QCon
全球软件开发大会

全球视野下的合规之道
携程海外数据安全管理实践

演讲人：胡立平

携程集团 / 数据安全合规负责人

公司介绍

携程集团（Trip.com Group）是全球领先的一站式旅行平台，公司旗下的平台，包括携程旅行、Trip.com、去哪儿、天巡等，可面向全球用户提供一套完整的旅行产品、服务及差异化的旅行内容。携程于2003年在美国纳斯达克交易所上市，并于2021年在香港联合交易所上市。携程集团力争于3-5年内成为亚洲最领先的在线旅行平台，以及全球最领先的在线交通票务平台。

目 录

01 企业国际化与数安风险

外-国际化过程中面临的客观风险现实

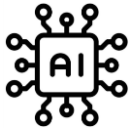
地缘政治博弈

对本国重要数据及敏感个人信息流向对方的顾虑

数据泄露成本增加

泄露赔偿、诉讼、品牌损失等各种直接和间接成本

新技术带来挑战



智能化带来的安全体系重塑及用户权力保障

不断增加的适用法律和监管

多一个成熟法域的站点，增加15+数据安全相关的法律法规和标准

隐私意识加强

投诉处理不当，一个case即可引发PR事件

内-业务国际化扩张与安全诉求

	业务诉求	风险	安全诉求
产品	便捷的下单转化	授权缺失	透明性及必要的授权
研发	快速的产品开发迭代	架构不合规，未适配海外规范	合规的架构设计，收集最小必要，SDK合规
数据分析	准确的海外用户画像	超范围采集和超期存储	采集合规+最小存储+删除权实现
营销	快速便捷的海外获客、再营销	用户权力无法保障	用户拒绝权+Cookie合规
供应链	供应链中数据自由流通	数据跟着货品服务全球流通，权责不清晰	明确安全保障在内的各方权责，用户对三方的知情权，安全水位拉齐
人力资源	保障业务快速扩张	员工意识不足带来的安全隐患，员工隐私不合规	足够的安全意识，员工隐私保护

部分与中国出海公司/行业相关的数安事件

序号	事件描述	时间	行业	法域	安全类别
1	某支付平台在香港因留存用户数据违规受到消协质疑	2016/10	移动支付	香港	个人信息存储
2	某短视频APP因儿童隐私问题被美国FTC罚款570万美元	2019/2	短视频	美国	儿童数据隐私
3	某ICT服务提供商因未及时响应员工隐私诉求被德国杜塞尔多夫法院判定败诉	2020/4	ICT服务	德国	员工隐私
4	印度宣布将永久禁止59款中国APP	2020/6	移动应用	印度	其他
5	美国安全公司Palo Alto发现某互联网公司开发的两款APP未按照《安卓最佳实践指引》收集IMSI等个人信息，Google Play在确认后下架了这两款APP	2020/10	互联网地图	美国	APP隐私
6	某头部互联网企业内审门事件导致企业遭遇公众信任危机	2022/12	互联网综合类	美国	违规查询
7	某短视频APP因Cookie违规被法国CNIL处以500万欧元的罚款	2023/1	短视频	法国	Cookie隐私
8	某短视频APP因未经儿童父母同意滥用13岁以下儿童数据，被英国ICO罚款1270万英镑	2023/4	短视频	英国	儿童数据隐私
9	美国国会下属美中经济与安全审议委员会发布分析师报告，认为中国跨境电商存在数据安全等问题，建议美国政府应保持警惕。	2023/4	电商	美国	数据安全
10	某短视频APP因儿童隐私问题被爱尔兰数据保护委员会罚款 3.45 亿欧元	2023/9	短视频	爱尔兰	儿童数据隐私
11	美国白宫发布声明，宣布将对中国进口汽车是否对美国国家安全造成威胁进行调查，调查将重点关注收集敏感数据和远程控制车辆等风险	2024/2	网联汽车	美国	数据安全隐私
12	某短视频APP未能通过适当的机制监控平台上发布的内容，尤其是那些可能威胁未成年人和弱势群体安全的内容，被意大利竞争管理局（AGCM）罚款1000万欧元	2024/3	短视频	意大利	算法内容安全
13	美国阿肯色州司法部长在美国巡回法院对某中资电商APP提起诉讼，声称该APP作为恶意软件运行，并未经授权访问用户位置、联系人、短信等隐私数据	2024/6	电商	美国	APP安全&隐私
14	某电商平台因未向韩国用户披露18万海外卖家的详细信息，被韩国PIPC处以近19.8亿韩元罚款	2024/8	电商	韩国	数据跨境

海外监管对各自法域的最高处罚案例（部分）

欧盟

法国广告技术巨头Criteo因未能就定向广告征求用户同意而被法国CNIL处以**4000w欧元**的罚款

英国

英国航空公司因2018年数据遭泄露被英国信息专员办公室ICO开出**1.83亿英镑**罚单。万豪因泄露3亿客人信息被罚**1.6亿英镑**。

美国

因剑桥分析事件，Facebook被美国联邦贸易委员会FTC处以**50亿美元**罚款

韩国

韩国Kakao因疏于管理和保护用户信息导致超过6.5万条个人信息遭到泄露，被个人信息保护委员会罚款约151亿韩元（约**1100w美元**）

新加坡

新加坡IHiS 因数据库遭遇攻击，致使150万名病患个人资料，以及16万人门诊开药记录泄露，被罚款**75w新元**

泰国

泰国某企业因未任命DPO、未充分保护数据、泄露未通报等被泰国个人数据保护委员会PPDC罚款700万泰铢（约合**20w美元**）

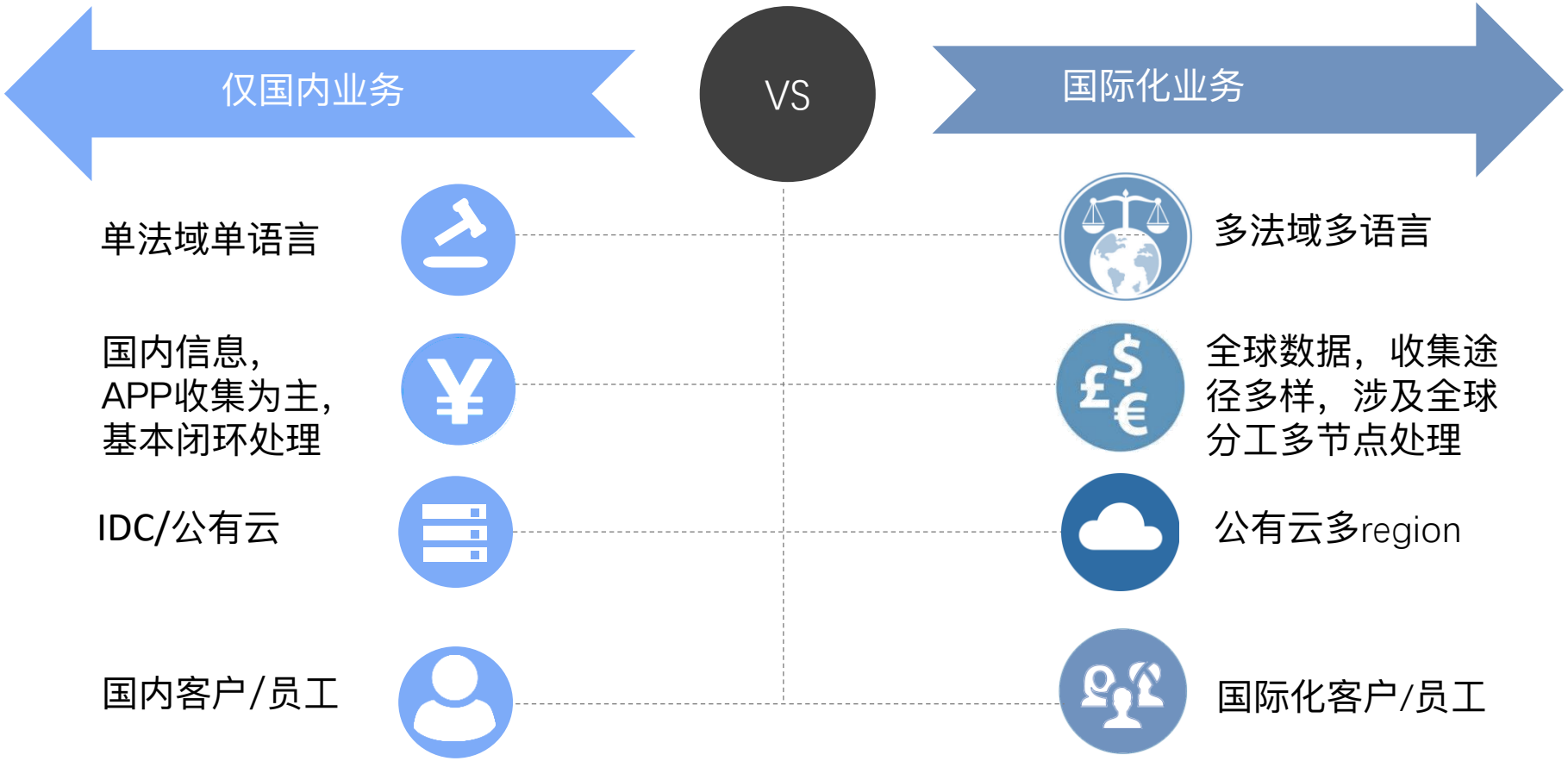
澳大利亚

因澳大利亚医疗保险巨头Medibank 970 万名客户的个人数据泄露。2024年6月，OAIC 已经对其提起民事诉讼，要求其承担相应责任。

02

哪些关键点不应被忽略?

规划-国际化带来哪些风险差异?



规划-风险偏好，关乎目标、成本

风险偏好

- 4 激进（Moderate）
- 3 中等适度（Moderate）
- 2 保守（Conservative）
- 1 风险厌恶（Risk-averse）

安全合规当前风险及目标

- 数据保护：无黑客攻击导致的数据泄露
- 事件运营：告警事件MTTR<1h
- 隐私合规：海外监管零通报
- 安全资质：超出海外竞品
- 三方管理：供应商风评线上化

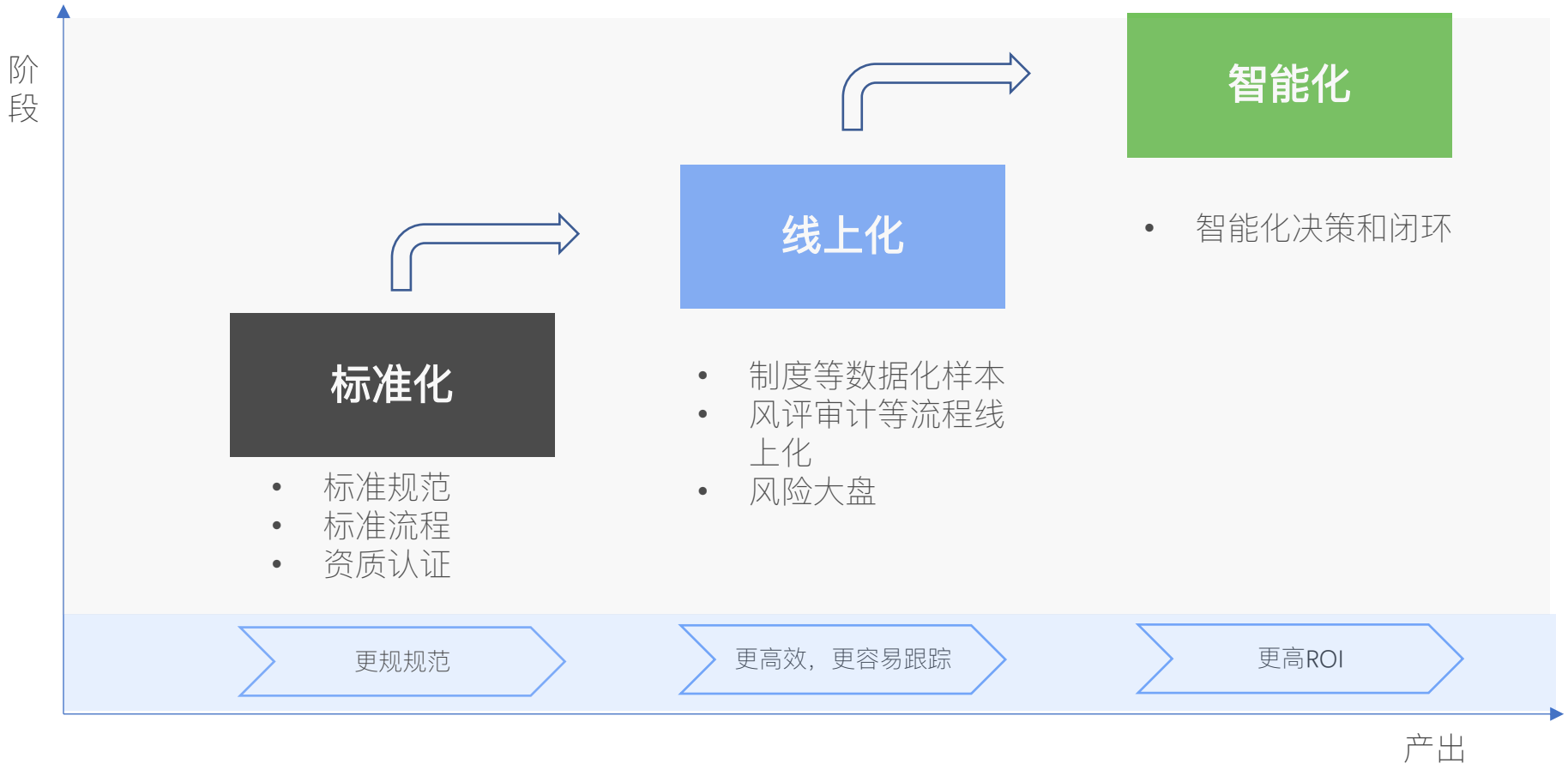
控制措施成熟度

- C5 持续优化（闭环流程改进控制）
- C4 量化控制（有KIR描述效率、质量和风险）
- C3 充分定义（标准充分定义，不依赖个人）
- C2 计划跟踪（有流程并文档）
- C1 非正式执行（缺乏组织，依赖个人经验）

规划-组织，推进落地的基础

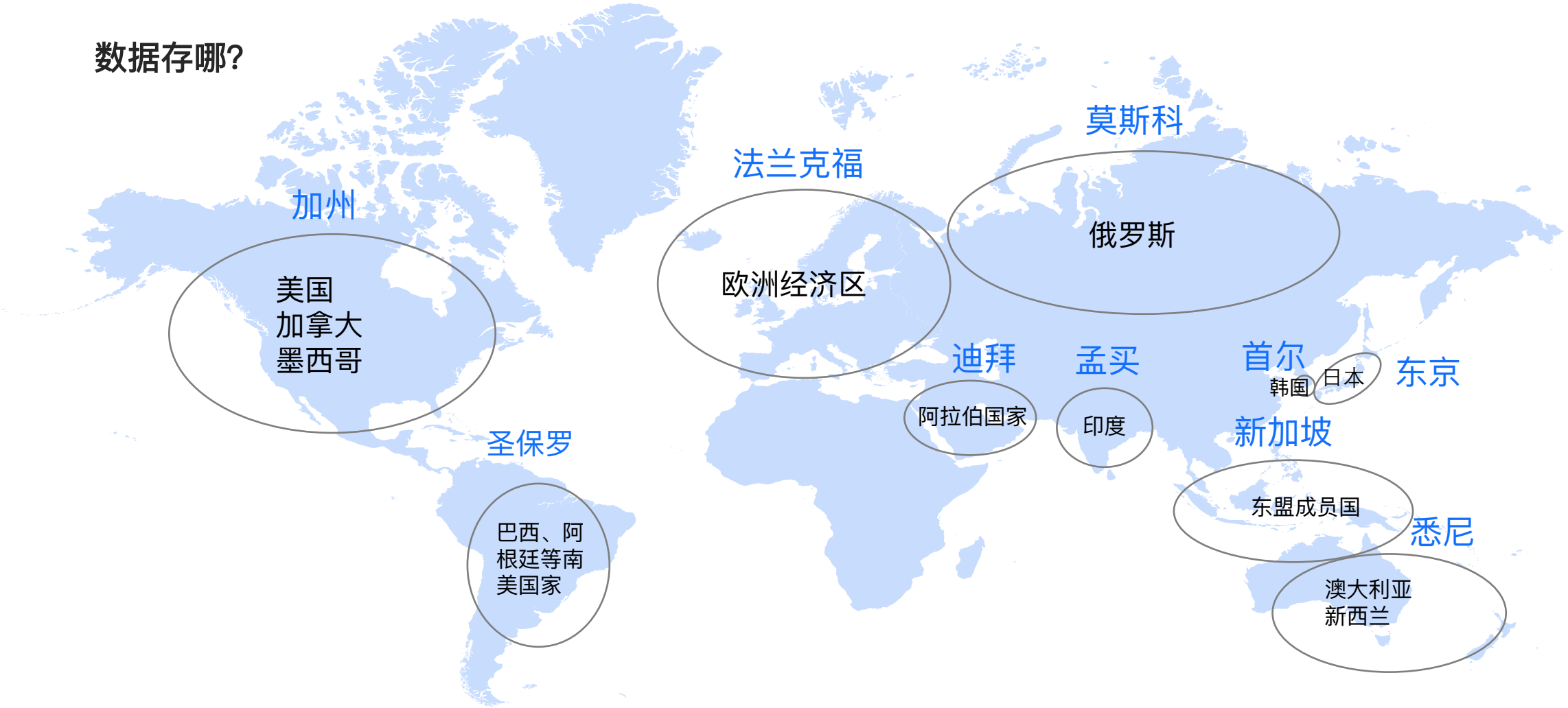
一个典型的涉及数据安全合规管理职能的组织架构

规划-智能化为更高目标，实现提效

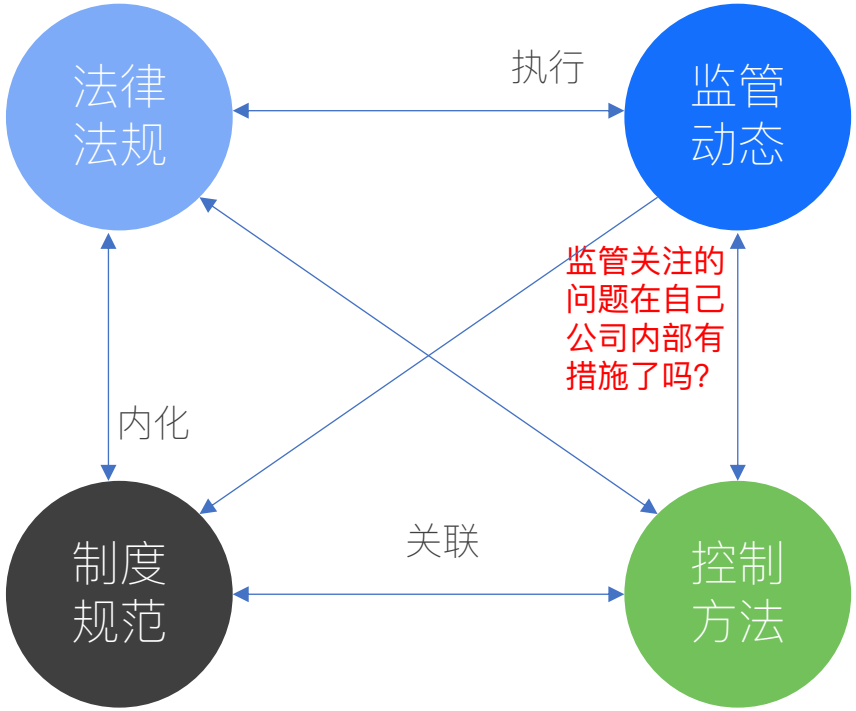


规划-深入到架构设计

数据存哪?



规划-处理好以下四个元素的关系



落地-情报，外部驱动的关键所在

监管机构网站	法院	聚合性平台	非营利性组织
欧盟数据保护委员会	欧洲联盟法院CJEU	Dataguidance	Noby.eu
荷兰数据保护局	法国行政法院Conseil d'Etat	Enforcementtracker	
英国信息专员办公室	阿姆斯特丹法院	...	
韩国个人信息保护委员会	澳大利亚联邦法院		
日本个人信息保护委员会	...		
新加坡个人信息保护委员会			
SEC			
FTC			
...			

落地-关键要求无死角

这些你们都关注了吗?

美国

- 《外国投资风险审查现代化法案》-外国投资的美国业务涉及关键技术、关键基础设施或美国公民敏感个人数据，交易当事人必须向CFIUS提交强制申报。
- 《保护美国人数据免受外国监视法案》-个人敏感数据禁止流向对手国家
- 《上市公司网络安全风险管理、策略、治理及事件披露规则》-4个工作日内通报重大安全事件

欧盟

- 《GDPR》-30天内完成DSR处理，72h内完成数据泄露通报
- 《电子通信法案》-未授权情况下禁止种植非必要的Cookie
- 《人工智能法案》-禁止AI用于社会评分
- 《数字服务法案》-应删除非法内容

俄罗斯

《第242-FZ号联邦法》-须使用位于俄罗斯的服务器来处理俄罗斯公民的个人数据

韩国

- 《个人信息保护法案》-禁止收集个人纳税人识别号(RRN)，出境单独同意并披露境外国家、日期、三方的名字和联系方式

越南

- 《53号法令》-向越南客户提供电信和在线服务的国内公司都必须在越南本地存储某些与客户相关的数据

新加坡

- 《个人信息保护法案》-禁止任何机构向谢绝来电登记簿登记的新加坡电话号码发送营销信息

落地-基于差异的精细化管理

序号	议题 \ 法域	欧盟	英国	美国（加州）	日本	韩国	新加坡	泰国	菲律宾	马来西亚	中国香港
1	DPO任命	明确	明确	未明确	未明确	明确	明确	明确	明确	未明确	未明确
2	安全保护	明确	明确	明确	明确	明确	明确	明确	明确	明确	明确
3	RoPA	明确	明确	未明确	未明确	未明确	维护个人信息资产目录	明确	未明确	未明确	未明确
4	数据保护影响评估	明确	明确	明确	未明确	仅公共机构强制	明确	安全措施评估	明确	未明确	未明确
5	敏感个人信息额外要求	明确	明确	明确	明确	明确	有指引非强制	明确	明确	明确	其他规范明确
6	儿童信息监护人同意门槛	各国定义，最低13	<18岁	<13岁	无相关要求	<14岁	<14岁	<10岁	无相关要求	<18岁	无相关要求
7	特殊证件信息（示例）	因各国而异	BRP, Citizen Card	州身份证（State Identification Card）	个人编号卡（My Number card）	居民登记号码(RRN)	Sinpass	Thai ID Card	统一多用途身份证(UMID)	MyKad	香港身份证
8	Cookie banner及设置	明确	明确	未明确	未明确	未明确	未明确	明确	未明确	未明确	未明确
9	数据可携带权	明确	明确	明确	未明确	明确	未明确	明确	明确	未明确	未明确
10	DSR删除	明确	明确	明确	明确	明确	明确	明确	明确	未明确	未明确
11	数据泄露通知监管时效	72h	72h	15个工作日	3~5天	72h	72h	72h	72h	暂无	无强制通报要求
12	数据本地化&跨境管理	无&严格	无&严格	无&一般	无&一般	无&严格	无&一般	无&一般	无&一般	无&一般	无&一般