2023

制造业CIO出海系列沙龙

企业出海中的数据合规

宣讲人：刘歆轶　公司：非夕机器人

企业网DINet 企业IT第1门户

信众智 CIO智力输出及社交平台

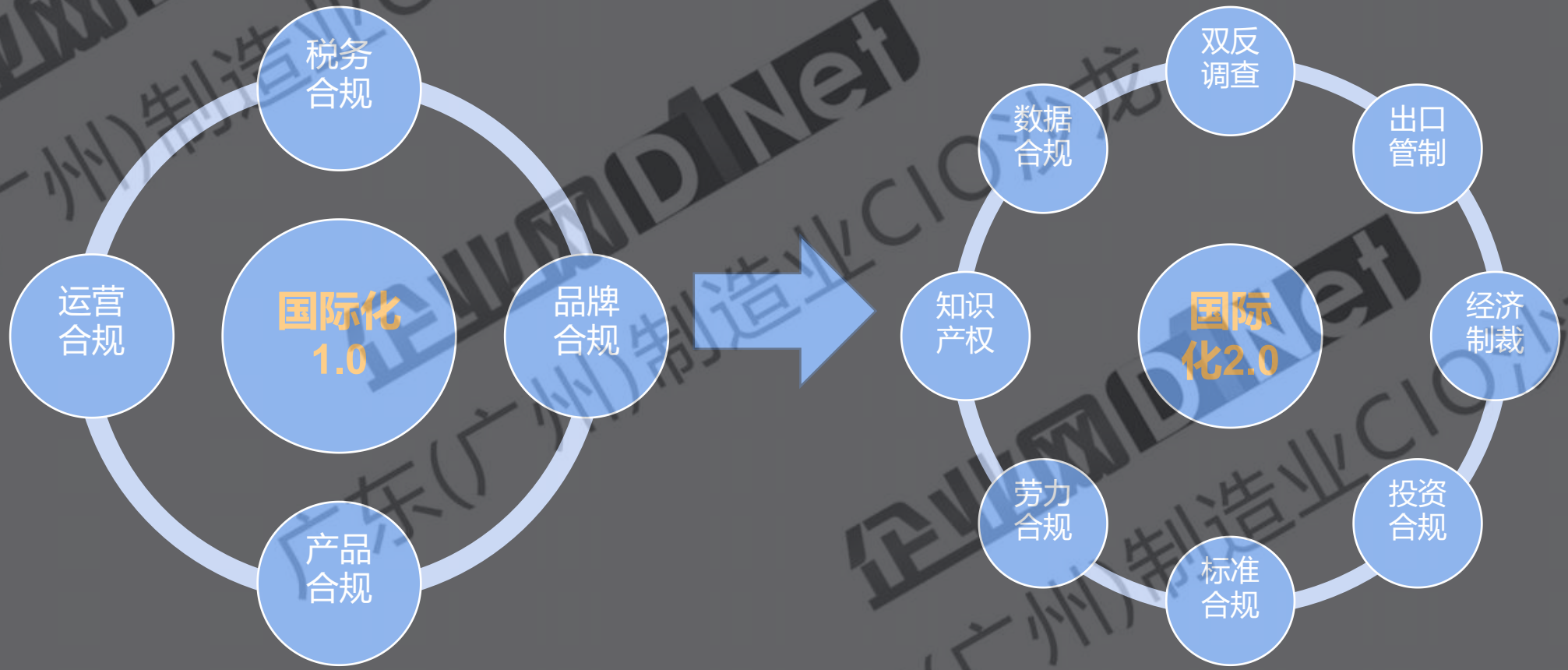
目录

Contents

企业出海合规

01 企业出海常见风险

01 合规风险：从“国际化1.0”到“国际化2.0”



01 国际化1.0时代的合规痛点

时间成本和潜在损失

卖家为满足各国的各类合规将花费大量时间如果仍未满足要求，还将面临产品下架、处罚乃至关店停业问题，给经营带来损失

不了解当地法律

国内卖家通常无法对海外国家的相关法律法规保持高度关注，了解各类监管要求的时效性和准确度都不足。

不具备相关专业知识

无论是税务、产品、品牌领域的合规工作都需要相关的专业知识来应对处理，国内卖家可能不具备相关的专业技能

不在本地，沟通不畅

处理一些数字化程度不高的国家和地区的合规工作需要和当地办事人员、公务员进行书信甚至当面沟通，对国内卖家较为困难

语言能力不足

包含通用的英语在内，卖家还需要掌握欧洲中东等国的其他小语种以应对各类事务，国内卖家通常无此能力。

01 国际化2.0合规之双反调查

反倾销调查

- 出口产品存在倾销
- 对进口国内行业产生损害
- 倾销与进口国内产业损害之间存在因果关系

反补贴调查

- 政府机构提供财政资助
- 直接和潜在资金或债务转移到政府
- 放弃或未征收税收
- 政府提供基础设施外的货物或服务
- 政府向筹资机构付款
- 委托私营机构履行上述一或多种职能

对企业影响

- 不仅针对涉案企业，所有同类产品企业都受影响
- 应诉企业可能获得单独的税率或加权平均税率
- 不应诉不配合的企业适用最高的惩罚性统一税率
- 初裁后，进口商需支付双反税率押金才可清关

01 国际化2.0合规之出口管制国际条约

国际条约	多边条约	地区管制
• (1)联合国安理会1540号决议 • (2)核不扩散条约 • (3)禁止生物武器 • (4)禁止化学武器公约	• (1)瓦森纳安排 • (2)核供应国集团 • (3)澳大利亚集团 • (4)导弹及其技术控制制度	• The European Union (EU)

01 国际化2.0合规之美国出口管制措施

禁止的最终用途

- 核用途,火箭系统及无人飞行器
- 生化武器
- 出口至或用于特定外国船只/航空器
- 向特定受制裁人(与大规模杀伤武器相关)出口
- 将特定照相机、系统或相关部件用于军事用途
- 对俄罗斯军事用户的特殊限制(特殊的FDP规则)
- 将特定微处现器用于特定国家的军事用途

禁止的最终用户

- 实体清单
- 被拒绝人员清单
- 未核实清单
- 军事最终用户清单
- 缅甸、柬埔寨、中国、俄罗斯、委内瑞拉的军事最终用户

01 国际化2.0合规之美国强迫劳动法案

UFLPA要点

- 主要内容：制裁新疆，禁止新疆产品入境
- 法案效果：降低了美国对华制裁的门槛，扩大对华供应链制裁范围
- 实现手段：检验或扣押货物，禁止进入美国市场
- 证书责任：进口商承担
- 实施时间：2022年6月21日起，UFLPA生效180天后

执法行动

- 扣留
- 放行
- 禁止清关
- 没收

01 国际化2.0合规之中国两用物项出口管制

《中华人民共和国出口管制法》

第二条国家对两用物项、核以及其他与维护国家安全和利益、军品、履行防扩散等国际义务相关的货物、技术服务等物项(以下统称管制物项)的出口管制，适用本法。

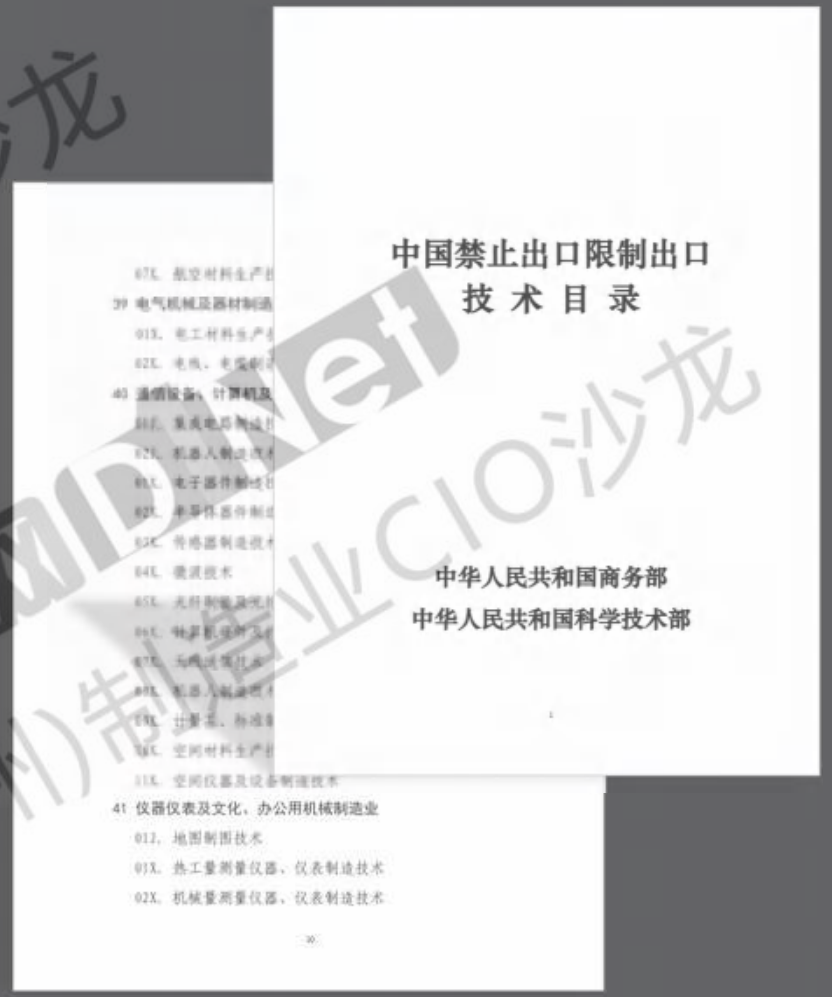
- 前款所称管制物项，包括物项相关的**技术资料等数据**。
- 本法所称出口管制，是指国家对从中华人民共和国境内向境外转移管制物项，以及中华人民共和国公民法人和非法人组织向外国组织和个人提供管制物项，采取禁止或者限制性措施。
- 本法所称**两用物项，是指既有民事用途，又有军事用途**或者有助于提升军事潜力，特别是可以用于设计、开发、生产或者使用大规模杀伤性武器及其运载工具的货物、技术和服务。
- 本法所称军品，是指用于军事目的的装备、专用生产设备以及其他相关货物、技术和服务。
- 本法所称核，是指核材料、核设备、反应堆用非核材料以及相关技术和服务。

01 国际化2.0合规之中国知识产权及技术资料出境管控

技术资料数据出境

管制物项出口?

技术资料所含的数据，属于禁止或限制出口的管制物项，则除了数据合规义务以外，还要同时考虑出口管制的合规义务履行（例如查阅《中国禁止出口限制出口技术目录》）。



《数据安全法》第二十五条：国家对与维护国家安全和利益、履行国际义务相关的**属于管制物项的数据**依法实施**出口管制。**

《出口管制法》第二条：国家对两用物项、军品、核以及其他与维护国家安全和利益、履行防扩散等国际义务相关的货物、技术、服务等物项（以下统称**管制物项**）的出口管制，适用本法。

前款所称**管制物项，包括物项相关的技术资料等数据。**

01 国际化2.0合规之信息安全相关标准合规

ISO 27001

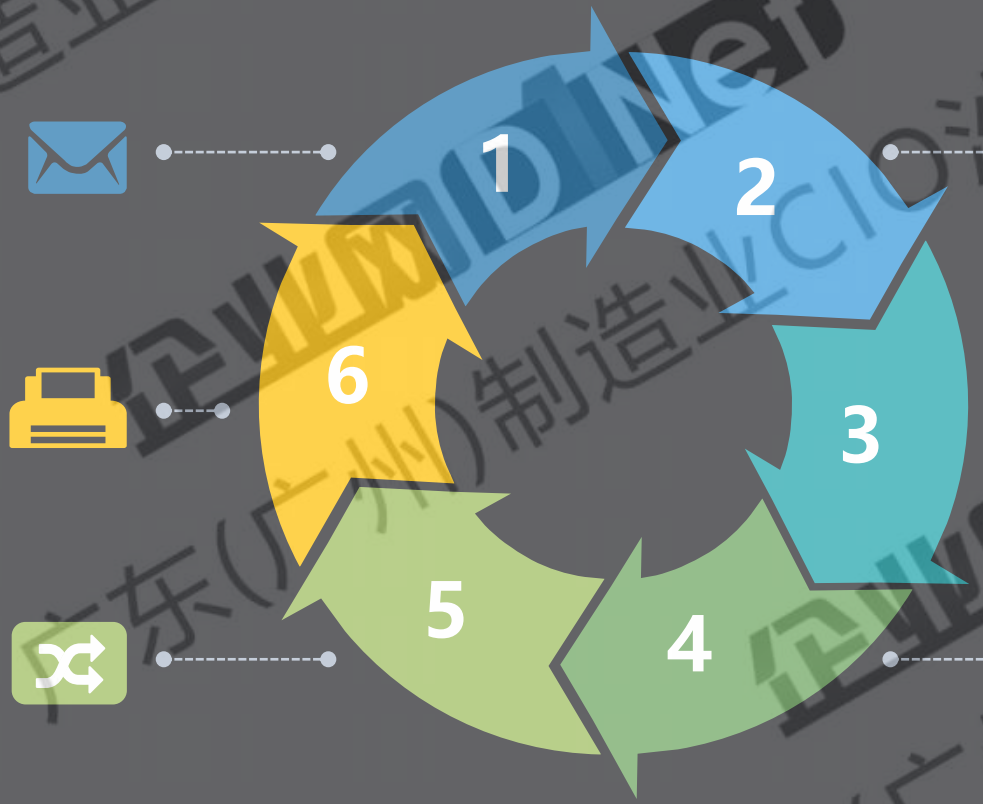
全球范围内最广泛采用的信息安全管理体系认证标准

隐私认证

ePrivacy和TrustArc

NISTIR 8259

物联网设备安全能力评估框架



ISO 27701

全球市场的个人信息保护管理体系认证标准

IEC 62443

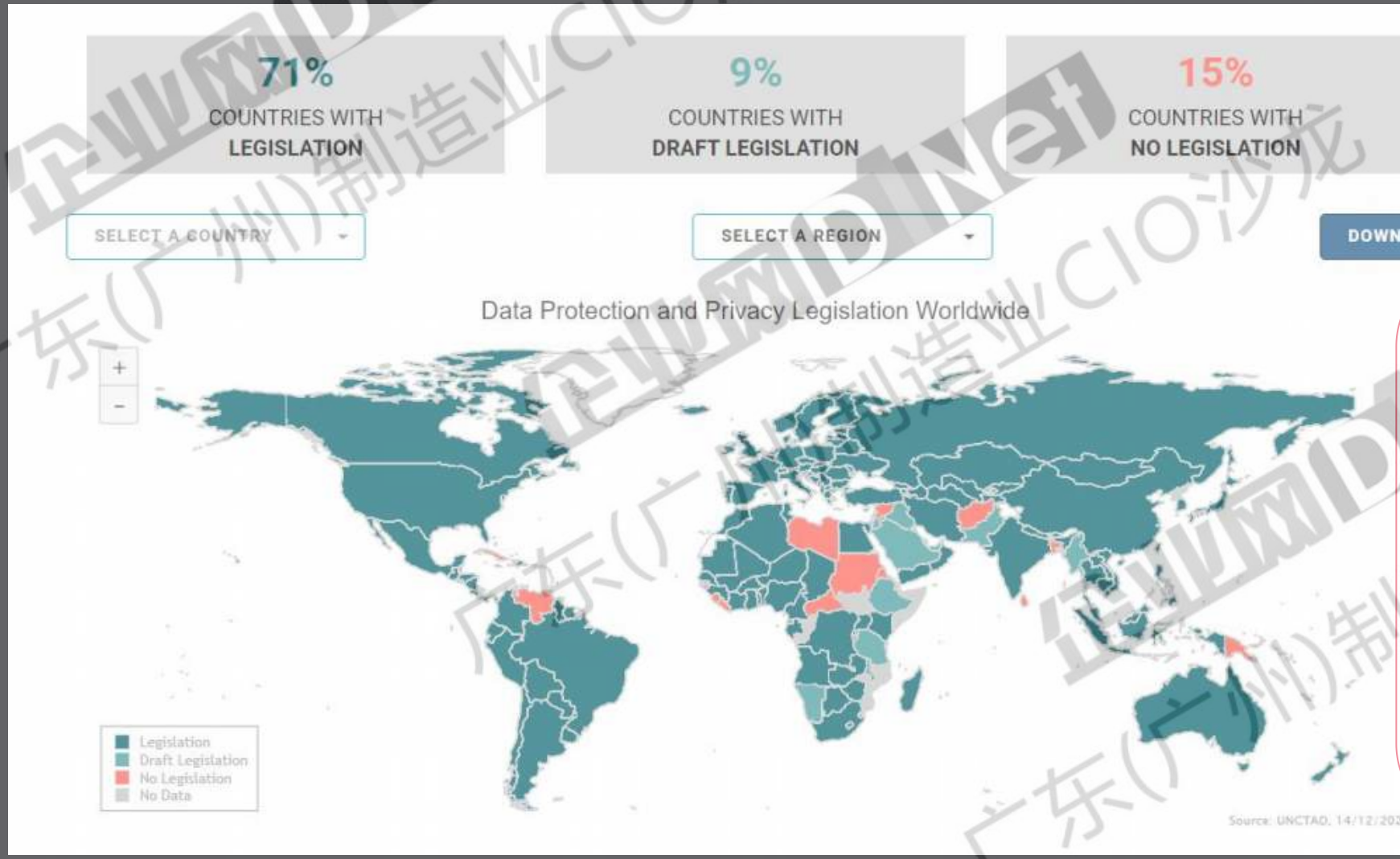
面向工控系统的网络安全标准

ETSI EN 303645

物联网设备安全标准

02 数据跨境合规

02 全球数据保护与隐私立法概览



主要立法模式

多部立法+不同场景/行业立法

- **中国：**
  网安法、数安法、个保法
  场景立法（数据出境）、行业立法

统一立法+指引

- **欧盟：**GDPR+EDPB指引

无统一立法+不同州/行业立法

- **美国：**州立法（CCPA、CPRA）、
  行业立法（通信、金融、消费）

02 全球数据跨境法律法规

国家/地区	法律法规名称
EEA	GDPR
英国	GDPR 英国数据保护法
墨西哥	《关于私主体个人数据保护义务的联邦法律》
土耳其	《个人数据保护法（LPPD）》
巴西	《巴西通用数据保护法（LGPD）》
哥伦比亚	2012 年《第 1581 号成文法》 2013 年《第 1377 号成文法》
秘鲁	《个人数据保护法 N° 29733》
俄罗斯	《第 152 FZ 号数据保护法》 《第 242 FZ 号数据保护法》 《第 405 FZ 号数据保护法》
印度	2019 年《个人数据保护法案》草案
印度尼西亚	未有个人数据保护法，《政府电子系统和交易实施条例》对公共电子系统提出了若干要求，对私数据库没有相关要求
日本	《个人信息保护法》
菲律宾	《2012 年数据隐私法》
巴基斯坦	2020 年个人数据保护法案（草案）
孟加拉国	暂无成文个人信息保护法，仅有《2018 年数字安全法案》，其中暂无数据跨境传输相关内容。
越南	暂未有成文个人信息保护法
缅甸	暂未有成文个人信息保护法
泰国	《个人数据保护法》2020
马来西亚	《2010 年个人数据保护法令》
乌克兰	关于个人数据保护的第 2997-VI 号法律 第 4452-VI 号法律（修正案） 第 5491-VI 号法律（修正案）
尼泊尔	暂未有个人数据保护法令
新加坡	《个人信息保护法案》2012，2020 年的修订并未涉及数据跨境传输部分

国家/地区	法律法规名称
韩国	《个人信息保护法》
埃及	《数据保护法》
埃塞俄比亚	无生效数据保护法，仅关于支付类的指引规则中有本地化的要求。
南非	《南非个人信息保护法》
尼日利亚	《2019 年尼日利亚数据保护条例》
阿尔及利亚	《2018 年第 18-07 号法律》
贝比亚	《2020 第 3 号数据保护法》
利比亚	目前利比亚没有数据保护法，亦无相关规定。
乌干达	《数据保护和隐私条例》
安哥拉	《数据保护法》
摩洛哥	《个人信息保护第 09-08 号法律》
阿联酋	阿联酋暂无隐私保护法令，信息和通信技术保健法第 13 条中提到了本地存储要求 DIFC 于 2007 年制定了隐私保护法令，于 2020 年进行了补充修订，Data Protection Law（DIFC Law No. 5 of 2020）
香港	《个人资料（私隐）条例》（未有关于数据跨境的规定）
中国	《网络安全法》 《数据安全法》 《个人信息保护法》 《网络安全审查办法》 《数据出境安全评估办法（征求意见稿）》 《数据安全管理办法（征求意见稿）》 《信息安全技术 数据出境安全评估指南（征求意见稿）》 《个人信息和重要数据出境安全评估办法（征求意见稿）》 《个人信息出境安全评估办法（征求意见稿）》

02 全球数据跨境管控要求

国家/地区	法律法规名称	相关规定/重点要求
中国	《中华人民共和国网络安全法》	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；
	《个人信息和重要数据出境安全评估办法（征求意见稿）》	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，应当按照本办法进行安全评估；
	《数据安全法》	在一般数据安全保护义务之上，对重要数据的处理者规定了“增强型”的保护义务： 1. 重要数据的处理者应当设立数据安全负责人和管理机构，落实数据安全保护责任； 2. 重要数据的处理者应当按照规定对其数据活动定期开展风险评估，并向有关主管部门报送风险评估报告；风险评估报告应当包括本组织掌握的重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。
	《信息安全技术 重要数据识别指南（草案）》	首次提出了重要数据的完整定义（从数据的作用、安全属性可能带来的影响等角度，将重要数据分为国民经济运行类、资源环境类、自然资源与环境类、健康类、敏感技术类、国户安及政府工作秘密类），并列举了29个行业的重要数据实例。范围、在重要数据的定义中，附带给出了重要数据判定准则。按照数据泄露后的危害，丢失、滥用、篡改或销毁，或汇聚、整合、分析后可能造成的后果，列出了9种情况；
	《基础电信企业重要数据识别指南（草案）》	内容涉及重要数据的定义、运营基础电信业务过程中识别重要数据的原则、规则、工作流程等。
德国	《电子通信法》	原始数据的本地存储进行规定
印度	《国家电子商务政策》	将重点建立基础和技术框架为如下情形的跨境数据流动提供便利：（1）发源在公共场所的物联网设备收集的数据；以及（2）印度用户通过各种来源产生的数据，包括电子商务平台、社交媒体、搜索引擎等。但是也列出了一些允许跨境流动的例外情形，例如云计算服务中不涉及个人和社区数据的技术数据。
	《统一许可协议》	许可不得将下列内容传输给任意其他人/印度之外的场所： 1. 与订阅者有关的任何会计信息（除了国际漫游/账单）（注意：这要求不排斥与执法定要求披露财务信息）； 2. 用户信息（除了在漫游期间使用印度运营商网络的外国订阅者或IPLC的订阅者）
	《电子药房规则草案》	以电子医药行业为试点推行了反对数据跨境流动的政策
	《国家数据分享和准入政策》	所有通过使用公共基金收集的数据均存储于本国境内
印度尼西亚	《电子系统和交易条款的2019年第71号政府法规》	公共电子系统运营商必须将其电子系统和数据（包括政府、能源、交通、金融、医疗、IT和通信、国防等战略性数据）放置在印度尼西亚。而非公司另有规定，否则私人电子系统运营商可以将其电子系统和数据放置在印度尼西亚境内或境外。但是，私有电子系统运营商必须允许政府机构进行“监督”，包括访问电子系统和数据，以进行监控和执法。

国家/地区	法律法规名称	相关要点/重点要求
越南	《互联网服务和在线信息管理、提供和使用条例》	要求信息收集网站，社交网站，移动通信网络服务提供者，在线游戏服务提供者等，至少将一个服务器设置在越南境内 同时，在《网络安全法》中，要求互联网和在线附加服务提供服务的国内外企业，收集，利用，分析和处理信息数据，个人，服务用户的关系数据以及越南服务用户创建的数据必须进行存储。
韩国	《电子金融交易监管条例》	根据本地化措施适用于金融领域。电子金融交易监管条例禁止韩国金融机构跨境传输持有的可识别信息，并要求这些机构在韩国安装服务器和灾难恢复设施，只有对电子金融交易的安全性和可靠性影响有限，且可能因此被指定为“非关键”的信息处理系统，才可建立在国外。
	《金融机构外包数据处理业务和IT设施条例》	金融领域的数据处理外包适用特定的限制。26韩国境内的金融公司必须向金融服务委员会（FSS）报告法律在外包数据处理规定的特定事项，无论此类数据处理发生在韩国境内或外国管辖范围内。
美国	受控非密数据清单	1. 根据适用法律，法规和政府政策进行保护或传播控制的信息，分为： 仅供官方使用信息（FOUO INFORMATION）； 执法敏感信息（LES INFORMATION）； 国防部受控非密核信息（Do D UCNI）； 限制分发信息（LIMITED DISTRIBU-TION INFORM ATION）；国务院敏感非密信息（Do S SBU）； 编毒署敏感信息（DEA Sensitive Information）； 外国政府信息（FOREIGN GOVERNMENT INFORMA-TION）； 技术文件分发声明（DISTRIBUTION STATE-M ENTS ON TECHNICAL DOCUM ENTS） 2. 受控非密信息的管理包括： 监管机构创建或处理非机密信息的机构应采取保护措施和控制措施，以保护CUI免受未经授权的侵害访问； 法律，法规或政府范围的政策是否应包括传播控制或指定特定说明，并在CUI注册表中提供参考； 当不再需要采取保护措施时，应尽快解除CUI的控制和最终当局的传播控制等
俄罗斯	《互联网主权法案》	1. 俄罗斯互联网稳定运行的主要责任主体是电信运营商以及技术通信网络，网络流量交换点，自治系统号码（ASN）的所有者； 2. RKN通过定义路由政策，协调电信运营商和责任方以及他们之间的连接，从而执行集中化的通信网络管理职能。 3. 责任方义务包括：参加稳定俄罗斯网络的常规演习；安装技术设备，以防范对俄罗斯境内互联网运营的稳定性、安全性和完整性的威胁等。
土耳其	/	土耳其信息技术和通信管理局发布了两项决定，以管制存在因引起有缺陷的嵌入式SIM技术，尤其是电子呼叫系统的SIM卡事故化要求，以防止车辆永久漫游；第一个决定规范车辆中的电子呼叫服务，第二个决定规范远程可编程的eSIM技术。
阿尔及利亚	/	阿尔及利亚通过立法要求电子商务运营者从阿尔及利亚境内的数据中心提供服务。

02 主要国家数据跨境管控特点对比

国家/国际组织	数据跨境政策	特点
欧盟(成员国)	以地理区域为准,以充分性为原则	程序冗杂,标准严苛
美国	以组织机构为准,以问责制原则为核心	规制功能下降,惩罚力度小
俄罗斯	以地理区域为准,以数据本地化为原则	过于排斥
澳大利亚	以利益均衡为导向,以折中型为特征	法律不协调,针对性弱
日本	设立独立监管机构,设置一般性规定,增加主体同意原则的例外性规定	“国内—双多边—全球”由内及外推进
印度	以本地化为主,数据分级分类管制、设有豁免规则	运营成本增加,数字贸易发展有限
韩国	以数据主体明确同意为原则,重要信息本地化	以法案为核心,不断更新与修订
中国	以主体同意为原则,关键数据本地化,出境需安全评估	管理体系不成熟,存在较多短板

02 我国数据保护与隐私立法历程

2017

4月

《个人信息和重要数据出境安全评估办法（征求意见稿）》发布

6月

《网络安全法》生效

8月

《信息安全技术-数据出境安全评估指南（征求意见稿）》发布

2018

6月

《网络安全等级保护条例（征求意见稿）》

2019

1月

《电子商务法》生效

6月

《个人信息出境安全评估办法（征求意见稿）》

12月

MLPS2.0生效

2020

1月

《密码法》生效

7月

《数据安全法（草案）》发布

10月

《个人信息保护法（草案）》发布

2021

4月

《数据安全法》《个人信息保护法》二次审议稿发布

6月

《数据安全法》发布（9月1日生效）

8月

《个人信息保护法》发布（11月1日生效）

10月

《数据出境安全评估办法（征求意见稿）》发布

11月

《网络数据安全管理条例（征求意见稿）》发布

2022

6月

《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》

《个人信息出境标准合同规定（征求意见稿）》

7月

《数据出境安全评估办法》

9月

《数据出境安全评估申报指南（第一版）》

2023

02 我国数据保护与隐私立法历程

2023

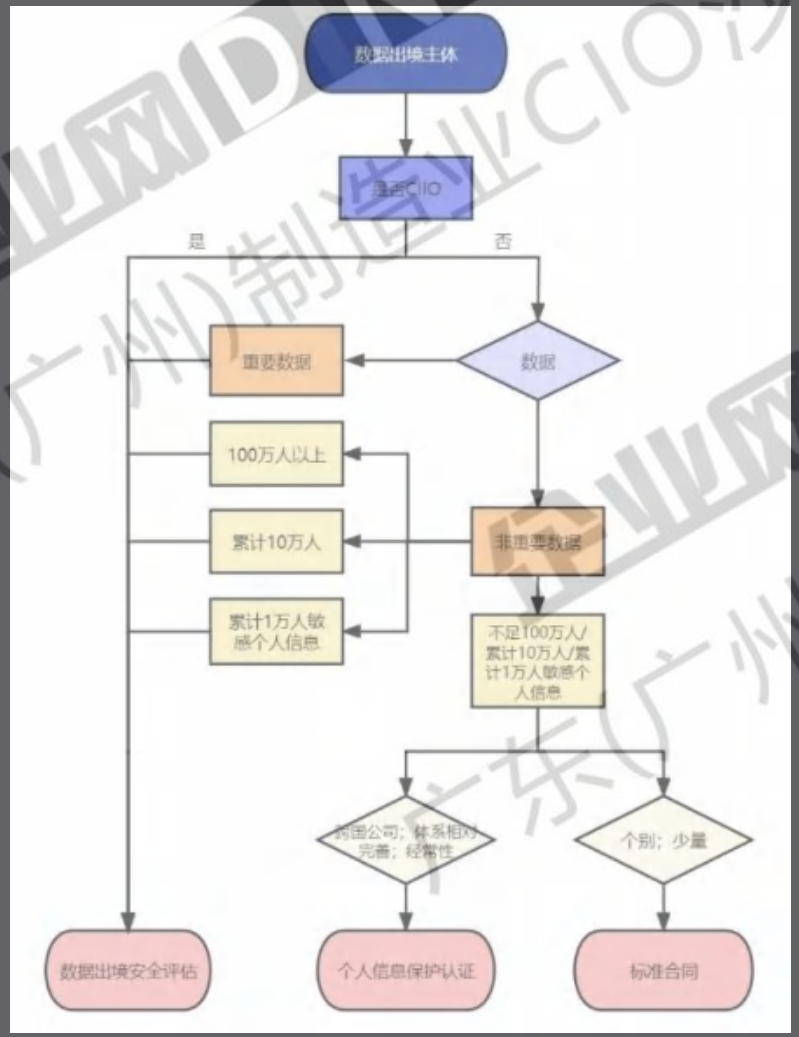
《个人信息保护认证实施规则》
《个人信息出境标准合同办法》
《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》
《征信业务管理办法》
《关于构建数据基础制度更好发挥数据要素作用的意见》
《网络数据安全风险评估实施指引》征求意见稿
《科技伦理审查办法（试行）》
《规范和促进数据跨境流动规定》（征求意见稿）

2024

《未成年人网络保护条例》

02 数据出境安全评估办法

02 数据出境的三种途径



	数据出境安全评估	个人信息保护认证	个人信息出境标准合同
适用情形	① 关键信息基础设施运营者； ② 处理100万人以上个人信息的数据处理者向境外提供个人信息； ③ 自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息； ④ 向境外提供重要数据	个人信息处理者开展个人信息跨境处理活动	① 非关基运营者； ② 处理个人信息不满100万人； ③ 自上年1月1日起累计向境外提供个人信息不满10万或自上年1月1日起累计向境外提供敏感个人信息不满1万人
法律依据	2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》	2022年6月24日，信安标委秘书处发布《网络安全标准实践指南 个人信息跨境处理活动安全认证规范》； 12月16日，信安标委再次发布《网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0》； 2022年11月18日，市场监管总局、国家网信办发布《个人信息保护认证实施规则》	2023年2月24日，国家互联网信息办公室发布了《个人信息出境标准合同办法》及其附件《个人信息出境标准合同》
常见类型	法定触发	频发、长期 跨国集团、关联实体	少量、偶发 跨境商业交易或合作 出境场景直接、清晰
有效期	2年	3年	依照合同约定
实施主体	国家网信部门	特定认证机构（如CCRC）	个人信息处理者及境外接收方
自评估	数据出境安全自评估+个人信息保护影响评估	个人信息保护影响评估	个人信息保护影响评估（备案）
备案要求	无	无	合同生效后10个工作日内向省级网信部门备案
费用	无	认证机构收取认证费用	无

02 重要数据的界定

影响政治安全

- 直接影响国家主权、政权安全、政治制度、意识形态安全

用以实施社会动员的数据

影响国土安全

- 直接影响领土安全和国家统一，或反映国家自然资源基础情况

未公开的领陆、领水、领空数据

影响军事安全

- 可被其他国家或组织利用发起对我国的军事打击，或反映我国战略储备、应急动员、作战等能力

满足一定精度指标的地理信息

战略物资产能、储备量信息

影响经济安全

- 直接影响市场秩序或国家经济命脉安全

支撑关键基础设施所在行业、领域核心业务运行或重要经济领域生产的数据

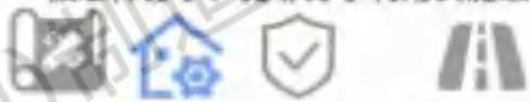
影响文化安全

- 反映我国语言文字、历史、风俗习惯、民族价值观念等特质

历史文化遗产信息

影响社会安全

- 反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可被恐怖分子、犯罪分子利用实施破坏



重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）的施工图、内部结构、安防等信息

未公开的专用公路、机场信息等

02 重要数据的界定

影响科技安全

- 关系国家科技实力、影响国际竞争力，或关系出口管制物项

反映国家科技创新重大成果

描述我国禁止出口限制出口物项的设计原理、工艺流程、制作方法等的信息

源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告

影响网络安全

- 反映关键信息基础设施总体运行、发展和安全保护情况，可被利用实施对关键信息基础设施的网络攻击

反映关键信息基础设施系统配置信息、核心软硬件设计信息、系统拓扑、应急预案、测评、监测、审计等情况的数据

- 可被利用实施对关键设备、系统组件供应链的破坏，以发起高级持续性威胁等网络攻击

政府或军工单位客户清单

未公开的重大漏洞

未公开的产品和服务采购情况

影响生态安全

- 反映自然环境、生产生活环境基础情况，或可被利用造成环境安全事件

未公开的土壤数据、气象观测数据、环保监测数据等

影响资源安全

- 反映水资源、能源资源、土地资源、矿产资源等资源储备和开发、供给情况

未公开的水文观测数据

未公开的耕地面积或质量变化情况

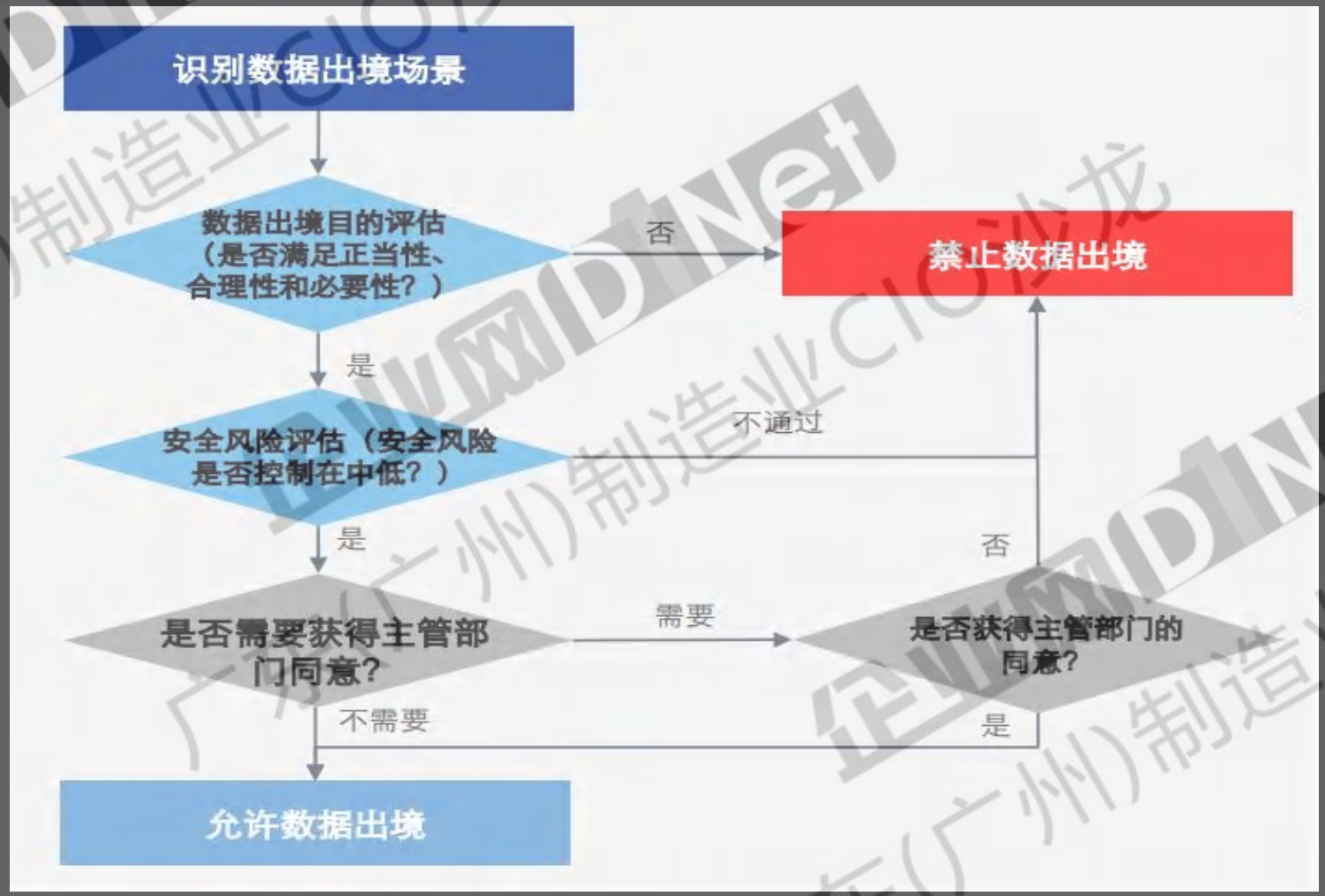
影响核安全

- 反映核材料、核设施、核活动情况，或可被利用遭破坏或其他核安全事件

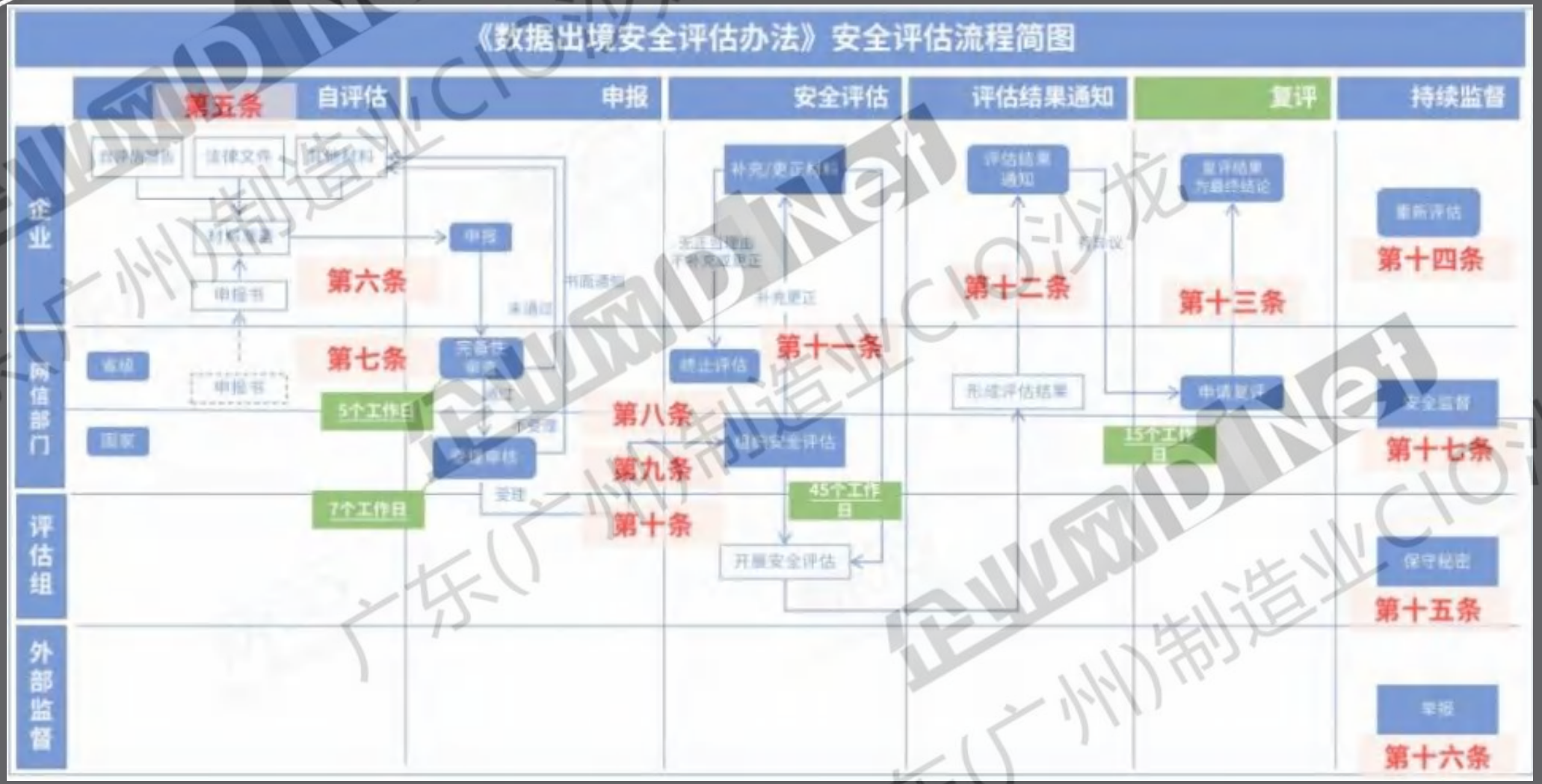
核电站设计图、核电站运行数据等

02 重要数据的界定

02 数据出境评估流程



02 数据出境评估流程

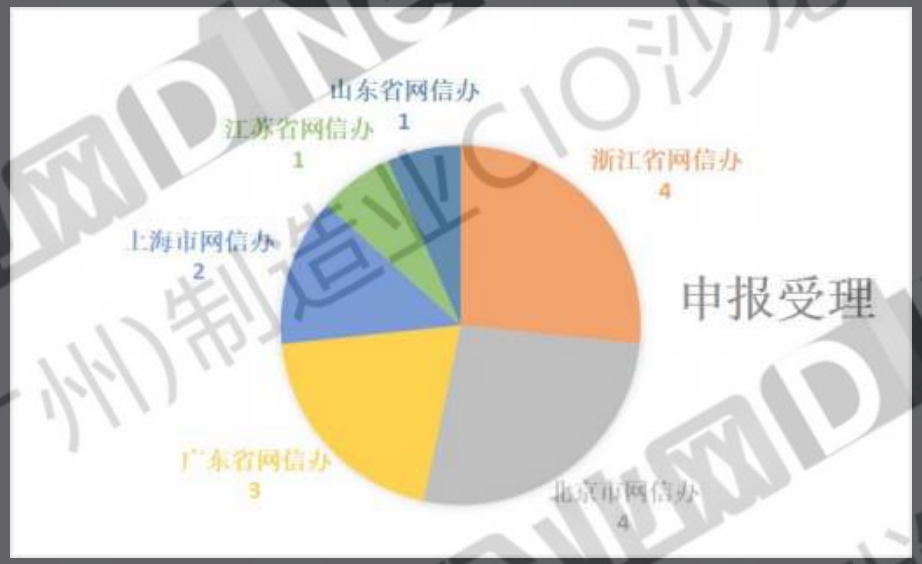


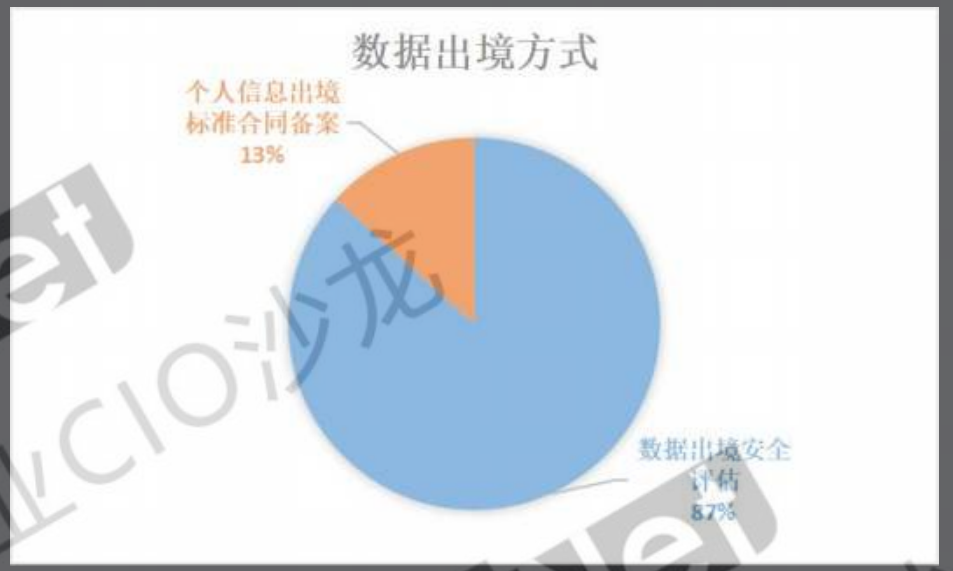
02 数据跨境违规处罚

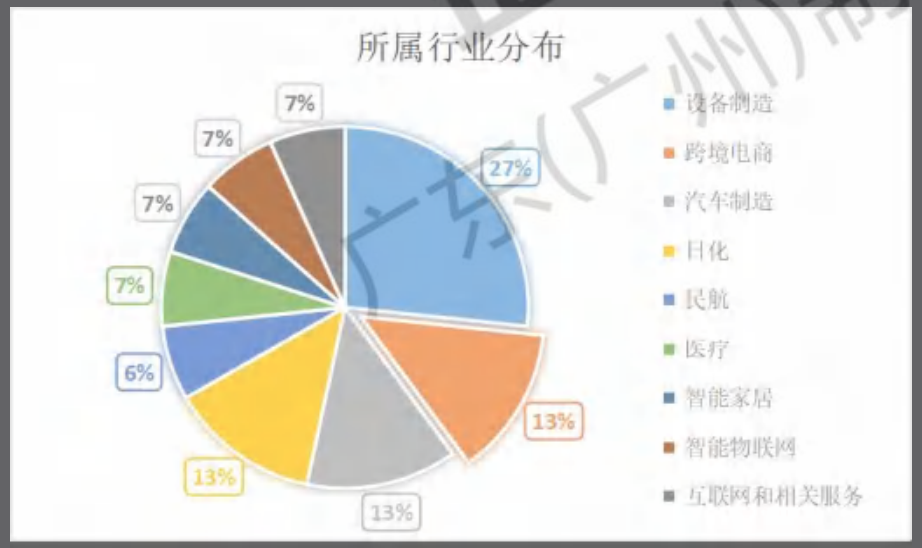
02 数据跨境合规审批现状

序号	企业名称	公布时间	申报受理
1	北京市友谊医院（与荷兰阿姆斯特丹大学医学中心合作研究项目）	2023年1月	北京市网信办
2	中国国际航空股份有限公司	2023年1月	北京市网信办
3	北京现代汽车有限公司	2023年5月	北京市网信办
4	马自达（中国）企业管理有限公司	2023年5月	上海市网信办
5	丝芙兰（上海）化妆品销售有限公司	2023年5月	上海市网信办
6	焦点科技股份有限公司（中国制造网外贸电商平台业务）	2023年5月	江苏省网信办
7	杭州海康威视数字技术股份有限公司	2023年5月	浙江省网信办
8	杭州萤石网络股份有限公司	2023年5月	浙江省网信办
9	支付宝（杭州）信息技术有限公司（跨境小程序业务相关数据）	2023年6月	浙江省网信办
10	安利(中国)日用品有限公司	2023年6月	广东省网信办
11	绿点科技（深圳)有限公司	2023年6月	广东省网信办
12	捷普电子（威海）有限公司	2023年6月	山东省网信办
13	捷普电子（广州）有限公司	2023年6月	广东省网信办
14	北京德亿信数据有限公司	2023年6月	北京市网信办
15	邦贝液压机械（杭州）有限公司	2023年7月	浙江省网信办

02 数据跨境合规审批现状





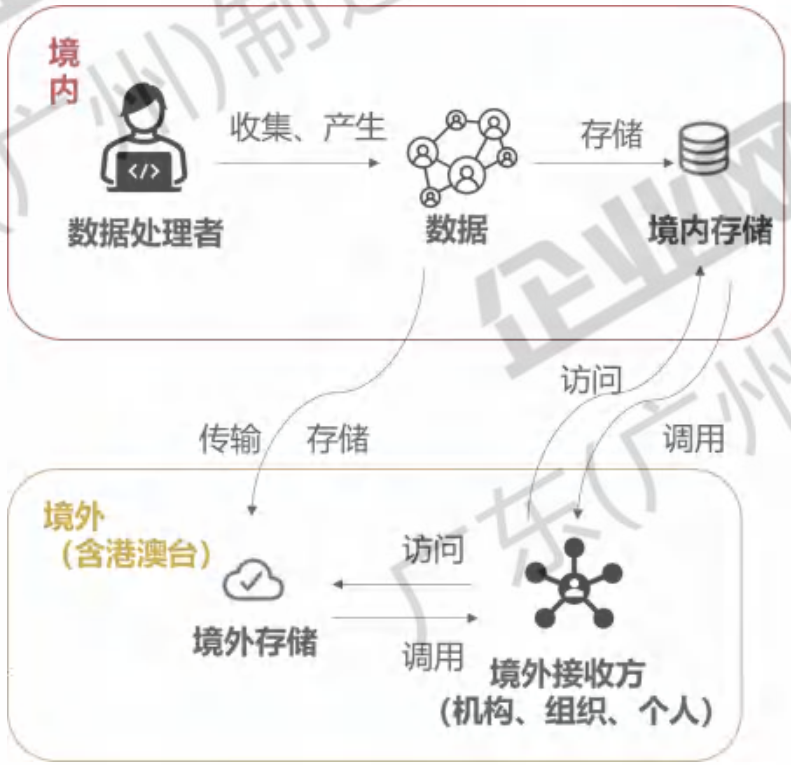


02 数据跨境合规的复杂性

02 数据跨境常见场景

02 数据跨境之“境”

“境”——司法管辖区域



情形一

境内主体向另一个位于境内的外资企业的办事处传输数据，是否属于“数据出境”？

情形二

数据没有传输也没有存储到中国境外的任何地方，但外资企业的境外主体可以访问、查看到这些数据，是否属于“数据出境”？

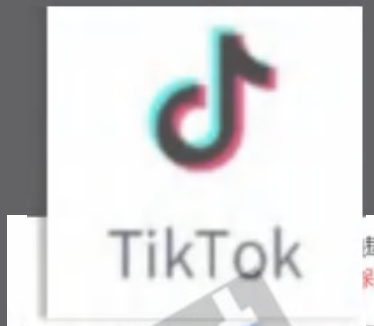
情形三

跨国企业内部的数据传输行为，是否属于“数据出境”？

03

个人信息合规

03 全球隐私违法处罚案例



Meta

2022年，爱尔兰数据保护局宣布Facebook母公司Meta未采用适当的技术和组织措施保护用户数据，违反GDPR，征收1700万欧元罚款。

2021年，挪威数据保护局通知Ferde公司处以500万挪威克朗罚款，该公司涉嫌非法向中国的数据处理者转移驾驶者个人信息。

03 全球隐私违法处罚案例

2022年7月21日，国家互联网信息办公室依据相关法律法规，对滴滴全球股份有限公司处人民币80.26亿元罚款，对滴滴董事长兼CEO程维、总裁柳青各处人民币100万元罚款。

经查明，滴滴公司共存在16项违法事实，归纳起来主要是8个方面。

一是违法收集用户手机相册中的截图信息1196.39万条；
二是过度收集用户剪切板信息、应用列表信息83.23亿条；
三是过度收集乘客人脸识别信息1.07亿条、年龄段信息5350.92万条、职业信息1633.56万条、亲情关系信息138.29万条、“家”和“公司”打车地址信息1.53亿条；
四是过度收集乘客评价代驾服务时、App后台运行时、手机连接桔视记录仪设备时的精准位置（经纬度）信息1.67亿条；
五是过度收集司机学历信息14.29万条，以明文形式存储司机身份证号信息5780.26万条；
六是在未明确告知乘客情况下分析乘客出行意图信息539.76亿条、常驻城市信息15.38亿条、异地商务/异地旅游信息3.04亿条；
七是在乘客使用顺风车服务时频繁索取无关的“电话权限”；
八是未准确、清晰说明用户设备信息等19项个人信息处理目的。

此前，网络安全审查还发现，滴滴公司存在严重影响国家安全的数据处理活动，以及拒不履行监管部门的明确要求，阳奉阴违、恶意逃避监管等其他违法违规问题。滴滴公司违法违规运营给国家关键信息基础设施安全和数据安全带来严重安全风险隐患。因涉及国家安全，依法不公开。

03 全球隐私违法处罚

1、全球隐私保护立法越来越多且罚款高昂（2%-5%）；欧盟提出NIS指令2.0和 网络弹性法案草案，电子产品网络安全成为产品必须满足的法定要求；

2、中国网络空间三驾马车（网络安全法、数据安全法、个人信息保护法），个保法高额罚款时代来临（滴滴82亿）；

3、高风险业务领域（如服务算法、AI、儿童隐私保护、生物识别、广告业务、 监控场景、跨境传输等）执法频发，面临高额罚款和集体诉讼风险；

4、欧洲、美国、中国是执法高发区域，罚款金额持续攀高；

5、隐私保护在美国被上升为国家安全，与政治风险混同。

03 全球制定了隐私立法的国家

03 全球主要隐私法律概述

1. 欧盟的《通用数据保护条例》，实施强治性措施（发布禁令、命令删除数据、撤回认证）、以及极具威慑力的行政处罚

2. 美国的《加州消费者隐私法》《儿童在线隐私权保护法》，规定了高昂的罚款上限，程序性设计更具有合理性，在行政罚款和私人诉讼中都规定了改正期（cure period）制度

3. 中国的《个人信息保护法》《数据出境安全评估办法》，进一步规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动

03 全球主要隐私法律比较 个人信息

	GDPR（第四条）	中国《个人信息保护法》（第四条）	加州隐私法（CCPA&CPRA）（第1798.140条（v）项）
定义	与任何已识别或可识别的自然人（“数据主体”）**相关**（relating to）的信息	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**	直接或间接地识别、关联、描述、能够**合理地**与某一特定消费者或家庭相关联**或可以合理地与之相关联的信息。**
列举类型	姓名 身份编号 地址数据 网上标识 自然人所持有的一项或多项身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份	无列举	识别码 生物识别信息 地理位置数据 专业或就业相关信息 受保护的特征 网络活动信息 用户画像的推论 商业信息 教育信息
排除	匿名化信息[31]	匿名化信息	1.去识别化信息 2.汇总的消费者信息 3.可公开获取的信息 4.合法获得的、引起公众关注的真实信息[32]

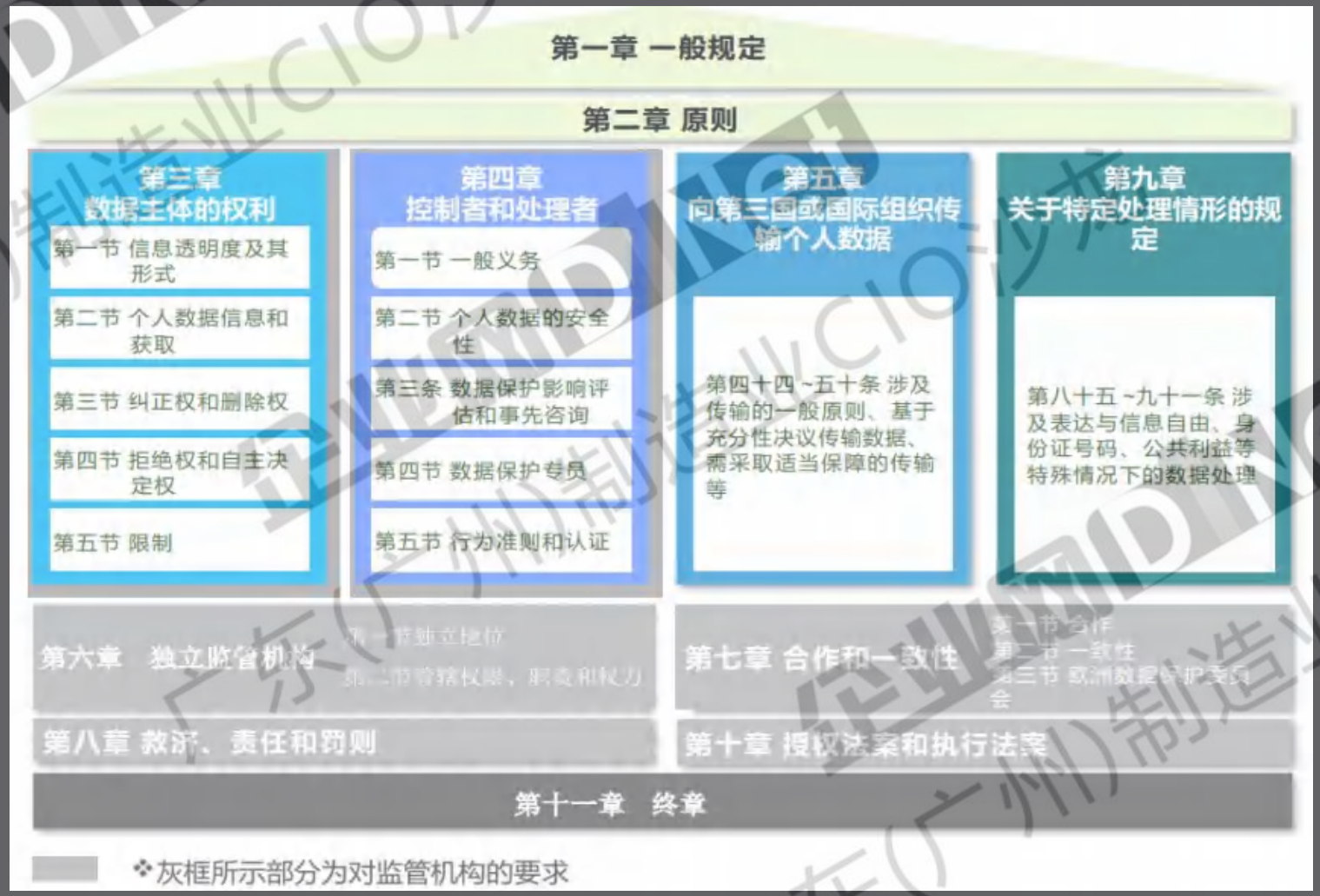
03 全球主要隐私法律比较 个人敏感信息

	GDPR（第九条）	中国《个人信息保护法》（第二十八条）	加州隐私法（CCPA&CPRA）（第1798.100条）
敏感信息定义	特殊类型数据（无概括性定义）	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[33]。	列举"敏感个人信息"类别（无概括性定义）
敏感信息列举	种族或民族背景	特定身份	人种与民族信息
	工会成员的个人数据		工会会员身份
			社会保障、驾驶执照或护照号码
			个人通讯
	政治观念		
	宗教或哲学信仰	宗教信仰	宗教信仰
	基因数据	生物识别	遗传数据
	为了特定识别自然人的生物性识别数据		生物特征
	和自然人健康相关的数据	医疗健康	健康信息
	和个人性生活或性取向相关的数据		有关性生活或性取向的信息
		金融账户	财务账户信息
		行踪轨迹	精确的地理位置
		不满十四周岁未成年人的个人信息	

03 全球主要隐私法律比较 敏感信息处理

	GDPR（第九条）	中国《个人信息保护法》（第二十八条）	加州隐私法（CCPA&CPRA）（第1798.100条）
处理的要求	特定情况下可以处理： 1.数据主体明确同意 2.处理对于数据控制者履行责任、保护数据主体权利、另一自然人的核心利益是必要的 3.非盈利机构的正当性活动 4.已经明显公开的相关个人数据的处理 5.司法活动 6.公共利益（包括医学、公共健康、科学或历史研究）	处理必须具有特定的目的和充分的必要性，并采取严格保护措施	
可公开获取的敏感个人信息		在合理范围内处理个人自行公开或者其他已经合法公开的个人信息不适用同意规则[34]	可公开获取的敏感个人信息不再是敏感个人信息或个人信息[35]，因此不适用相关的处理规则
同意规则	明确同意	取得信息主体的单独同意或书面同意[36]	无规定
自动化决策	只有在数据主体明确同意或者处理是对实质性公共利益是必要的情况下，才能利用此类数据进行对数据主体具有法律影响或类似严重影响的自动化决策。[37]	无规定	无规定
其他	无规定	法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的,从其规定。[38]	无规定

03 欧盟GDPR主要内容



03 欧盟GDPR核心7原则

03 欧盟GDPR核心要求

RDT
当事人权利

当事人可行使的权利

个人具有将其数据删除的权利、访问权、更正权、限制处理权、反对权、携带权，反对自动化决策权等权力。

IA
告知

收集和处理当事人个人信息需告知并获取其同意

组织必须在告知个人的隐私声明中提供数据收集、使用和共享相关安全控制信息。

PBD
默认的隐私保护

从产品/服务设计的初的安全控制措施

组织从设计系统开始就应包含隐私数据保护的应用，而再不是追溯性的补充性应用。

PR
处理者

第三方服务供货商安全管理

代表组织处理个人信息的供货商和其他组织必须采取适当的技术和组织性措施已达到GDPR需求。

DS&RP
数据安全与处理活动记录

个人信息的安全与处理活动记录维护

组织需考虑采用安全措施（如去对个人信息进行识别化或去连结化处理）以保证数据的安全水平，同时保留数据处理记录。

NP
信息泄露通知

将在72小时内发出违规通知

数据外泄必须在没有过度延迟的情况下通知相关监管机关，并不迟于72小时通知。必要时也需通知当事人。

DPIA
隐私保护影响评估

DPIA

当新的业务流程或系统上线时，组织需执行或重新检视隐私数据影响评估（DPIA），以便发现和降低风险。

DPO
数据保护官

数据保护官

组织需指派一个或多个具有隐私法和实务专业知识的数据保护官参与所有涉及个人信息保护的问题。

TP
跨境数据传输

跨境数据传输

BCRs制定了原则和可执行权利，并在国际集团公司内采取适当的保护措施。

RLP
救济、责任与罚则

欧盟成员国DPA监管罚则

成员国将依据GDPR起草和生效适用本国数据保护法案和惩罚措施。

03 美国加州消费者隐私法CCPA

一、立法背景

该法案是加州立法机关对于1972年加州宪法修正作出的响应，该修正将隐私权列入加州居民的基本权利之一，以保障个人得以控制对其自身信息的使用及交易。

二、保护客体

该法案的保护客体为加州自然人居民的个人信息。该法案对个人信息的定义比加州其他的法律都要更广泛，是指“能够识别、关联、描述以及能够与特定消费者或家庭关联或合理关联的信息。”

三、适用对象

该法案适用于在加州开展业务而收集消费者个人信息的营利性企业，包括个人独资企业、合伙企业、有限责任公司、公司、协会，或其他为其股东或其他所有者的利益或经济利益而组织或经营的法律实体，或是收集该资料的代表机构，并且符合以下一项或多项条件：

（1）年总收入超过2,500万美元；

（2）每年单独或与其他企业共同购买、接收、共享或出售超过50,000个消费者、家庭或设备的个人信息；

（3）年营收的50%或以上来自销售消费者个人信息。

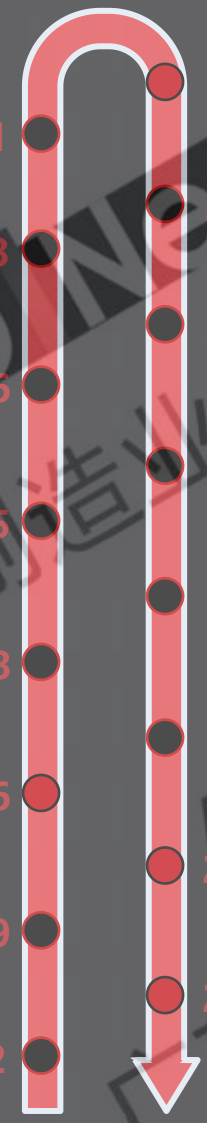
四、消费者的救济权利

该法案对消费者隐私权最重要的保护在于它为消费者提供了一系列金钱经济和非金钱的法律救济，从而使得非法搜集和使用个人信息的企业将面临更大的赔偿。同时，在个人信息领域一旦被消费者起诉，企业极可能面临由为数众多的消费者发起的集体诉讼。

五、执法机关及惩罚

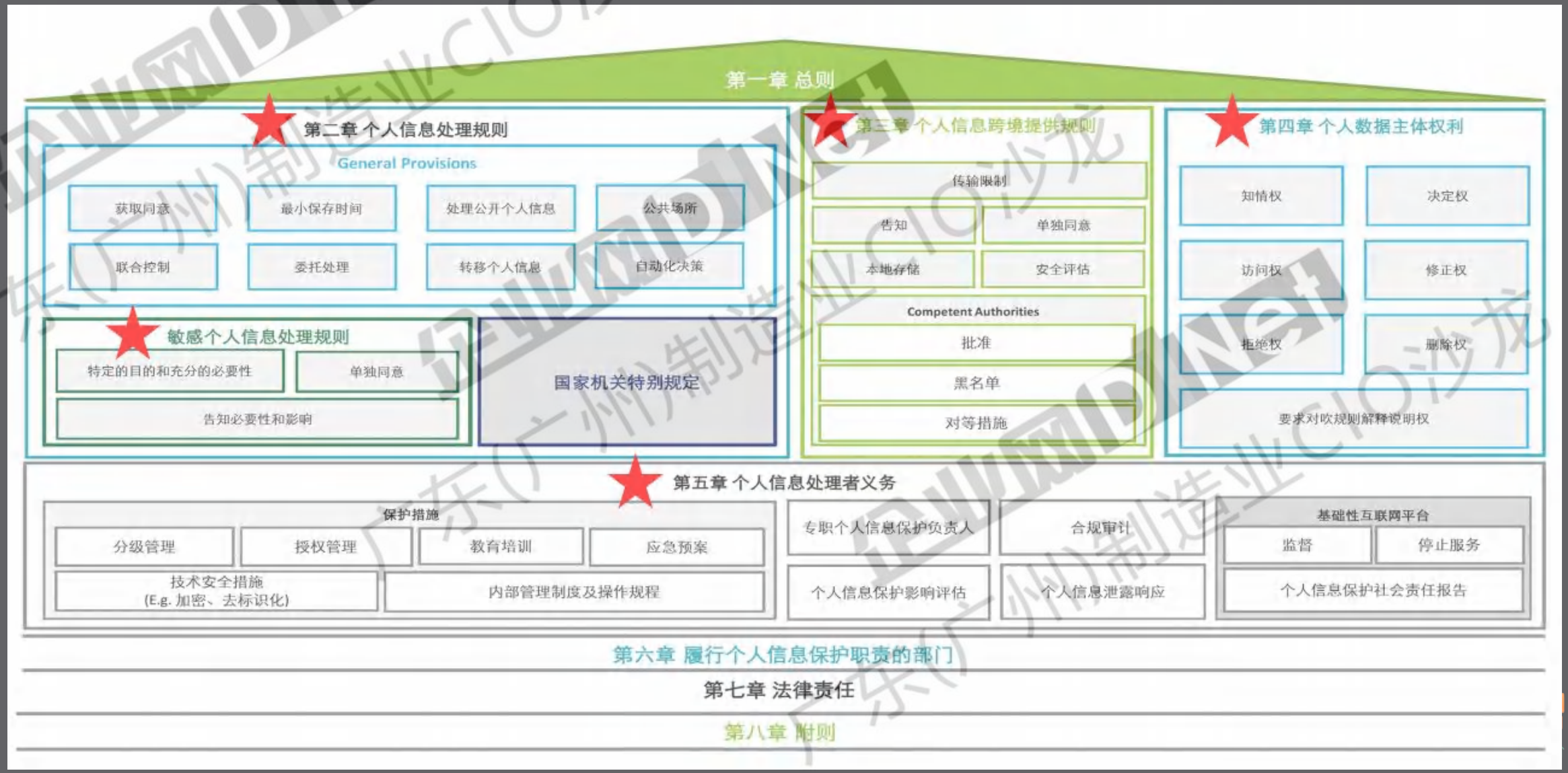
该法案将主要由加州司法部长负责监管与执行。对于违反该法案的每一项行为，罚款最高可达7,500美元/次。

03 我国个人信息保护立法沿革



- 2012.12 本全国人民代表大会常务委员会关于加强网络信息保护的决定
- 2013.09 电信和互联网用户个人信息保护规定
- 2017.06 《网络安全法》
- 2017.08 信息安全技术 数据出境安全评估指南（征求意见稿）
- 2019.05 数据安全管理办法（征求意见稿）
- 2019.06 个人信息出境安全评估方法（征求意见稿）
- 2019.08 信息安全技术 移动互联网应用程序（APP）收集个人信息基本规范（征求意见稿）
- 2019.11 APP违法违规收集使用个人信息行为认定方法
- 2020.01 《密码法》
- 2020.01 信息安全技术 个人信息告知同意指南（征求意见稿）
- 2020.02 国家政务信息化项目建设管理办法
- 2020.06 网络安全审查办法
- 2020.08 信息安全技术 网络数据处理安全规范（征求意见稿）
- 2020.10 GB/T 35273-2020信息安全技术 个人信息安全规范
- 2021.09 《数据安全法》
- 2021.11 《个人信息保护法》

03 我国个人信息保护法主要内容



03 个人信息处理原则

前提条件

1.取得个人同意

2.为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需

3.履行法定职责或义务必需

4.突发紧急应对必需

5.为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息

6.自行公开或其他已合法公开的

7.其他情形

具体要求	
明示同意	充分知情、自愿明确
授权同意	法定单独或书面同意
重新取得同意	变更需重新同意
撤销权	个人有权撤回其同意

*注：第2-7项规定情形的，不需取得个人同意

个人信息保存期限以最短必要为原则

以最短必要为原则

根据必要性的要求，规定在满足处理目的后，最短时间内尽快予以删除。需要企业制定相应内部合规制度，就个人信息的存储及删除时间进行明确规定。

兜底条款

对个人信息保存期限另有规定的，从其规定。

告知要求

- 个人信息处理者的名称或者姓名和联系方式;
- 个人信息的处理目的、处理方式和处理的个人信息种类、保存期限;
- 个人行使权利的方式和程序;
- 其他法定告知事项。

两种例外情形：

法定保密或豁免告知第一款

紧急情况 事后告知

*针对第一种情形，最为典型的是根据《中华人民共和国反恐怖主义法》第五十一条的规定，即公安机关在调查恐怖活动的案件中，可以获得事先告知豁免。

03 个人信息处理规则

不得过度收集个人信息

有利于规范个人信息的收集活动

禁止数据歧视

数据质量引发的歧视

对大数据运用质量不高而造成的数据歧视形成制约，将个人信息质量作为法定义务，有助于督促个人信息处理者提升数据获取的准确度。

算法引发的歧视

- 不得实行不合理差别待遇
- 便捷拒绝
- 说明义务

人力资源管理纳入范围

人力资源管理具有隶属关系场景特殊

撤回同意便捷化

基于个人同意而进行的个人信息处理活动，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

未成年人信息归入敏感信息

明确了**只要涉及儿童的个人信息均以个人敏感信息的标准进行保护**，体现了法律对于儿童个人信息保护的重视。

告知同意与例外

体现了个人信息处理者在处理前的告知义务以及取得同意的前提条件

例外情形

- 合同必需
- 处理人力资源事项
- 法定责任
- 紧急情况
- 合理处理已公开信息
- 公共利益的报道与监督
- 用于维护公共安全

国家机关的特别规定

国家机关作为**特殊个人信息处理者**不得超出履行法定职责所必需的范围和限度。

03 个人敏感信息处理规则

个保法对于个人敏感信息的定义

1. 种族、民族、宗教信仰
2. 个人生物特征
3. 医疗健康、金融账户
4. 个人行踪等

处理个人敏感面临的主要挑战:

个人敏感信息识别

动态的识别各个不同业务中的个人数据、个人敏感数据，标识不同种类和级别数据，尤其是个人敏感信息

个人敏感信息的流动监测

个人敏感信息在不同业务之间的流动情况监测；在不同API接口中调用的情况；在不同web页面中的展示情况

个人敏感信息出境

网信安全评估、个人信息保护认证；
个人信息处理活动达到本法规定的个人信息保护标准；

行使个人享有的权利

知情权、决定权、拒绝权、删除权

个人敏感信息保护

个人敏感信息匿名化算法
个人敏感信息访问控制

个人敏感信息存储

个人敏感信息分级分域存储

03 个人信息处理者的义务

1. 义务执行依据：

个人信息处理目的、处理方式、信息种类及个人权益的影响、潜在风险等；

2. 义务执行目的：

符合法律、行政法规的规定，并防止未授权访问及个人信息泄露、篡改、丢失。

义务说明

- 安全技术措施采用
  - **安全措施说明：**
    1、加密：对数据进行密码变换以产生密文的过程（GB/T 39786-2021）
    2、去标识化： 去标识化建立在个体基础之上，保留个体颗粒度，采用假名、加密、哈希函数等替代对个人信息的标识（GB/T 35273— 2020）
- 制度规程制定
- 应急预案制定
- 信息分类管理
- 内部人员管理
  - 操作**权限确定**
  - 定期教育培训
- 法定其他措施

- 安全负责人指定
  - **需指定负责人情形：**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
- 机构设立/代表指定/报送义务
  - **适用情形：**境外个人信息处理者
- 定期合规审计
- 事前个人信息保护影响评估
  - **适用情形：**
    - 敏感信息处理
    - 自动化决策
    - 委托、提供、公开 境外提供
    - 其他有重大影响
  - **内容要求：**
    合法、正当、必要
    个人权益影响及安全风险
    合法性、有效性、匹配性
    报告和记录至少保存三年
- 事后事项通知

通知内容

情形条件

1、个人信息遭受泄露、篡改、丢失；
2、相关部门提出要求。

通知个人

1、豁免条件：采取措施能有效避免危害的发生，可以不通知个人；
2、限制条件：相关部门认为可能造成危害的，有权要求通知个人。

03 个人信息保护法罚则

法律责任

《个人信息保护法》法律责任的***最高罚款限额5000万人民币***或者5%的年营业额，与《网络安全法》最高罚款限额100万对比，大幅度提高了个人信息处理者的违法成本，显示了国家对于保护个人信息的重视程度。

与《网络安全法》、《数据安全法》相同，《个人信息保护法》也规定了对于“***直接负责的主管人员***”和“***其他直接责任人员***”的罚则，金额最高100万。可见责任具体到个人，从反面促进个保法的贯彻落实。

以及对于违法程度轻重不同，规定了多元化的处罚措施，并针对一般违法和情节严重的违法进行了区分。

明确了侵权行为民事责任确定的具体方式，并考虑到个人信息领域个人举证存在举证困难，确立了***推定过错***的损害赔偿责任，即信息处理者若不能举证自己无过错的，则需承担损害赔偿责任。

将个人信息纳入可提起***公益诉讼***的范畴，个人信息处理者所面临的诉讼风险提高。

类型	行为	罚则
行政	违法处理，或未履行法定保护义务	责令改正，警告，没收违法所得
	违法APP	**暂停或终止服务**
	拒不改正	100万以下罚款 责任人罚1-10万
	情节严重	没收违法所得 5000万以下或上年度**营业额5%** 停业 责任人罚10-100万
民事	损害个人权益	赔偿
刑事	犯罪	刑事责任

附则

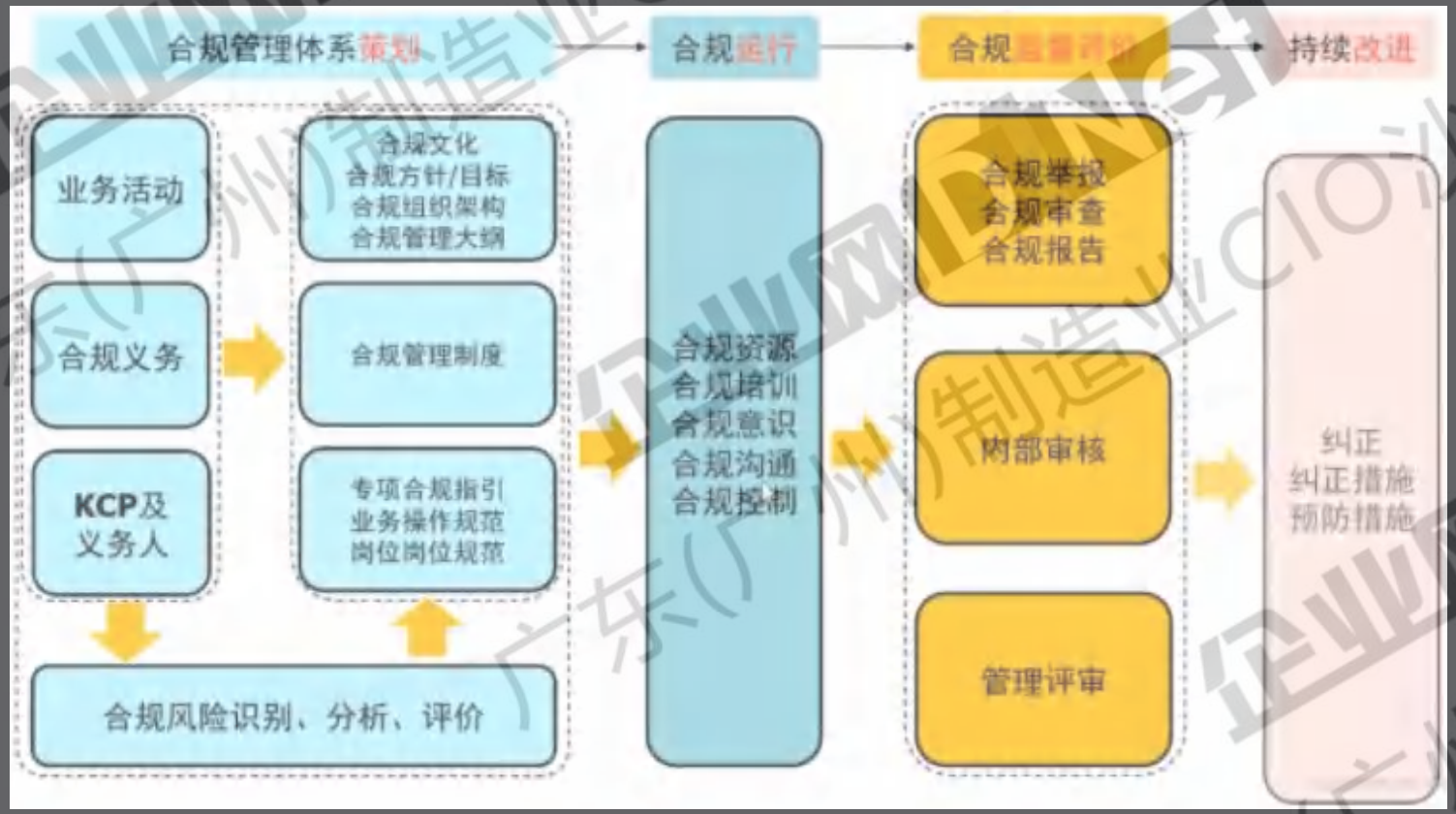
第七十二条规定自然人因个人或者家庭事务处理个人信息的，不适用本法。

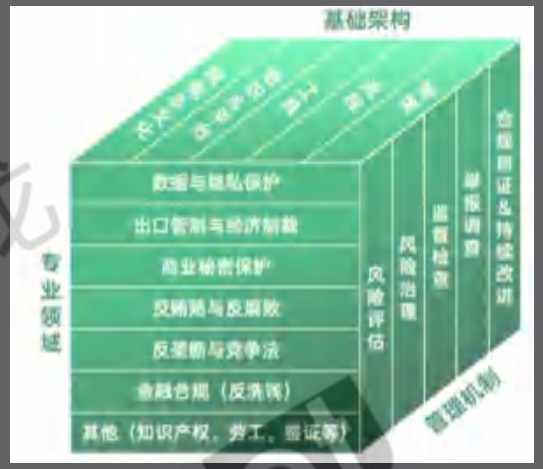
法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

04 合规应对策略

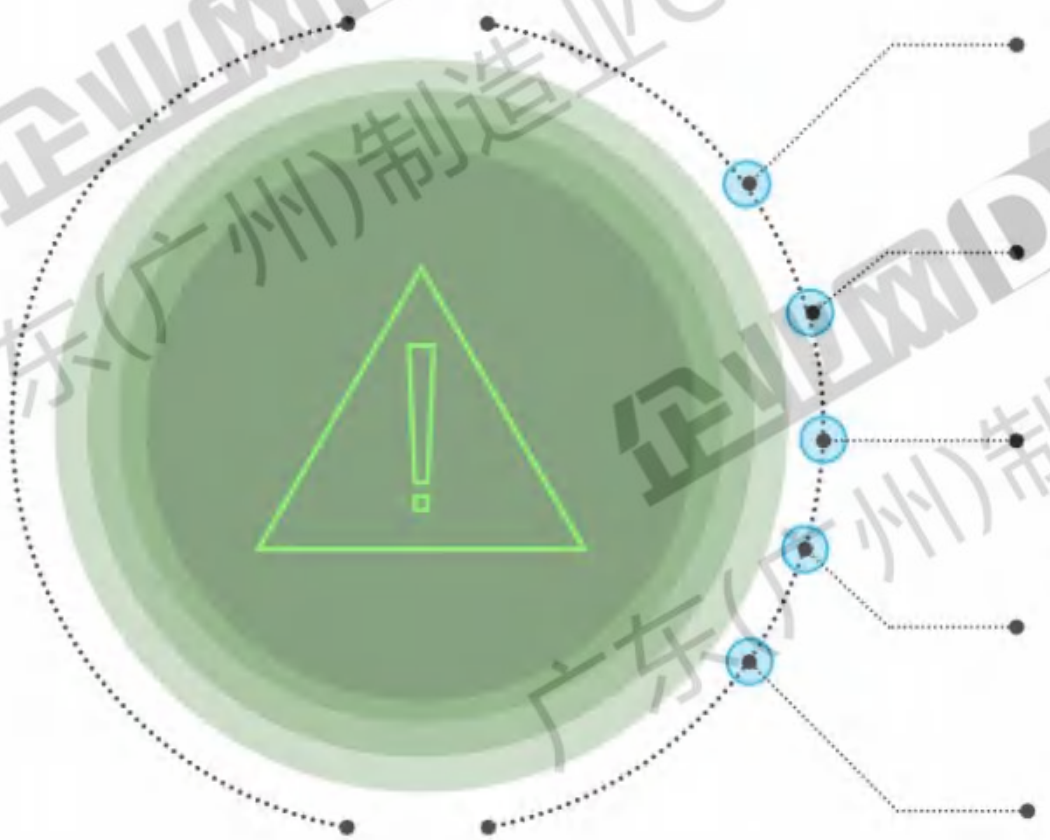
04 合规管理体系：ISO37301标准

04 企业合规管理体系





04 推行企业合规管理工作



境外法律体系

企业出海前应通过专家咨询、实地考察等方式，详细了解目标国家的法律体系，对企业出海法律风险进行全面评估

境内法律规定

我国境内对外汇管理、数据跨境等存在一系列规定，企业应分析境内相关法律法规要求，明确限制条件，准备应对方案。

目标企业调查

如企业出海过程中涉及跨国并购，应通过专业机构充分调查目标企业状况，防止信息不对称风险。

合同审查管理

企业应加强对合同的审查和管理，对合同条款明确、细化，防止合同法律风险。

人才配备

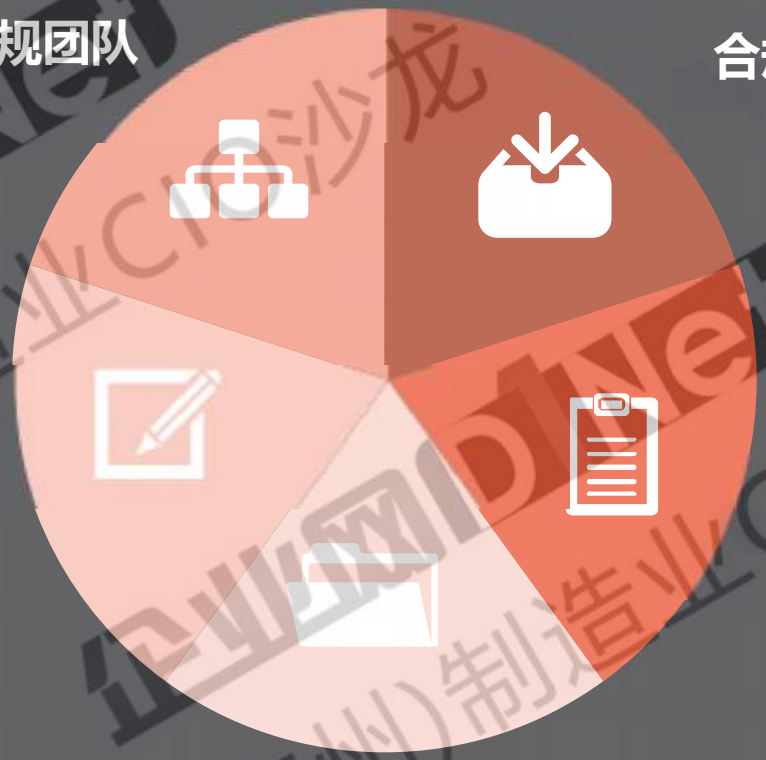
企业应针对各类合规风险，配备各领域专业人才。

04 内部及外部的合规面向主体的关系

04 企业数据合规管理

- **前提**：合法 、正当 、必要
- **原则**：HOW>NO
- **做法**：依法申报、合规治理

企业数据合规体系搭建



- 专门的数据合规团队
- 建流程、跨部门合作
- 数据分类、风险定级
- 确定职责、责任到人
- 合规落地、监督反馈

04 明确个人信息保护工作方针

个人敏感
数据管理

个人信息识别

静态识别+动态识别+变化感知
信息如何流转，系统之间的关联

个人信息备案

资产、信息的备案
权限、信息调用的备案

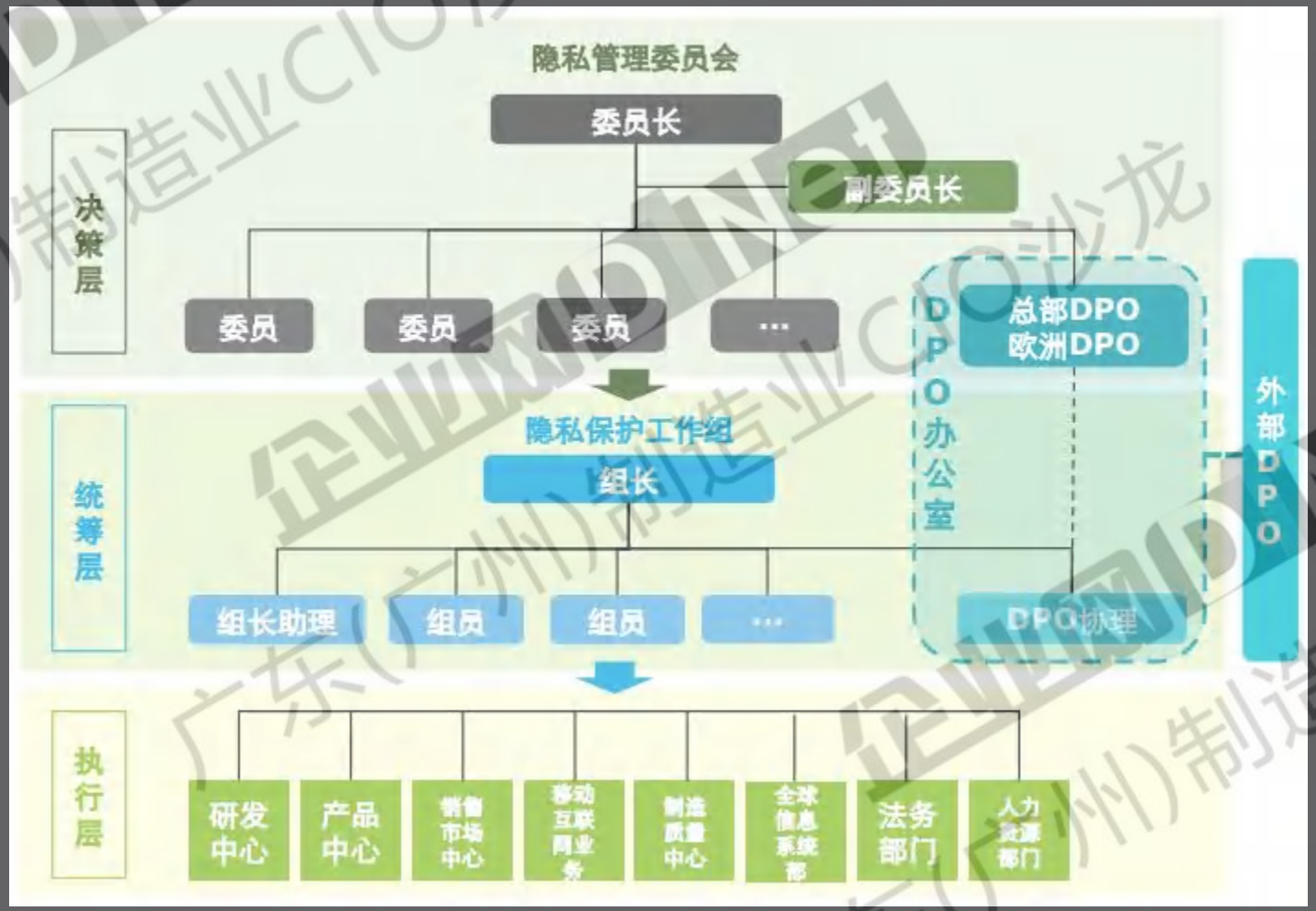
个人信息分类分级

数据分类分级
同步完成个人金融信息分类分级
数据标签化，清单输出、接口输出

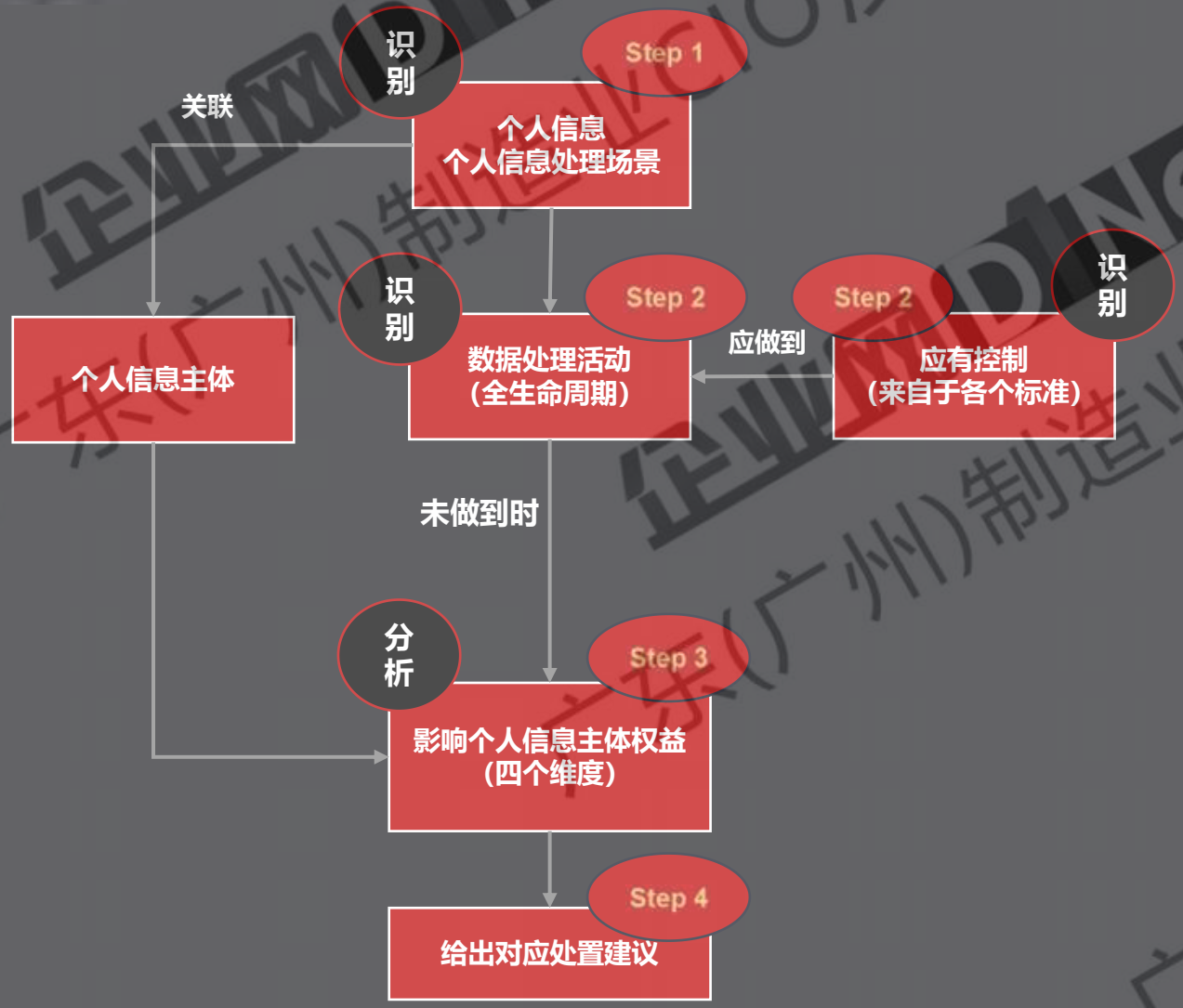
个人信息使用监测

不同业务人员的使用监测
不同运维人员使用监测
各类业务访问监测

04 建立个人信息保护角色职责



03 开展个人信息安全影响评估



- **Step 1：**识别个人信息处理场景，识别各个场景下的个人信息字段、数据量、涉及的第三方等，同时分析所对应的**个人信息主体**是否存在需特别考虑的**群体特征**。
- **Step 2：**识别各个个人信息处理场景下的数据处理活动（收集、存储、传输、使用、第三方交互等）；同时根据各个标准、法律法规、发文要求，识别在个人信息处理活动下**应有的控制要求**。
- **Step 3：**分析对各个处理活动的控制是否能满足应有控制的要求，**如不满足**，则对相应的个人信息主体造成了何种**权益影响**（四个维度）。
- **Step 4：**针对“**对个人信息主体造成中、高级别影响的处理活动**”给出处置建议。

04 建立隐私管理体系框架

04 完善隐私管理技术框架

安全运营

数据资源安全运营
- 数据资源稽核
- 数据地图

数据安全策略运营
- 规范标准库
- 安全策略稽核

数据安全事件运营
- 安全事件监测
- 安全事件处置
- 数据流转视图

数据安全风险运营
- 风险可视化
- 风险分析
- 风险感知

数据安全管控能力

数据资源管理
- 数据特征管理
- 数据资源清单
- 数据资源备案
- 分类分级管理
- 数据资源统计

安全策略管理
- 分类分级策略
- 数据加密策略
- 数据资源发现策略
- 数据水印策略
- 敏感数据识别策略
- 数据防护策略
- 风险监测策略
- 任务管理
- 数据脱敏策略
- 标准规范管理

风险事件监测

接口访问
- 访问数据内容
- 敏感数据访问
- 接口备案
- 访问频率

业务区域
- 异常访问行为
- 越权访问
- 高频访问
- 超量访问

数据生命周期
- 数据采集过程监测
- 数据处理过程监测
- 数据传输过程监测
- 数据交换过程监测
- 数据存储过程监测
- 数据删除监测

风险分析
- 接口访问分析
- URL访问分析
- 业务用数分析
- 开发测试分析

运行监控
- 组件运行状态监测
- 安全能力监测
- 平台日志检索
- 安全能力测试

基础安全能力

网络安全
- 防火墙
- 防病毒
- 入侵监测
- 防DDOS
- 网络审计
- 主机WAF
- 日志分析
- 网络DLP
- WAF
- 网络隔离

数据安全
- 数据库审计
- 数据库防火墙
- 传输加密
- 数据脱敏
- 数据水印
- 文件水印
- 数据发现和分类分级
- 数据库加密
- 屏幕水印
- 数据运维管控
- 文件系统加密
- 网页水印

应用安全
- API网关
- API应用审计
- 应用动态脱敏
- 网页防篡改

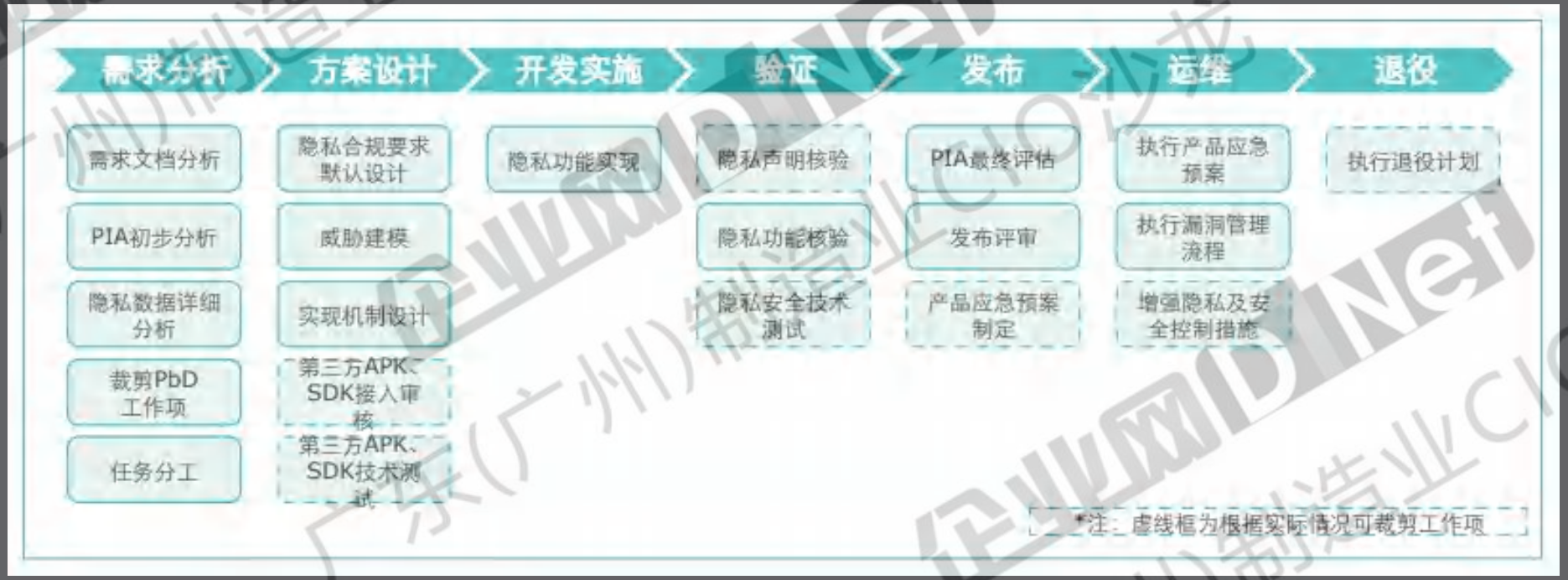
隐私计算
- 多方计算
- 联邦学习
- 差分隐私
- 可信环境

终端安全
- 身份认证
- 终端DLP
- 权限和准入控制
- 邮件DLP
- 移动存储管理
- 敏感数据监控
- 终端网络管理

数据安全监控和运营

基础监测和防护

04 建立隐私默认设计（PbD）原则



04 核心技术手段支撑：加密、脱敏、水印

04 强化隐私事件应急处置能力

- 主动识别个人信息，准确分类分级
- 使用机器学习技术提升工作效率

- 从外发通道管控、计算环境隔离、重要操作审计留痕、数据脱敏等环节入手，覆盖个人信息生命周期中的采集、存储、使用、传输、共享、销毁等各环节
- 使用UEBA技术分析用户各类操作行为，对高价值数据的流动及访问进行自动化风险识别和告警

- 使用水印、录屏等技术进行数据标记和操作留痕
- 备份外发文件，保留关键证据

04 建设全方位的数据合规机制

建立全球化的信息安全治理框架

信息安全政策制定
全球信息安全团队
全球风险评估

制定符合当地法律法规的合规措施

法律团队支持
合规流程建设
隐私政策透明

与三方律所建立合作伙伴关系

专业法律咨询
风险评估与预警
法律文件准备
合规培训与指导

加强员工培训与意识教育

安全培训计划
模拟钓鱼演练

与第三方供应商建立合作伙伴关系

供应商安全审查
合同条款明确

加强威胁情报与漏洞管理

威胁情报共享
漏洞管理与修复

2023

制造业CIO出海系列沙龙

谢谢观看！

宣讲人：刘歆轶　公司：非夕机器人

企业网DINet 企业IT第1门户

信众智 CIO智力输出及社交平台