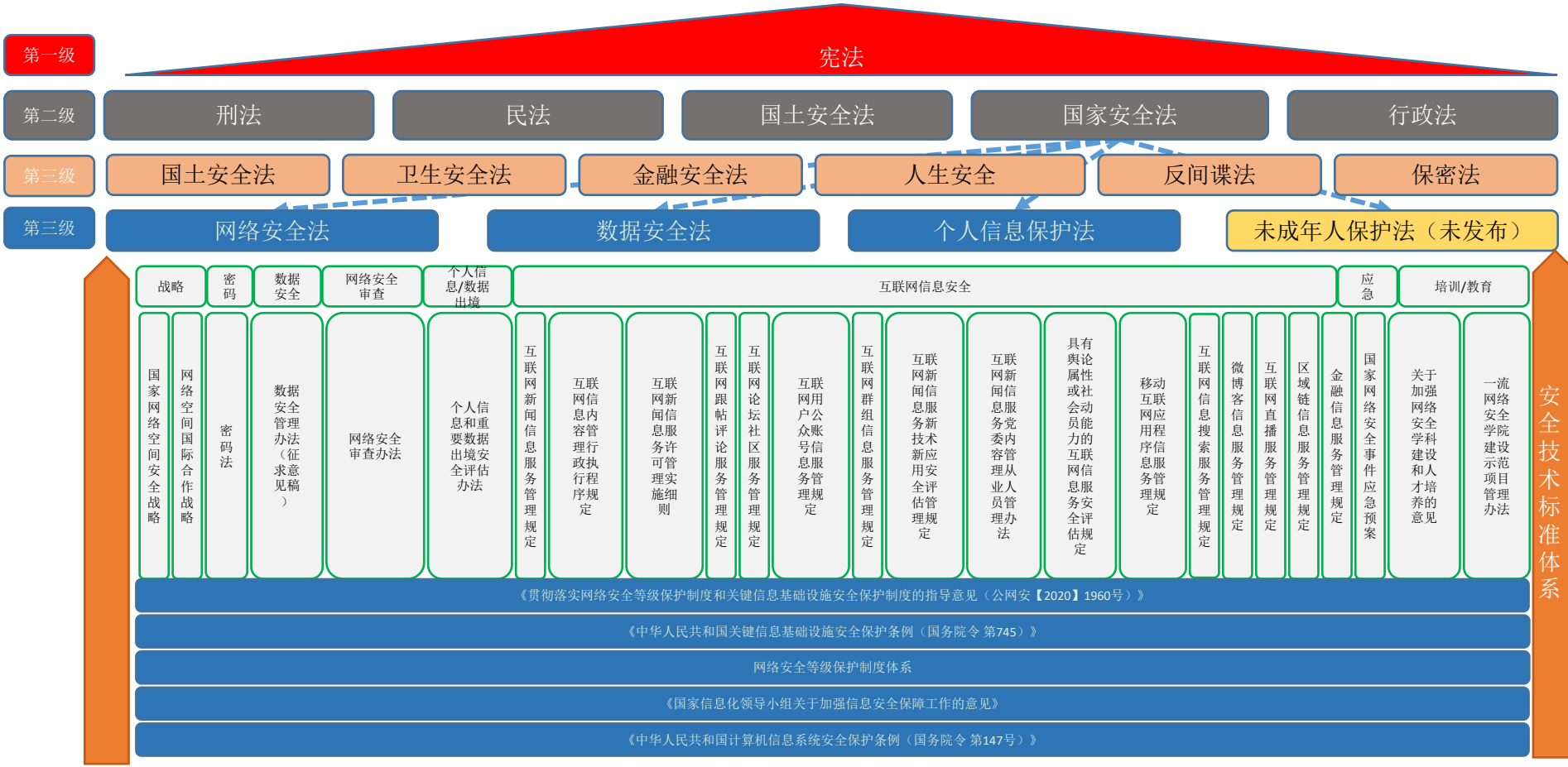
信息安全法律法规相关

目录

Catagory


1 立法体系
2 等级保护
3 个人信息保护
4 关基保护
5 网络安全
审查办法
6 数据安全法
7 跨境
8 密评
9 APP安全
10 云安全

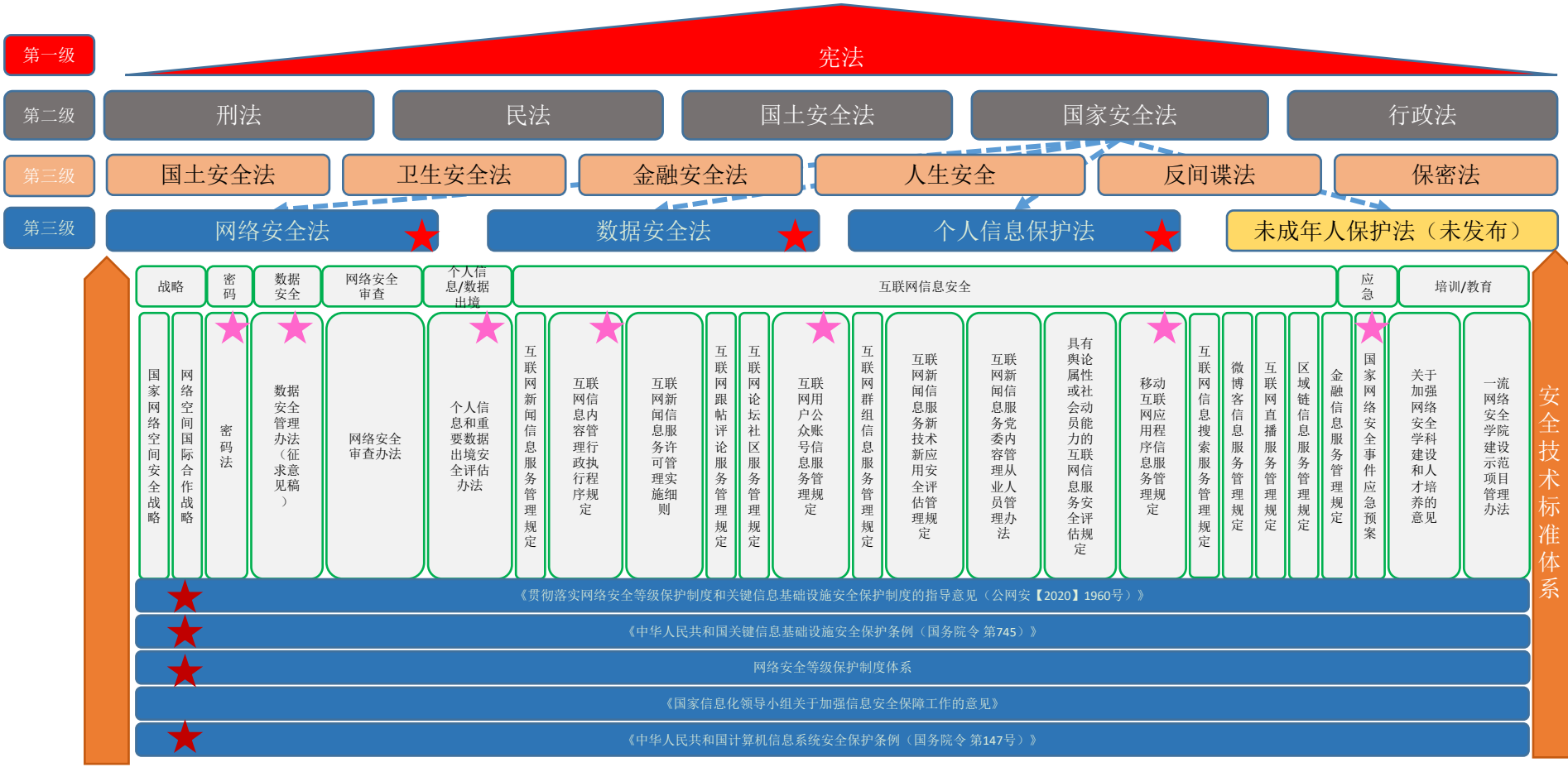
1 立法体系—全貌


第一级
宪法
第二级
刑法
民法
国土安全法
国家安全法
行政法
第三级
国土安全法
卫生安全法
金融安全法
人生安全
反间谍法
保密法
第三级
网络安全法
数据安全法
个人信息保护法
未成年人保护法（未发布）
战略
密码
数据安全
网络安全审查
个人信息/数据出境
互联网信息安全
应急
培训/教育
国家网络空间安全战略
网络空间国际合作战略
密码法
数据安全管理办法（征求意见稿）
网络安全审查办法
个人信息和重要数据出境安全评估办法
互联网新闻信息服务管理规定
互联网信息内容管理行政执行程序规定
互联网新闻信息服务许可管理实施细则
互联网跟帖评论服务管理规定
互联网论坛社区服务管理规定
互联网用户公账号信息服务管理规定
互联网群组信息服务管理规定
互联网新闻信息服务新技术新应用安全评估管理规定
互联网新闻信息服务党内管理从业人员管理办法
具有舆论属性或社会动能力的互联网信息服务安全评估规定
移动互联网应用程序信息服务管理规定
互联网信息搜索服务管理规定
微博客信息服务管理规定
互联网直播服务管理规定
区域链信息服务管理规定
金融信息服务管理规定
国家网络安全事件应急预案
关于加强网络安全学科建设和人才培养的意见
一流网络安全学院建设示范项目管理办法
《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见（公网安【2020】1960号）》
《中华人民共和国关键信息基础设施安全保护条例（国务院令 第745）》
网络安全等级保护制度体系
《国家信息化领导小组关于加强信息安全保障工作的意见》
《中华人民共和国计算机信息系统安全保护条例（国务院令 第147号）》
安全技术标准体系

1 立法体系—重要法规

领域	法律	关注内容
应用层	《密码法》	商用密码管理
	《互联网信息服务算法推荐管理规定》	互联网信息业务、互联网服务的安全算法、数据保护、信息保护
	《网络安全审查办法》	网络安全运营、网络安全审查、安全事件管理、应急响应、自查、自报告等
内容层	《网络安全法》	网络信息内容安全等
	《互联网信息服务管理办法》	互联网信息服务
数据层	《数据安全法》	数据安全、重要数据保护
	《个人信息保护法》	个人信息搜集、使用、保护
	《重要数据跨境评估管理办法》	重要数据、个人信息跨境评估+保护
基础设施层	《网络安全法》	开展网络安全等级测评、认证、实施保护
	《关键信息基础设施安全保护条例》	关键基础设施行业、企业、组织的安全保护
	《电信条例》	通讯、通信领域的网络安全保护，以传输保护为主

1 立法体系—我司相关


第一级
宪法
第二级
刑法
民法
国土安全法
国家安全法
行政法
第三级
国土安全法
卫生安全法
金融安全法
人生安全
反间谍法
保密法
第三级
网络安全法
数据安全法
个人信息保护法
未成年人保护法（未发布）
战略
密码
数据安全
网络安全审查
个人信息/数据出境
互联网信息安全
应急
培训/教育
国家网络空间安全战略
网络空间国际合作战略
密码法
数据安全管理办法（征求意见稿）
网络安全审查办法
个人信息和重要数据出境安全评估办法
互联网新闻信息服务管理规定
互联网信息内容管理行政执行程序规定
互联网新闻信息服务许可管理实施细则
互联网跟帖评论服务管理规定
互联网论坛社区服务管理规定
互联网用户公账号信息服务管理规定
互联网群组信息服务管理规定
互联网新闻信息服务新技术新应用安全评估管理规定
互联网新闻信息服务党内管理从业人员办法
具有舆论属性或社会动能力的互联网信息服务安全评估规定
移动互联网应用程序信息服务管理规定
互联网信息搜索服务管理规定
微博客信息服务管理规定
互联网直播服务管理规定
区域链信息服务管理规定
金融信息服务管理规定
国家网络安全事件应急预案
关于加强网络安全学科设人才培养的意见
一流网络安全学院建设示范项目管理办
《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见（公网安【2020】1960号）》
《中华人民共和国关键信息基础设施安全保护条例（国务院令 第745）》
网络安全等级保护制度体系
《国家信息化领导小组关于加强信息安全保障工作的意见》
《中华人民共和国计算机信息系统安全保护条例（国务院令 第147号）》
安全技术标准体系

2 我司性质

企业维度	数据维度	个人信息保护	跨境场景
涉密企业如党政军	关键基础设施数据	普通个人信息	境内
大型企业如互联网公司	重要数据	敏感信息	境外
大型企业如上市公司	一般数据	隐私信息	第三方
一般企业		其它信息	

说明：

1 、互联网公司、上市公司，根据数据性质+数量，确定是否属于关键基础设施

2、跨境的第三方，主要是指未与中国建立外交、互信关系的国家（组织），以及无国籍人士、国籍人士----这一类是属于不可达、不可信、不可交流的范围，应该处于禁止范畴

说明：

1、 我司属于上市公司

2、我司不属于关键基础设施行业

3、我司在网络安全、数据安全、个人信息保护、跨境保护、合规遵循方面，比其它企业、普通企业更高

3 各领域重点TOP5

企业	数据	个人信息保护	跨境
• 大型企业如上市公司	• 关键基础设施数据 • 重要数据	• 敏感信息 • 隐私信息	• 境内

企业	数据	个人信息保护	跨境
1、不得接触无关客户、用户	1、开展数据安全法评估	1、开展个人信息评估	1、关键基础设施数据不得处境
2 、开展等级保护工作	2、开展数据安全自评、自整改	2、开展个人信息保护自评、自整改	2、建立关基数据跨境评估、审核、审批机制
3、开展关键基础设施评估	3、建立动态、常态数据监控、运营体系	3、建立动态、常态数据监控、运营体系	3、建立重要数据跨境评估、审核机制
4、开展涉密企业安全保护	4、配合各行业开展数据分级分类	4、建立个人信息保护运营机制	4、建立个人信息跨境评估、审核机制
5、建立有效安全运营机制	5、建立数据安全运营机制	5、建立成熟、可靠的个人信息保护能力和技术体系	5、建立成熟、可靠的网络保护能力和技术体系

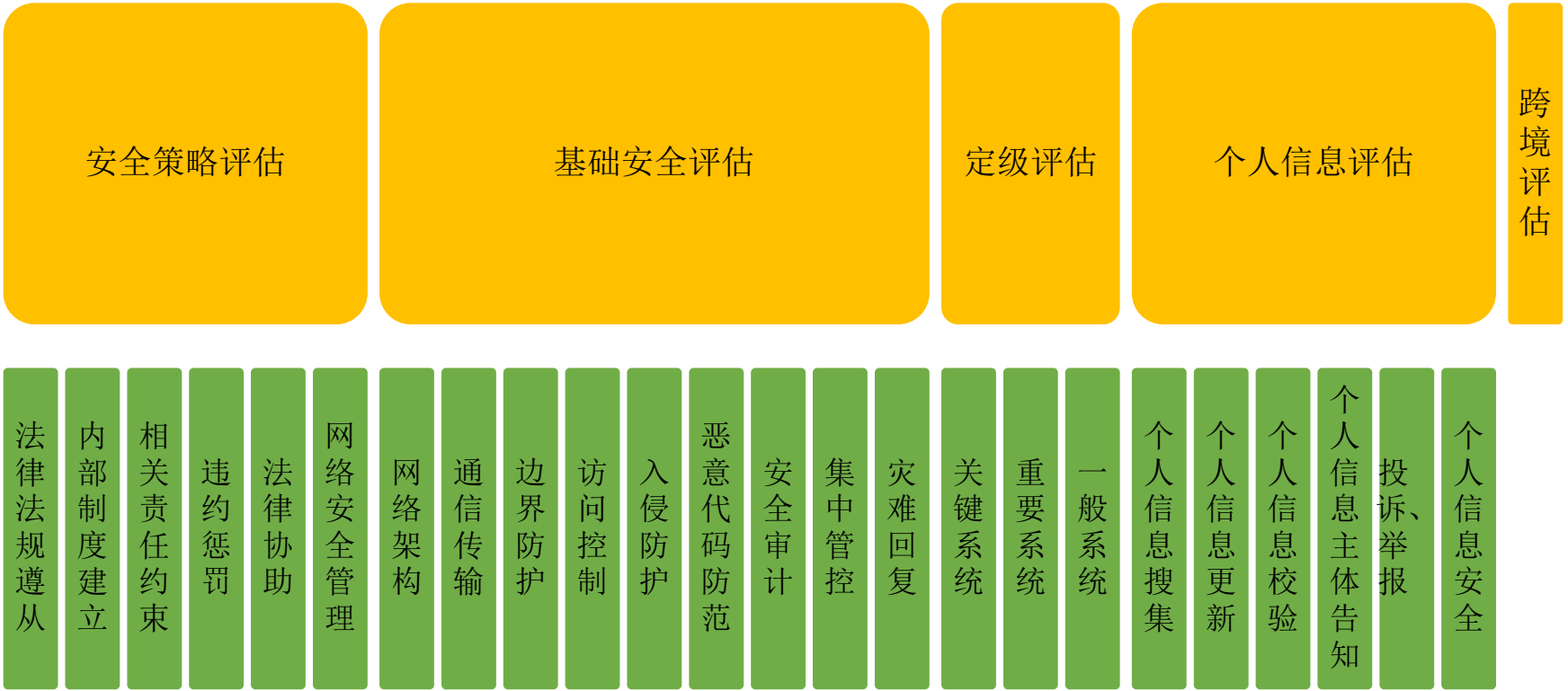
其它工作包括:

- ✓ 1、 配备专业专职安全组织 + 专职安全人员
- ✓ 2、根据各领域要求，建立对应的管理制度和流程、管理办法
- ✓ 3、建立成熟、可靠、高效的技术团队和管理团队
- ✓ 4、建立动态、常态化运营体系
- ✓ 5、建立可靠、高效、有效的合规体系+ 服务支持体系
- ✓ 6、建立有效、高效的上报、审核、审批、报告机制

跨境评估全貌

跨境数据评估方法					
评估领域	评估目标	评估内容	结果		
数据发送方	中国的数据中心	发件人对安全能力的评估。 发件人数据退出的技术保证能力。	允许跨境	整改后允许跨界	不允许跨境
数据接收方	国外的数据中心	实体资格 接收者对安全能力的评估。 接收方数据出口的技术保证能力。 该国的政治和法律环境评估。			
App	应用系统和项目	APP跨境技术保证能力			

跨境评估-1 范围


跨境评估
安全策略评估
基础安全评估
定级评估
个人信息评估
法律法规遵从
内部制度建立
相关责任约束
违约惩罚
法律协助
网络安全管理
网络架构
通信传输
边界防护
访问控制
入侵防护
恶意代码防范
安全审计
集中管控
灾难回复
关键系统
重要系统
一般系统
个人信息搜集
个人信息更新
个人信息校验
个人信息主体告知
投诉、举报
个人信息安全

跨境评估-双方

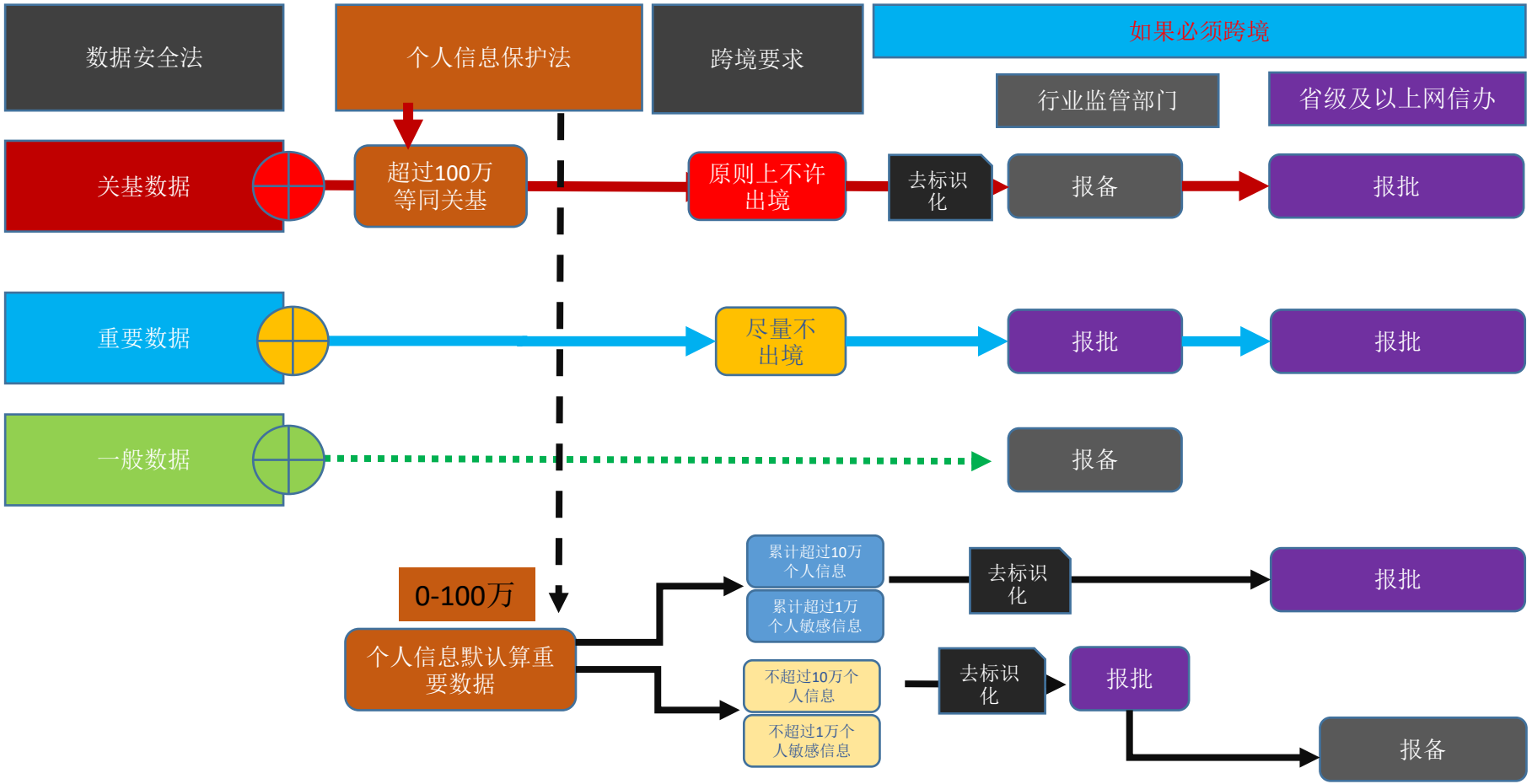
跨境评估-发送方

- 管理制度保障能力
  - 安全管理制度
  - 人员管理
  - 合同约束审查
  - 审计机制
  - 应急处置
  - 申诉管理
- 技术手段保障能力
  - 安全技术能力

跨境评估-接收方

- 主体资格
  - 资质资格
  - 业务范围
  - 违法记录
  - 背景关系
- 管理制度保障能力
  - 管理制度保障能力
  - 人员管理
  - 审计机制
  - 应急处置
  - 政治法律环境 for PII
  - 涉及重要数据的政治法律环境
- 技术手段保障能力
  - 安全技术能力

7 跨境-整体框架


数据安全法
个人信息保护法
跨境要求
如果必须跨境
行业监管部门
省级及以上网信办
关基数据
超过100万
等同关基
原则上不许
出境
去标识
化
报备
报批
重要数据
尽量不
出境
报批
报批
一般数据
报备
0-100万
个人信息默认算重
要数据
累计超过10万
个人信息
累计超过1万
个人敏感信息
去标识
化
报批
不超过10万个
人信息
不超过1万个
人敏感信息
去标识
化
报批
报备

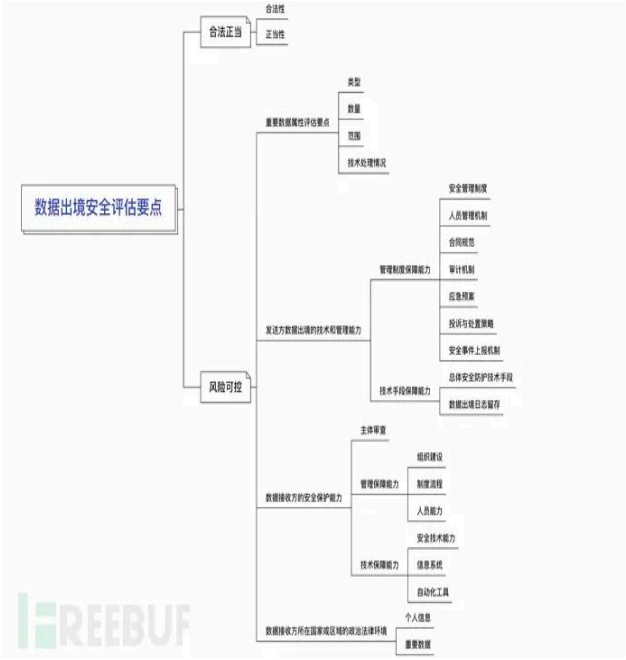
7 跨境- 流程

1、成立安全自评估工作组，制定数据出境计划
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；
涉及重要数据情况，包括重要数据的类型、数量和范围等；
涉及的信息系统情况；
数据发送方安全保护能力；
数据接收方安全保护能力及其所在的国家或地区的基本情况。

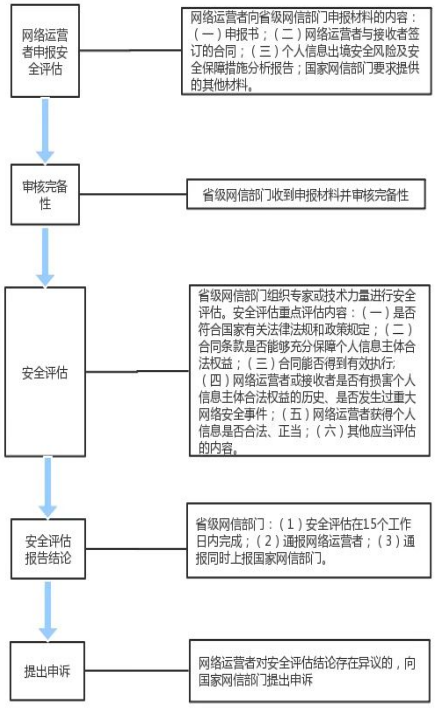
2、评估数据出境计划的合法性和正当性

3、形成评估报告，进行相应调整
安全自评估报告应至少保存2年，并在如下情况下将安全自评估报告上报行业主管部门，行业主管部门不明确的，报国家网信部门。
关键信息基础设施运营者开展的安全自评估；
一年内出境的个人信息数量达到国家网信部门、行业主管部门上报要求的；
包含核设施、生物化学、国防军工、人口健康等领域数据，大型工程活动、海洋环境敏感地理信息数据，以及其他重要数据的；
涉及关键信息基础设施的安全缺陷、具体安全防护措施等网络安全信息的；
其他可能影响国家安全、经济发展和社会公共利益的。

重要数据跨境评估



个人信息跨境评估



0—重点解读

方向	内容	对应关系	备注
数据出境管理	国家建立重要数据出境网关，全方面管理控制	跨境	其它渠道如翻墙 代理 自建vpn 自建网关 可能违法
信息上报	重要数据或者10万个人信息泄露损毁丢失 8小时内上报 市级网信办和监管部门	数据安全管理 个人信息保护 事件管理+应急响应	
事件处置上报	事件处置完毕后五个工作日内向设区的市级网信部门和 有关主管部门报送调查评估报告	事件管理+应急响应	
个人权利（明示同意、单独同意）	个人同意记录及个人信息提供记录保存5年	个人信息知情权、同意权、拒绝权	建议单独保存
特殊敏感个人信息	需要单独同意	敏感个人信息	建议单独使用、单独存储、单独处置 日志也单独存储
重要数据跨境备案	重要数据如有跨境需求需在15日内备案	重要数据跨境	建议单独设置重要数据跨境通道 跨境日志保存不少于2年
安全评估报告	每年1月31日前提交上一年度数据安全评估报告	数据安全管理	报告本身要留存3年
数据跨境报告	每年1月31日前提交数据出境安全报告	重要数据跨境 个人信息跨境	重点是1）哪些数据出去了2）给了谁3）对方从管理、技术上是否满足要求 4）对方能否提供相应的证据、报告 5）违规处置意见和结果等 6）下一年度建议（延续、整改、更换、终止等）

7 —跨境要求

	要求
个人信息出境通用规则	采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准
	通过国家网信部门组织的安全评估
	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
	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
	取得个人的单独同意
	事前进行个人信息保护影响评估
	经中华人民共和国主管机关批准，才可向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息

3—个人信息跨境

分类	类型	跨境要求		如果必须出境	
		默认能不能出境	出境数量限制	行业监管部门	省级及以上网信办
C1	CII行业数据	原则上不可以	无限制，1个也算	N/A	审批
C2	CII 行业特殊人群个人信息	原则上不可以	无限制，1个也算	N/A	审批
C3	CII 行业普通人员个人信息	可以	10万以上	N/A	审批
C4	CII 行业个人敏感信息	可以	1万以上	N/A	审批
B1	行业特殊的重要数据	原则上不可以	无限制，1个也算	审批	审批
B2	行业特殊、重要人员信息	原则上不可以	无限制，1个也算	审批	审批
B3	行业普通重要数据	可以	各行业定义	审批	审批
B4	行业普通人员个人信息	可以	10万以上	报备	审批
B5	行业人员个人敏感信息	可以	1万以上	报备	审批
所有行业	处理个人信息数量超过100万	可以，必须进行网络安全审查	没明说，潜台词是出境一条也算	审批	审批
	处理个人信息数量10万到100万	可以，建议进行网络安全审查	10万-100万	审批	审批
	普通个人信息	可以	10万以下	审批	报备
	个人敏感信息	可以	1万以下	审批	报备

1 适用对象、范围

在中华人民共和国境内利用网络开展数据处理活动，以及网络数据安全的监督管理

- 包括
  - 国内企业
  - 外企
  - 合资公司
  - 各类组织
  - 各类社会性组织
- 不包括（此类组织、人员不受中国法律保护）
  - 非认可组织
  - 无国籍人士
  - 多国籍人士
  - 被国家认定的特殊机关
  - 特殊部门
  - 其它认定的组织
- 说明
  - 港澳台算境外
  - 港澳台单独制定法律法规

包括

- ◆ 以向境内提供产品或者服务为目的
- ◆ 分析、评估境内个人、组织的行为
- ◆ 涉及境内重要数据处理
- ◆ 法律、行政法规规定的其他情形

不包括

- ■ 个人事务
- ■ 家庭事务
- ■ 特殊部门、机关、组织
- ■ 军事

2 目标 & 方式

目标

包括

- 促进数据开发利用
- 保障数据安全
- 加强数据安全防护能力建设
- 保障数据依法有序流动
- 促进数据已发合理有效利用

方式

包括

- 国家建立数据分级分类制度（一般数据、重要数据、核心数据）

  ---核心数据对应CII 和 部分特殊重要数据

  - 个人信息+重要数据 开展重点保护
  - 核心数据（CII） 开展严格保护
- 国家机关、行业组织、企业、教育科研机构、专业机构合作，既利用数据、又保护数据
- 行业、地区、各部门 分别管理自己的领域
- 国家建立健全数据交易管理制度
  - 个人交易可能违法
  - 组织交易可能违法

6 跨境判断-国内企业

跨境场景下，存留相关日志记录和数据出境审批记录三年以上

发起主体	接收主体	发起主体控股权	接收方控股权	接收人	算不算跨境	说明
国内企业	国内企业	100%中国股份或者绝对控股地位	100%中国股份或者绝对控股地位	境内自然人	不算	
				境外人士	算	
			非绝对中方控股地位		部分算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境
		非绝对控股地位	Any		都算	如DD
	海外分公司	100%中国股份或者绝对控股地位	100%中国股份或者绝对控股地位	境内自然人	不算	即使人在境外，也算境内人士
				境外人士	算	
			非绝对中方控股地位	Any	部分算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境
		非绝对中方控股地位	Any	Any	都算	
	海外公司（外资）	any	any		算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境（信息没用于其它用途）
	第四方（非建交、非授信、无国籍、多国籍人员）	Any	Any	Any	违规	
	第四方（国际组织如红十字会、联合国教科文组织、医疗组织等）	Any	Any	Any	区别对待、特审、特批	

6.2 跨境判断-外资企业

跨境场景下，存留相关日志记录和数据出境审批记录三年以上

发起主体	接收主体	发起主体控股权	接收方控股权	接收人	算不算跨境	说明
外资	国内企业(含合资公司)	非绝对中方控股地位	100%中国股份或者绝对控股地位	境内自然人	不算	
				境外人士	算	
			非绝对中方控股地位	Any	算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境
	海外分公司	非绝对中方控股地位	非绝对中方控股地位	Any	部分算	
			非绝对中方控股地位	Any	部分算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境
	海外公司（总部）	any	any	Any	算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境（信息没用于其它用途）
	第四方（非建交、非授信、无国籍、多国籍人员）	Any	Any	Any	违规	
	第四方（国际组织如红十字会、联合国教科文组织、医疗组织等）	Any	Any	Any	区别对待、特审、特批	

6.3 跨境判断-合资企业

跨境场景下，存留相关日志记录和数据出境审批记录三年以上

发起主体	接收主体	发起主体控股权	接收方控股权	接收人	算不算跨境	说明
合资	国内企业(含合资公司)	非绝对中方控股地位	100%中国股份或者绝对控股地位	境内自然人	不算	
				境外人士	算	
			非绝对中方控股地位	Any	算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境
	海外分公司	非绝对中方控股地位	非绝对中方控股地位	Any	部分算	
			非绝对中方控股地位	Any	部分算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境
	海外公司（第三方合作伙伴，或控股股东方）	Any	Any	Any	算	需要注意甄别其中的细分场景，个别人员的行为，不一定算跨境（信息没用于其它用途）
	第四方（非建交、非授信、无国籍、多国籍人员）	Any	Any	Any	违规	
	第四方（国际组织如红十字会、联合国教科文组织、医疗组织等）	Any	Any	Any	区别对待、特审、特批	

其它重点

信息搜集：

- ✓ 按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意、更不得强制同意
- ✓ 处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意
- ✓ 搜集未成年人信息需征得监护人同意

生物信息：

数据处理者利用生物特征进行个人身份认证的，应当对必要性、安全性进行风险评估，不得将人脸、步态、指纹、虹膜、声纹等生物特征作为唯一的个人身份认证方式，以强制个人同意收集其个人生物特征信息

向境外提供个人信息：

数据处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的**单独同意**

大型互联网平台（日活1亿以上）

- ➢ 隐私政策需得到省级及以上网信部门、电信主管部门同意
- ➢ 第三方产品和服务，一起负责，并签署合同约定安全责任和义务
- ➢ 第三方风险，互联网平台先行赔付
- ➢ 定期进行安全审核、披露审核规则
- ➢ 优先使用国家网络身份认证公共服务基础设施（国家监管和控制）
- ➢ 委托第三方审计，披露审计结果

国家层面： 1 、建立数据跨境网关 2 建立安全审计制度

解读： 1、VPN/mpls vpn ,代理、翻墙、托管都可能违规 2、国家审计，无权拒绝

向第三方提供个人信息：

数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规定：

1. 向个人告知提供个人信息的目的、类型、方式、范围、存储期限、存储地点，并取得个人单独同意，符合法律、行政法规规定的不需要取得个人同意的情形或者经过匿名化处理的除外
2. 与数据接收方约定处理数据的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全责任义务，并对数据接收方的数据处理活动进行监督
3. 留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。

向境外提供重要数据：

（一）不得超出报送网信部门的个人信息保护影响评估报告中明确的目的、范围、方式和数据类型、规模等向境外提供个人信息；
（二）不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供个人信息和重要数据；
（三）采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式使用数据，履行数据安全保护义务，保证数据安全；
（四）接受和处理数据出境所涉及的用户投诉；
（五）数据出境对个人、组织合法权益或者公共利益造成损害的，数据处理者应当依法承担责任；
（六）存留相关日志记录和数据出境审批记录三年以上；
（七）国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示；
（八）国家网信部门认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救

其它细节

日常运营管理

提交年度数据安全评估报告 事中： 整体情况，不仅仅是跨境

A: 处理重要数据的 B: 赴境外上市的 C: 处理个人信息超过100万的

要求：每年1月31日前上报市级网信部门，报告内容包括

（一）处理重要数据的情况；

（二）发现的数据安全风险及处置措施；

（三）数据安全管理制度，数据备份、加密、访问控制等安全防护措施，以及管理制度实施情况和防护措施的有效性；

（四）落实国家数据安全法律、行政法规和标准情况；

（五）发生的数据安全事件及其处置情况；

（六）共享、交易、委托处理、向境外提供重要数据的安全评估情况；

（七）数据安全相关的投诉及处理情况；

（八）国家网信部门和主管、监管部门明确的其他数据安全情况。

数据处理者应当保留风险评估报告至少三年。

跨境前评估、申报、审批

重要数据跨境评估报告内容包括（事前：**申报、申请用**）

（一）共享、交易、委托处理、向境外提供数据，以及数据接收方处理数据的目的、方式、范围等是否合法、正当、必要；

（二）共享、交易、委托处理、向境外提供数据被泄露、毁损、篡改、滥用的风险，以及对国家安全、经济发展、公共利益带来的风险；

（三）数据接收方的诚信状况、守法情况、境外政府机构合作关系、是否被中国政府制裁等背景情况，承诺承担的责任以及履行责任的能力等是否能够有效保障数据安全；

（四）与数据接收方订立的相关合同中关于数据安全的要求能否有效约束数据接收方履行数据安全保护义务；

（五）在数据处理过程中的管理和技术措施等是否能够防范数据泄露、毁损等风险。

评估认为可能危害国家安全、经济发展和公共利益，数据处理者不得共享、交易、委托处理、向境外提供数据。

跨境后检查、定责、审查

数据出境安全报告（已发生的、事后）

每年1月31日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况：

（一）全部数据接收方名称、联系方式；

（二）出境数据的类型、数量及目的；

（三）数据在境外的存放地点、存储期限、使用范围和方式；

（四）涉及向境外提供数据的用户投诉及处理情况；

（五）发生的数据安全事件及其处置情况；

（六）数据出境后再转移的情况；

（七）国家网信部门明确向境外提供数据需要报告的其他事项。

常见个人信息去标识化方法

统计	数据聚合：只提供统计信息，无法定位个人 统计抽样：提取部分数据，无法确定真实个体	
假名	假名创建、假名密码化，如真名张三， 在系统里、数据库存储的是james/A1B1 这类无法直接获取个人信息	
合成	叠加一定的特征数据或校验信息，算法不可逆	如姓名张三，合成为张AB等，李四变成李EF
加密	通过加密算法，保证个人信息不可还原，不可解密，算法不可逆	
泛化	通过算法，对数据进行泛华处理，如取整，截零、范围约定等	如薪资，在10-15万元， 不能明确说出是12.22
匿名	通过屏蔽改变共性参数或数据类型，添加印记等方式进行处理	如年龄为25， 实际显示30（+5），或者显示为25-29（+0~4）
抑制	通过屏蔽部分信息，或局部抑制、或记录抑制，避免定位到个人	如手机号码为1335050XXXX，133****5050
随机	通过噪声添加、置换、微聚集等技术，改变数据内容	如手机号码为13350501234，133ABCD505*
差分	通过设置范围段，或统计类信息，屏蔽直观个人信息	

企业应该怎么做

- ✓ 明确专门的数据安全负责人和管理机构
- ✓ 部署数据安全管理类系统，开展数据保护和个人信息自评估、自整改，以及开展重要数据、个人信息跨境安全评估
- ✓ 建立数据安全相关重大决策、数据安全事件应急响应、数据安全风险监测、数据安全风险和事件处置、数据安全风险评估，提升数据安全管理能力
- ✓ 建立应急处置机制，建立应急预案，并按照数据安全事件、数据泄露风险和网络安全事件等三类事件及其严重程度，制定相应的应急处置要求
- ✓ 定期开展风险评估，并向有关主管部门报送风险评估报告
- ✓ 设置个人信息权益维护投诉渠道、建立处理机制
- ✓ 借助外部机构，开展数据安全、个人信息保护、跨境方面的安全评估（每年至少1次）
- ✓ 尽量避免把总部 、研发中心、研发中心、运营中心放在境外