阿里云 | Deloitte.

行稳致远：
中国企业海外业务数据合规指导书

阿里云出海能力中心 | 德勤中国

阿里云 | Deloitte.

目录
Contents

1 中企出海的主要合规场景

1.1 中企出海面临的主要合规挑战 02
1.2 隐私保护与数据安全 02

2 中企出海数据合规建议框架

2.1 评估规划 04
2.2 人员组织 04
2.3 流程制度 05
2.4 技术方案 07
2.5 持续运营 08
2.5.1 数据保护分类分级 08
2.5.2 数据合规报备 09
2.5.3 数据保护影响评估和个人信息安全工程运营（PbD） 09
2.5.4 个人信息主体权利行使运营 09
2.5.5 数据保护事件响应和应急管理 09

3 云平台能力保障出海数据合规

3.1 云平台合规能力 10
3.2 阿里云对于云上客户的隐私保护 14
3.3 云平台安全能力 15
3.3.1 数据保护分类分级 15
3.3.2 数据合规报备 15
3.3.3 数据保护影响评估和个人信息安全工程运营（PbD） 16
3.3.4 个人信息主体权利行使运营 16

4 全球主要数据合规法规与建议

4.1 欧盟 18
4.1.1 GDPR简介 18
4.1.2 GDPR基本原则 18
4.1.3 数据主体的权利 19
4.1.4 数据控制者和数据处理者的责任 19
4.1.5 GDPR处罚 20
4.1.6 GDPR合规主要关注点 20
4.1.7 GDPR合规建议 22
4.1.8 常见问题 23
4.2 东南亚 23
4.2.1 新加坡PDPA简介 24
4.2.2 新加坡PDPA合规主要关注点 25
4.2.3 新加坡PDPA合规建议 26
4.2.4 泰国PDPA合规概览 26
4.2.5 常见问题 27
4.3 北美 28
4.3.1 美国数据合规相关立法 28
4.3.2 美国数据合规主要关注点 29
4.3.3 数据合规建议 30
4.3.4 常见问题 30
4.4 日韩 31
4.4.1 日本数据合规相关立法 31
4.4.2 日本数据合规主要关注点 31
4.4.3 日本数据合规建议 32
4.4.4 日本数据合规常见问题 32
4.4.5 韩国数据合规主要立法 33
4.4.6 韩国数据合规主要关注点 33
4.4.7 韩国数据合规建议 34
4.4.8 韩国数据合规常见问题 34
4.5 印度 35
4.5.1 印度数据合规相关立法 35
4.5.2 印度数据合规主要关注点 35
4.5.3 印度数据合规建议 36
4.5.4 常见问题 36
4.6 南美 36
4.6.1 巴西数据合规主要立法 36
4.6.2 巴西数据合规主要关注点 37
4.6.3 巴西数据合规建议 37
4.6.4 阿根廷数据合规概览 38
4.6.5 常见问题 38
4.7 澳新 39
4.7.1 澳大利亚数据合规主要立法 39
4.7.2 澳大利亚数据合规主要关注点 40
4.7.3 阿里云数据合规建议方案 41
4.7.4 常见问题 41
4.8 中东区域 42
4.8.1 沙特数据合规主要立法 42

Contents

Contents

4.8.2 沙特数据合规主要关注点 42
4.8.3 沙特数据合规建议 43
4.8.4 阿联酋数据合规主要立法 43
4.8.5 阿联酋数据合规主要关注点 43
4.8.6 阿联酋数据合规建议 44
4.8.7 常见问题 44
4.9 海外各国数据本地化与DPO要求小结 45

5 出海企业数据合规体系化能力建设

5.1 数据合规体系建设基础 47
5.1.1 强化全员合规意识 47
5.1.2 理解数据全生命周期 47
5.1.3 定期进行风险度量 48
5.2 管控内外部数据使用 48
5.2.1 明确数据使用角色 49
5.2.2 设计数据使用授权 50
5.2.3 业务数据访问控制 50
5.2.4 通过云产品实现数据权限管理 53
5.2.5 办公数据访问与保护 53
5.3 数据生产与采集 54
5.3.1 数据采集与生产合规 55
5.3.2 场景举例 55
5.4 数据分类与分级处理 57
5.4.1 数据分类 57
5.4.2 数据分级 59
5.4.3 数据分类分级建议 59
5.4.4 敏感数据监督 60
5.4.5 云产品实现数据分类分级 60
5.5 数据存储与传输 62
5.5.1 数据存储合规 63
5.5.2 数据非跨境传输 64
5.5.3 数据跨境传输 65
5.6 规范数据加工与开放 65
5.6.1 数据加工合规 65
5.6.2 数据开放 67
5.6.3 构建可信计算 67
5.7 合规审计与风险度量 68
5.7.1 在线审计 68
5.7.2 离线审计 69
5.7.3 配置审计 69
5.7.4 操作审计 70
5.8 使用数据合规工具与技术 70
5.8.1 源头审计 70
5.8.2 跨境过滤 71
5.8.3 流程管控 71
5.8.4 数据过滤 72
5.8.5 数据删除与恢复 73

6 阿里云全球合规生态能力

6.1 阿里集团合规实践方案 76
6.2 全球合规生态资源 76
6.3 德勤咨询服务 79

7 参考资料

Contents

Contents

阿里云出海能力中心&德勤中国

ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

中企出海的主要合规场景

1.1 中企出海面临的主要合规挑战

1.2 隐私保护与数据安全

01 中企出海的主要合规场景

中国经济已经步入高质量发展的新时代。立足于经济转型升级需求，中国企业出海已经不仅是个别企业的选择，而成为时代发展的必然趋势。海外市场蕴藏着巨大的机会，同时出海的企业也面临着巨大的挑战，通常需要在以下三个方面建设合规能力：

· **财务合规：**企业在财务合规方面要重点关注会计政策统一性、会计科目梳理匹配和财务及管理报告三个要素，例如企业应该考虑境外财税披露要求、海外单体管理报表要求等。

· **税务合规：**企业进入目标市场时应考虑利润分布、税务申报、税务会计、国际贸易、人力成本等因素；未来需要退出目标市场时，还要考虑退出方式和税务应对策略。

· **数据合规：**出海企业需要重点关注的问题，也会在本建议书进行详细的介绍。

1.1 中企出海面临的主要合规挑战

中国的出海企业通常会面临三大合规方面的挑战：

· 合规风险意识薄弱：在国际化商业活动中，对于数据合规（本建议书主要论述）、进出口管制、金融限制与制裁、环保风险、社会责任等新型风险，大部分企业认知不足。

· 企业合规能力建设不健全：欠缺有效识别和规避风险的机制措施，导致丢失商业机会，还可能因此造成投资的重大损失乃至罚款。

· 国际化企业法务人才稀缺：相比欧美成熟的国际化大公司，大部分国内企业不仅法务人员数量不足，而且国内法务人员在处理诸多海外场景的业务时，对当地法律文化与法规不熟悉，无法对企业的风控与决策形成有效支撑。

1.2 隐私保护与数据安全

众所周知，数据的价值，基于经济活动中信息交互所产生；数据越流通，应用在不同场景，其价值会得到不断放大及提升。所以数据也理所当然地被认为是“资产”，是数字经济的“石油”，各个国家争相立法保护数据安全与隐私，形成了不同的数据跨境流动合规规制圈。这固然是不同国家平衡“数据安全”与“数字红利”的结果，但却也使的企业在出海时面临的数据合规场景变的异常复杂，不同国家地区这方面的法律不尽相同，而且各国家间的数据跨境传输需要考虑的复杂性也被成倍放大。

发展带来的问题终究还是要靠发展来解决。在数据流通过程中，企业不可避免的会遇到数据安全，隐私保护等问题，本建议书即旨在通过场景化的拆解与映射，将出海数据合规问题化整为零变成企业可理解、可落地、可持续的方案。以技术手段为主，咨询服务为辅，帮助企业建设合规风控的体系能力和运营机制。

阿里云出海能力中心&德勤中国

ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

中企出海
数据合规建议框架

2.1 评估规划

2.2 人员组织

2.3 流程制度

2.4 技术方案

2.5 持续运营

02 中企出海数据合规建议框架

对于有出海需求的企业，我们建议从如下五个步骤开展数据合规能力的建设，包括：评估规划、人员组织、流程制度、技术方案和持续运营。

2.1 评估规划

企业在出海之前应进行充分的合规准备工作，最有效的方式是通过差距分析、风险评估和规划，以此了解企业自身已建设或正在建设的数据合规管理和技术措施是否已能满足出海目标国家的数据合规监管要求。如果存在差距，企业可以趁此契机，结合企业自身的业务需求和风险偏好，规划或调整当前的数据安全合规建设。具体在评估规划当中，我们建议可以执行如下步骤：

- **现状调研：**企业结合出海业务的需求，全面梳理出海目的国家的相关监管机构的数据保护与网络安全的法律法规，通过对条款解读与分析形成自查的评估问卷或形成合规基线要求。
- **风险评估：**企业基于评估问卷或合规基线要求，对自身的组织和人员、制度和流程、技术管理等方面进行审视，发现其中的数据合规差距和问题，通过与相关关系部门的问题确认与风险分析，获得最终合规问题发现及优先级排序。
- **蓝图规划：**基于风险评估的问题发现，并结合企业自身的出海业务战略，企业规划数据合规建设，一般可从如下方面进行规划，包括：人员组织、流程制度、技术方案和持续运营。

2.2 人员组织

企业首先要成立一个专职的合规团队，可以是实体组织，也可以是虚拟组织，关键是要有明确的责任人和责任团队。其中作为数据控制者任命的数据保护官DPO应符合专业要求，明确其岗位角色和职责。建议基于欧盟数据保护监管机构最新的系列判例，包括：

- 保持其自主性和独立性，不建议由合规部门负责人或执行具体合规工作责任人兼任，以避免利益冲突；
- DPO在汇报工作时，应能直接接触公司的最高管理层，避免违反GDPR第38（3）条；
- 当公司选择外部提供的DPO服务时，公司应为其分配执行任务所需资源、允许外部DPO能够主动干预公司的数据处理活动的目的和处理方式、支持其有效地控制数据合规计划或监控的程序，为组织提供数据保护合规性建议与合规陪伴。
- DPO要有绝对的独立性，不能兼职等，不能超过两层向董事会汇报，不能跟实施的人（合规委员会、数据安全团队）重叠。

该合规团队主要涉及四大职能：

· **企业业务合规体系建立：**这部分主要在企业内部建立合规相关的制度、流程和文化，是合规团队最主要的工作。在本建议书第三章将详细展开阐述，此处不赘述。

· **与监管机构沟通：**当监管机构介入对企业进行审查，以及下发一些新的合规规定的时候，需要能够找得到企业明确的对接人和责任人。除此之外，企业的合规团队还需要主动与所在国家、地区的监管机构取得联系，保障与监管机构的沟通管道是顺畅的，能及时获知与企业相关的合规方面的信息，以最大程度事前规避合规风险。

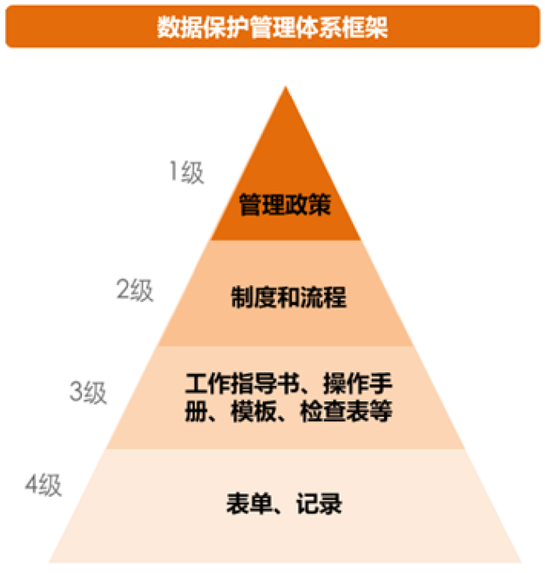
· **垂直行业合规理解：**不同的行业，在不同的国家，其合规相关法规条款也不尽相同，比较典型的如社交、电商、金融、医疗等行业。因此企业的合规团队务必要充分了解所在国、所在行业的相关合规法条，主动与行业协会、行业内的专业人士建立连接，不仅能够获取专业建议，也能从合规角度满足行业规定与标准要求。

· **咨询机构建联：**由于合规相关法律、规则的复杂性和多样性，合规团队需要善于利用外部咨询机构的能力来补足企业在合规能力上的短板。信任如律所、四大乃至云厂商等咨询机构的专业性，一切以保障业务免受合规惩罚为目标。在很多时候，直接采买咨询机构的能力是ROI最高的做法。

同时，合规团队也需要对云厂商本身的合规资质、云产品在海外各区域的数据处理能力、技术方案对各国合规要求的满足性等方面有充分的了解，并在产品的选择和使用方面提供自己的专业建议。人员组织方面的详细方案，和流程制度的设计是紧密结合的。部分内容在本建议书第三章有详细介绍，如果要进行完整的设计和规划，可以进一步咨询阿里云，阿里云会基于阿里集团的实践，联合生态伙伴共同提供完整的咨询方案。

2.3 流程制度

随着数据量的爆发式增长，如果企业缺乏标准化、体系化的流程与制度，那么数据合规建设面临的挑战将会指数级增加。建议企业参照国际标准结合海外数据合规监管要求定义数据保护的目标、管理策略以及构建与实施制度具体的规范和流程。数据保护的制度文件建议可分为4个层面，一、二级文件作为上层的管理要求，具备数据保护的合理性、完备性及普适性；三、四级文件是针对一、二级文件的管理要求进行细化或解读，具有指导企业在出海业务场景中如何开展可满足数据合规的工作



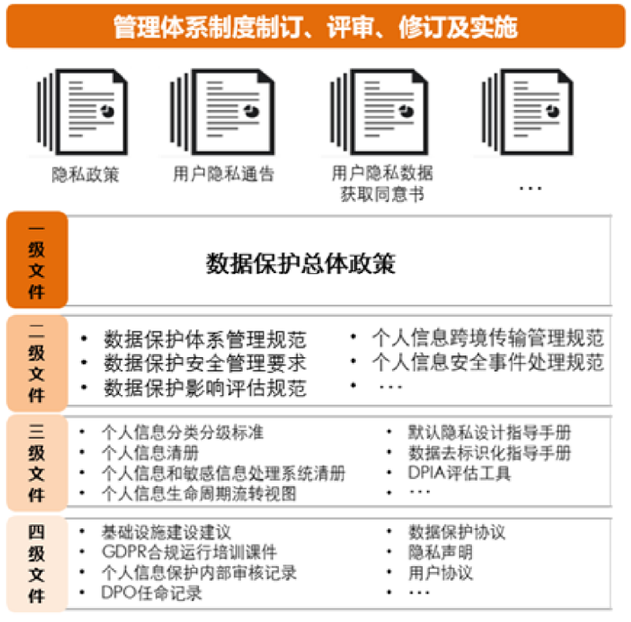
（1）一级制度：数据保护的管理政策
（2）二级制度：详细的数据保护制度和流程
（3）三级制度：完成数据合规所需的工作指导书、操作手册、模板和检查表等
（4）四级制度：完成数据合规工作所需的各类表单模板

我们建议企业在数据保护的一级、二级文件至少要覆盖以下内容：

（1） 数据保护策略（一级）
（2） 数据保护组织架构与职责说明（一级）
（3） 数据分级与分类制度（二级）
（4） 数据生命周期保护管理要求（二级）
（5） 数据保护事件管理制度（二级）
（6） 数据合规审计管理制度 （二级）等

我们建议企业在数据保护的三级、四级文件至少要覆盖以下内容：

（1） 数据安全分类分级管理流程
（2） 数据账号与访问权限管理流程
（3） 数据共享安全管理流程
（4） 数据跨境传输管理流程
（5） 个人信息主体权利管理流程
（6） 个人信息影响评估管理流程
（7） 个人信息安全工程管理流程
（8） 数据安全事件管理流程
（9） 第三方数据处理者管理流程等



以上列出的只是一些必选项，当企业数据规模、业务复杂性、国家覆盖面等合规关键影响因素开始彰显的时候，要建立的流程制度远不止上述几项。

关于流程制度的拆解和细化，可参考本建议书第五章内容。

2.4 技术方案

在技术方案维度，需要从三个层面来建设，如下图所示：

首先是底层云平台要能充分保障数据安全和上层的各种数据能力能够得到充分的支撑。这一部分详见本建议书第二章内容。然后是中间层依照数据生命周期各个环节，进行产品、方案和场景的映射与设计，如下图：

最后是与业务场景紧密结合的技术方案，基于中间层数据生命周期管理的各个积木，按照具体的业务场景，来灵活搭建所需的能力。如cookie的合规改造，用户数据行权中心建立，从A国到B国的具体数据跨境的管控，营销场景的数据跨主体管控等。如下图所示：

2.5 持续运营

企业通常需要在发展过程中持续运营以保持合规。

2.5.1 数据保护分类分级

在企业的数据保护工作中，核心是数据的分类施策，即根据出海目标国家相关数据合规监管要求的规定，建立数据分类分级管理机制。企业应该持续实施对结构化数据和非结构化数据的识别、标签和分类分级管理，重点关注个人敏感信息、国家或行业认定的重要数据，这些数据在数据采集、数据存储、跨境传输、数据处理和数据销毁全等过程中都必须遵循相应数据级别的管理和控制措施。

2.5.2 数据合规报备

由于全球各国都在开展有关数据保护的立法，企业在海外使用和处理数据时涉及向当地数据保护部门进行报备工作。因此，企业需要对出海国家的数据合规监管进行梳理，识别出需要向相关部门报备的情况，结合企业自身业务数据使用情况，提前做好准备和建立相应的流程机制。目前海外国家需要向有关部门报备与审批情况主要集中在数据跨境传输和发生对当地具有较大影响的数据安全事件这两个领域。

2.5.3 数据保护影响评估和个人信息安全工程运营（PbD）

结合GDPR及最佳的数据保护合规实践，我们建议企业需要将PIA（隐私影响评估）或DPIA（数据保护影响评估）等动作融入业务管理流程中，当业务、产品和应用系统涉及处理个人信息或出海国家认定的重要数据，在其新开展或变更的情况下执行相关影响评估动作，以提前识别这些业务、产品或应用系统是否存在数据保护的合规隐患，并尽早规划解决方案。

同时，为了能将解决方案在业务、产品和应用系统有效落地，建议企业在每一项产品和应用系统的研发过程中均引入个人信息安全工程的理念，从需求分析、产品设计、产品研发、产品测试等环节层层把关，以确保产品在上线后能够实现有效的数据保护功能或规避违规的数据操作。

2.5.4 个人信息主体权利行使运营

个人信息保护相关监管要求规定了在企业处理、使用个人信息过程中数据主体的权利范围，企业应尽可能通过自动化或人工的方式来确保满足个人信息主体的权利，下述举例了一些常见的数据主体权利：

（1）同意管理：企业收集用户信息都需要征得用户的同意，并形成同意记录；
（2）撤回同意：企业获得个人同意处理个人信息的，个人有权撤回其同意，企业应当提供便捷的撤回同意的方式；
（3）信息查询、更正权：企业应提供有效的查询、更正个人信息功能的渠道；
（4）删除或者限制处理权：企业为个人信息主体提供要求删除其个人数据或者限制对其个人信息进行处理的渠道；
（5）账户注销权：企业应提供并支持用户账号注销的功能，并确保在用户注销账号后，及时删除其个人信息或进行匿名化处理。

2.5.5 数据保护事件响应和应急管理

1. 事件管理机制

企业应组建数据安全运营团队持续对数据安全态势进行监测，制定数据安全事件监测规则，当发生数据安全事件时，根据数据安全事件的级别开展相应的数据安全事件响应、升级、解决、报告和复盘动作。

2. 预案演练与优化

企业定期开展应急预案演练活动，保证员工熟练数据合规应急预案的操作流程。并根据演练过程中发现的问题对应急预案进行修订和优化。

阿里云出海能力中心&德勤中国
ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

云平台能力
保障出海数据合规

3.1 云平台合规能力
3.2 阿里云对于云上客户的隐私保护
3.3 云平台安全能力

03 云平台能力保障出海数据合规

本章主要介绍阿里云的安全保障能力。云环境底层提供的能力构成了所有业务层数据安全和隐私保护的地基。这些能力如同海面下的冰山，并不为人所关注。但云厂商在这方面持续不断的巨额投入，既是阿里云自己合规经营、拿到诸多海外合规认证的基础，也是阿里云能够提供给客户的最终的合规能力的原料。本章主要包含合规与安全两部分，合规部分阐述的是云平台本身如何遵循合规要求，保护云上客户的隐私，以及如何将合规能力涉及到云平台的产品与服务中从而让云上的客户支撑自己的业务数据合规。在云平台安全部分，分成四个方面来介绍：基础设施安全、数据存储安全、数据网络安全、数据计算安全。这四个领域的安全是数据合规的必要条件，也是整个云平台合规体系的基石之一。

鉴于篇幅所限，有兴趣的读者也可以到阿里云安全团队出品的数据安全白皮书中了解详细信息：《阿里云数据安全白皮书》

3.1 云平台合规能力

阿里云的安全流程机制已经得到国内外相关权威机构的认可，我们将基于互联网安全威胁的长期对抗经验融入到云平台的安全防护中，将众多的合规标准融入云平台合规内控管理和产品设计中，同时广泛参与各类云计算服务相关的标准制定并贡献最佳实践，通过独立的第三方验证阿里云如何符合标准。

阿里云的安全流程机制已经得到国内外相关权威机构的认可，我们将基于互联网安全威胁的长期对抗经验融入到云平台的安全防护中，将众多的合规标准融入云平台合规内控管理和产品设计中，并通过独立的第三方验证阿里云如何符合标准。同样地，为了切实落实遵守数据安全和隐私保护相关的国际国内法规的承诺，阿里云在建立和执行内部数据安全和隐私保护管控体系之外，也积极对标通过了数据安全、隐私保护和其他安全合规的第三方审计，获得了国际、国内或行业标准认证。

全球通用认证举例如下：

CSA STAR
CSA和BSI联合推出的云安全云安全管理体系标准，阿里云获得全球首个金牌认...

ISO 27001
信息安全管理体系认证
从数据、网络、操作等各个方面证明阿里云履行其安...

ISO 20000
IT 服务管理体系认证
阿里云建立并严格执行标准的服务流程，降低 IT 整体...

ISO 22301
业务连续性管理体系认证
阿里云建立业务连续性计划并定期演练，提升云平台...

ISO 9001
质量管理体系认证
阿里云建立质量管理体系，在服务过程中持续改进其...

ISO 27017
云服务信息安全控制指引
从环境隔离、虚机强化等各个方面证明阿里云平台安...

ISO 27018
云上个人数据保护的国际行为准则，阿里云建立个人数据保护管理体系，并通过...

ISO 27701
扩展ISO 27001/27002的隐私信息管理，阿里云强化个人数据保护管理机制并通...

ISO 29151
个人身份信息保护行为准则，阿里云强化个人数据保护管理机制并通过认证

BS 10012
个人信息管理系统，阿里云强化个人数据保护管理机制并通过认证

PCI DSS
阿里云遵守支付卡行业数据安全标准，通过了1级服务提供商资质

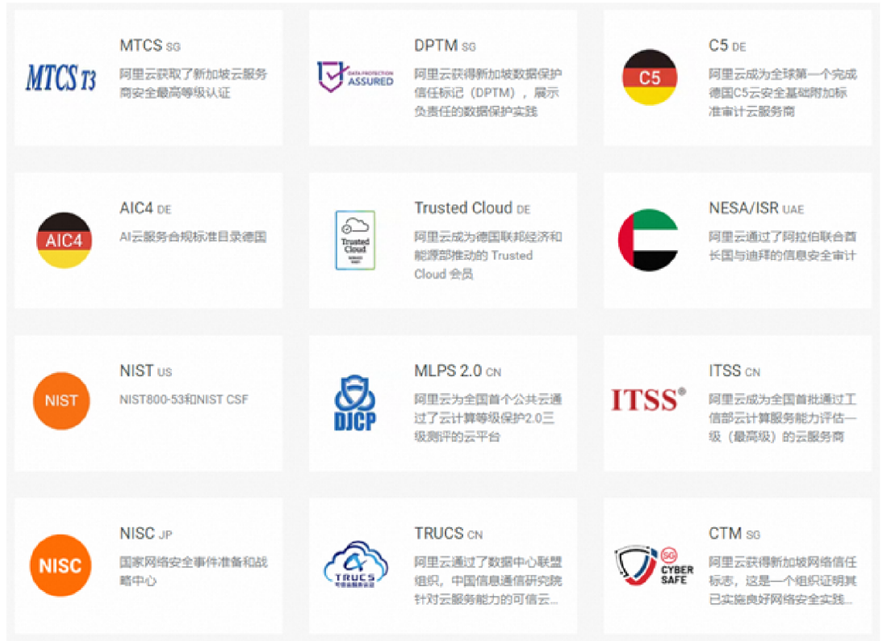
PCI 3DS
PCI 3DS核心安全标准，旨在保护3D协议执行环境中的3DS数据，技术和过程。

SOC1 Type II Report
针对财报的内控报告
为客户及其审计师就其财务报告内部控制的有效性服务

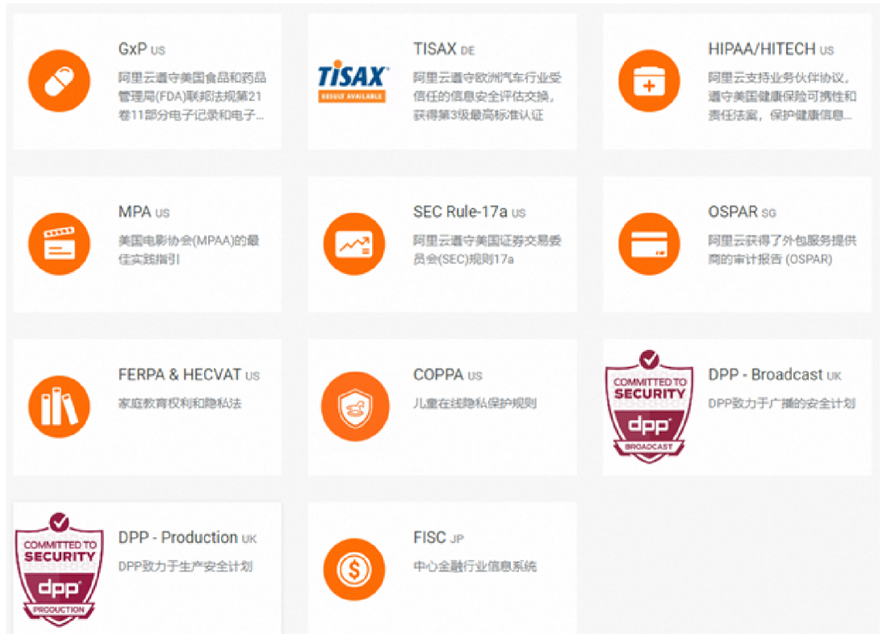
SOC2 Type II Report
安全性、可用性与机密性报告
为客户提供对阿里云安全...

SOC3 Report
安全性、可用性与机密性的一般控制报告

区域认证举例：



行业认证举例：



在数据保护与隐私方面的认证：

3.2 阿里云对于云上客户的隐私保护

长期以来，阿里云坚持致力于保护每位客户在云上产生的个人信息类隐私数据，保证客户对所有提供给阿里云的个人信息拥有所有权和控制权。与此同时，阿里云积极响应国家监管部门对企业承担个人信息保护责任的号召，持续完善内部的个人信息管理和保护体系。阿里云设置了专业的个人信息保护团队，在隐私权政策、客户权利保障等方面持续优化，建立了内部整体的数据安全管理体系，落地数据安全保护的核心技术，为客户个人信息提供了全生命周期的安全可靠的保护能力。在不幸发生用户信息安全事件（泄露、丢失等）后，阿里云将按照法律法规的要求，及时向客户告知：安全事件的基本情况和可能的影响、已采取或将要采取的处置措施、客户可自主防范和降低风险的建议、对客户的补救措施等。阿里云将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知客户，难以逐一告知用户信息主体时，阿里云会采取合理、有效的方式发布公告。同时，阿里云还将按照监管部门要求，上报用户信息安全事件的处置情况。

阿里云通过大量权威机构的认证证明个人信息保护能力/数据安全保护能力，并将持续建设阿里云整体的个人信息保护管理体系，在此领域内，阿里云已经获得包括ISO/IEC 27701:2019、ISO/IEC 29151:2017、ISO/IEC27018:2014、BS 10012:2017在内的所有关于国际隐私保护标准认证的“全满贯”。

阿里云拥有完善的隐私管理体系，同时通过各类管控流程和系统的落地，实现隐私保护工作在一线业务的推进，如下图所示：

基于隐私管理体系，阿里云提供了从用户启用云服务到离开云的全生命周期的隐私保护能力，在用户接触阿里云的每个环节，阿里云都严格遵守用户的授权，执行对其隐私数据的安全保护。

同时，用户能在阿里云上获得更多自主可控的权利。阿里云在官网控制台为用户提供了对营销推送的拒绝能力、对授权登录账号的一键解绑能力、离开阿里云时的一键账号注销能力等，以方便用户快速简单的执行相关操作，通过这种可感知的能力让用户对自己的隐私信息进行有效管理。不仅如此，阿里云还推出了内部操作透明化服务，让用户对阿里云内部运维操作日志清晰可见，且可追溯，提

升云平台对用户的透明度。

在客户使用阿里云服务的过程中，阿里云严格遵守相关合规规定，对用户信息的搜集，以及后续在客户授权情况下进行的共享、转让、披露等行为进行了严格的规定，保护客户云上隐私安全。
关于个人隐私保护的部分认证说明如下：

· 阿里云已经获得ISO/IEC 27701:2019、ISO/IEC 29151:2017、ISO/IEC 27018:2014、BS10012:2017在内的所有关于隐私保护标准认证的“全满贯”。
· ISO/IEC 27018云上个人隐私保护规范标准：保护在公共云中的个人身份信息（PII）。例如，对于应用程序代码，任何写入日志文件的输出都会通过数据清除程序，该数据清除程序会在将数据发送到中央系统之前删除客户数据。这些措施最大程度地减少了将客户数据复制到分析或操作存储库的风险。客户可以在阿里云官网的阿里云信任中心查看最新的ISO 27018认证证书。
· ISO/IEC 27701 (PIMS) 隐私管理体系标准：ISO/IEC 27701为ISO/IEC27001信息安全管理系统 和ISO/IEC 27002信息安全控制措施的扩展，考虑了对GDPR条款以及其他隐私相关标准的条款映射，是业内公认最具权威性的隐私管理体系建设指导标准。PIMS认证表明，阿里云提供了一套全面的管理和操作控制，可以帮助组织证明对隐私法律和法规的遵从性。客户可以通过阿里云官网获取最新的ISO 27701认证证书。
· ISO/IEC 29151 个人身份信息保护管理体系标准：为企业保障个人隐私安全及降低合规风险的控制提供了大量的实用指南，以满足与保护个人身份信息（PII）有关的风险和影响评估所确定的要求。该标准基于ISO/IEC 27002的准则，同时考虑到可能在组织的信息安全风险环境中适用的处理PII的要求。阿里云的ISO 29151证书也可以在官网下载。

客户可以通过阿里云官网的阿里云信任中心查阅阿里云的等保审核、PCI DSS标准认证等更多第三方安全合规资质信息，从而为客户履行自己的数据安全、隐私保护、安全合规相关的义务提供支持：https://www.alibabacloud.com/zh/trust-center

3.3 云平台安全能力

阿里云平台提供了完善的安全能力，帮助出海企业实现业务合规运行。

3.3.1 基础设施安全

基础设施指的是阿里云机房及其运维，阿里云的机房提供了完善的物理安防设备，设置了一批严格训练的安保团队，建立了一套分类分级管控、工单驱动、行为数据化、空地协同的安防体系。并在机房访问管理，停机维护等场景建立了完整的流程与经验能力。

此外，阿里云具有强大的机房容灾能力，保障在某一个机房发生灾难时，可以迅速地将数据和业务迁移到其他机房，从而确保客户的业务和数据安全。

3.3.2 数据安全

阿里云在数据存储安全方面，主要提供了以下6项能力。

· **数据写入稳定性：**阿里云为全球客户提供高可用的数据服务，包含业务可用性、数据可用性、维护和停机时间的规范。影响业务或数据的故障可实现自动恢复，坚守高可用的云上服务承诺。阿里云的数据库、云服务器、云实例、云容器等诸多产品均提供高可用的SLA承诺（SLA即服务等级协议，代表了云服务商承诺提供的计算服务所能达到的服务质量和标准）。如云服务器单实例的可用性为99.975%，多可用区多实例可用性为99.995%，OSS标准型存储SLA为99.995%，块存储提供99.9999999%的可靠性，ACK pro集群的服务可用性不低于99.95%。在这些与数据写入相关的云产品的高可用保障下，数据写入的稳定性得到了保障，从而也为阿里云客户符合所在国家的数据安全要求提供了保障。若阿里云提供的服务时间未达到承诺的标准，则将依据协议对客户作出赔偿。
· **存储介质管理：**阿里云不允许存储介质带数据迁移。针对维修替换、到期报废或者无法擦除的存储介质，阿里云数据中心规定此类存储介质需要在规定时间（一般为2分钟）投入存储介质安全箱内，以确保存储介质不会挪为他用。
· **销毁管理：**阿里云参考NIST SP800-88的安全擦除标准建立了存储介质数据安全擦除的机制并嵌入设备资产管理的控制机制中。针对需要重复使用的硬件存储介质，会对存储介质上的数据进行多次清除以完成数据销毁，并确保其不能被取证工具恢复。针对需销毁的存储介质，阿里云数据中心会对其进行完整的物理销毁。使用特殊机器对目标介质进行碾压、绞碎，破坏成粉碎小块，最终通过称重核实等方式完成物理销毁工作，确保无一存储介质遗漏。
· **独立报废：**为了确保数据安全，阿里云数据中心自建了独立的报废产线用以彻底粉碎存储介质。针对机械式硬盘设计了颗粒度≤30*60mm和半导体硬盘颗粒度≤5*5mm的物理粉碎标准。
· **存储数据加密：**块存储（EBS）数据落盘加密，对象存储（OSS）支持客户端与存储端的加密能力，文件存储（NAS）支持使用服务托管密钥和用户自选密钥作为主密钥进行数据加密，表格存储（TableStore）支持使用服务密钥和客户自选密钥作为主密钥进行数据加密。
· **冗余数据备份保护：**阿里云建立了完备的云上数据冗余机制，HBR、DBS、MaxCompute等产品均有数据备份功能，从磁盘、服务器、机房、集群等维度进行备份保护，保证客户哪怕遭受勒索软件攻击，数据也不会丢失，极大降低业务损失。

3.3.3 网络安全

数据的网路安全指的是数据在传输时的安全，基于阿里云的加密技术与充分的备份措施，可以确保数据在网络传输时不会被泄露，不会因为意外而丢失。

· **物理网络数据传输加密：**阿里云将网络数据保存到指定的存储空间中，留存时间符合法律法规要求，并采用密码技术对存储数据加密，保证存储过程中的保密性。
· **网络数据权限保护与加密保护：**在阿里云中，网络数据一般指系统账号、网络配置、网络监控数据这三种数据。对运营网络的账号，采用最小权限原则授权。鉴权系统采用口令、密码技术、生物技术等组合对用户身份进行鉴别，身份鉴别信息具有复杂度要求并强制定期更换。阿里巴巴对网络设备配置中的敏感字段（包括且不限于账号密码、管控协议密码、路由协议密码）进行不可逆加密，配置文件中无明文密码暴露。
· **网络数据备份：**阿里云采用本地数据备份和异地数据备份结合的策略，将网络数据实时备份至本地存储空间，并将重要网络数据定期备份至异地存储空间。配合数据的自动恢复能力，保证网络数据安全可用和重要数据的及时恢复。
· **云上传输加密：**阿里云对云上数据传输过程采取多种层次的手段进行加密，主要是传输层链路加密和传输层数据加密能力，加密能力可以单一使用，也可以组合使用，包含传输层链路加密和传输层应用加密。

3.3.4 计算安全

阿里云提供了硬件与软件领域的计算加密技术，具备可信环境，确保数据的计算安全。

· **硬件层机密计算：**机密计算亦可称为隐私计算、隐私增强计算，面向敏感数据有计算需求而又不担心泄漏风险，可以达到数据“可用不可见”的效果。阿里云通过硬件层、虚拟化层、应用层三种形态的机密计算能力为客户提供全方位的数据保护。阿里云新一代硬件基于Intel® SGX（Software Guard Extension）2.0构建可信执行环境。
· **虚拟化层机密计算：**阿里云虚拟化Enclave在ECS实例内部提供了一个可信的隔离空间，将合法软件的安全操作封装在一个Enclave中，保障客户代码和数据的机密性与完整性，不受恶意软件的攻击。
· **应用层机密计算：**阿里云于2021年4月发布公有云隐私增强计算平台，支持可信执行环境、联邦学习、安全多方计算等各类加密计算技术，提供不同类型多场景的解决方案。
· **可信计算：**从系统可信根、硬件固件安全、启动链可信以及运行时可信几个方面定义了云硬件安全架构，提供给客户安全可信的云上数据计算环境。可信云的底层信任基础是物理可信根，基于物理可信根，阿里云构建起云平台可信链。物理可信根通常由TCM/TPCM/TPM2.0和可信固件共同构成，可以有效保护其内部逻辑和数据。
· **可信计算环境：**阿里云基于TPM、VTPM、虚拟化Enclave等技术，构建了基于神龙安全芯片的全隔离、高可信的计算环境。阿里云可信计算环境的信任链起点在于硬件自身的不可篡改性。

阿里云出海能力中心&德勤中国

ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

全球主要数据合规法规与建议

4.1 欧盟

4.2 东南亚

4.3 北美

4.4 日韩

4.5 印度

4.6 南美

4.7 澳新

4.8 中东区域

4.9 海外各国数据本地化与DPO要求小结

04 全球主要数据合规法规与建议

全球范围内各国家、区域相继出台个人数据保护法，其中以欧盟、中国、美国的法规最严，执法力度最大。区域合规差异化及商业模式窗口期缩窄，企业实质合规一体化趋势将提升合规成本，同时全球数据本地化、数据法域外效力区域进一步拓展，数据合规成为国内业务出海需事前准备的核心问题之一。

虽然全球各国的法规不尽相同，但一个明显的趋势是，GDPR模式正在成为主流。因此，企业出海在考虑合规的关键场景和建设全球的合规能力的时候，建议主要参考GDPR。在这个基础上，再针对不同国家不同领域的数据做一些细节的补充。但对于一些行业也要考虑行业相关合规要求，例如医药或医疗器械行业，须关注美国和澳洲的行业法规，例如美国《健康保险携带与责任法》HIPAA对个人健康信息提出隐私保护要求、澳洲的《个人控制的电子健康记录法》要求一般情况下，法律规范的主体不得将个人健康数据向澳洲以外传输，主体需在澳洲境内建设数据中心处理健康相关数据或将相关服务外包至境内服务商。

当前全球的执法趋势：

- 执法重点：未成年人保护、 数据跨境传输、新技术（AI、面部识别、区块链、量子计算等）。
- 美欧、欧盟内部执法的国际合作与一致性加强。
- 国内执法从数据负向使用制止开始向正向规制拓展。

4.1 欧盟

4.1.1 GDPR简介

《通用数据保护条例》(GDPR) 是一项欧洲隐私法，已于 2018 年 5 月 25 日生效。GDPR 已取代《欧盟数据保护指令》（也称为指令 95/46/EC）。GDPR作为一部强制性法律，覆盖欧盟各个成员及使用个人数据的商业行为，旨在通过实施一个可约束每个成员国的数据保护法，来协调整个欧盟 (EU) 的数据保护法律。

GDPR主体内容包括这四个方面：基本原则、数据主体的权利、数据控制者和处理者的责任与处罚。

4.1.2 GDPR基本原则

GDPR制定了关于处理个人数据中对自然人进行保护的规则，以及个人数据自由流动的规则。核心目标是保护自然人的基本权利与自由，特别是自然人享有的个人数据保护的权利。不仅只是保护，还同时保障在欧盟内部个人数据流动的自由性，不能以保护处理个人数据中的相关自然人为由，对欧盟内部个人数据的自由流动进行限制或禁止。

1. 适用范围：

- 适用于在欧盟内设立的数据控制者或处理者对个人数据的处理，不论其实际数据处理行为是否在欧盟内进行。
- 适用于为欧盟内数据主体提供商品或服务，或对发生在欧盟范围内的数据主体活动进行监控这两种情形的个人数据处理，即使数据

控制者或处理者不在欧盟设立。

· 适用于在欧盟之外设立，因欧盟和其他国家区域签订的国际条约，从而对其有管辖权的数据控制者的个人数据处理。

2. 个人数据处理的原则

· 对个人数据的处理需要获得数据主体的同意。当数据主体是儿童且不满16周岁，需要获得具有监护责任的主体的同意或授权。

· 合法性、合理性和透明性：对涉及到数据主体的个人数据，应当以合法的、合理的和透明的方式来进行处理。

· 目的限制：个人数据的收集应当具有具体的、清晰的和正当的目的，对个人数据的处理不应当违反初始目的。

· 数据最小化：个人数据的处理应当是为了实现数据处理目的而适当的、相关的和必要的。

· 准确性：个人数据应当是准确的，如有必要，必须及时更新；必须采取合理措施确保不准确的个人数据，即违反初始目的的个人数据，及时得到擦除或更正。

· 限期储存：对于能够识别数据主体的个人数据，其储存时间不得超过实现其处理目的所必需的时间；除了为了实现公共利益、科学或历史研究目的或统计目的，为了保障数据主体的权利和自由，并采取了合理技术与组织措施。

· 数据的完整性与保密性：处理过程中应确保个人数据的安全，采取合理的技术手段、组织措施，避免数据未经授权即被处理或遭到非法处理，避免数据发生意外毁损或灭失。

4.1.3 数据主体的权利

数据主体是指任何已识别或可识别的自然人，数据主体的权利主要包括如下几类。数据主体的权利在因国家安全、国防、公共安全、司法保护等情况下可能会受到限制。

访问权	有权从数据控制者处获知数据处理的目的，数据类型，披露的对象，数据存储期限，数据的来源，用于决策时的数据处理逻辑等。
更正权	有权从数据控制者处及时得知对与其相关的不正确信息的更正。在考虑处理目的的前提下，有权完善不充分的个人数据，包括通过提供额外声明的方式来进行完善。
擦除权（被遗忘权）	有权要求控制者擦除关于其个人数据的权利，当具有如下情形之一时，控制者有责任及时擦除个人数据，除非为了国际利益或者法律性主张。
限制处理权	当数据准确性、处理目的不合法等情况下，有权要求控制者对处理进行限制。
携带权	数据主体有权获得其提供给控制者的个人数据，且其获得个人数据应当是经过整理的、普遍使用的和机器可读的，有权无障碍地将数据从控制者那里传输给另一个控制者。
反对权	当因为直接营销目的而处理个人数据，数据主体有权随时反对为了此类营销而处理相关个人数据，包括反对和此类直接营销相关的用户画像。

4.1.4 数据控制者和数据处理者的责任

1. 数据控制者的基本责任

· 控制者应当在决定处理方式时和决定处理时，应当采取合适的技术与组织措施，并且在处理中整合必要的保障措施，以便符合数据主体权利。

· 控制者有责任采取适当的技术与组织措施，以保障在默认情况下，只有某个特定处理目的所必要的个人数据被处理。这种责任适用于收集的个人数据的数量、处理的限度，储存的期限以及可访问性。

· 保持其所负责的处理活动的记录，包含所有如下信息：控制者姓名及联系方式、处理目的、数据类型、披露的对象范围等。

· 提供某种已生效的认证机制，证明符合上述规定。

2. 数据处理者的基本责任

· 如果没有控制者的特别授权或一般书面授权，处理者不应聘用另一个处理者。在具有一般书面授权的情形下，对于涉及到补充或替换其他处理者的变动，处理者都应当告知控制者，以便使控制者有机会反对此类变化。

· 处理者只有在收到控制者的书面指示时才可以处理个人数据，在涉及到将个人数据转移到第三国或某个国际组织的事项中亦是如此。

· 基于控制者的选择，在提供和处理相关的服务结束后，将个人数据删除或返还给控制者，并且删除已有备份，除非欧盟或成员国的法律要求储存个人数据。

· 保持其所负责的处理活动的记录，包含所有如下信息：控制者姓名及联系方式、处理目的、数据类型、披露的对象范围等。

· 给控制者提供所有能够证明其已经遵循规定责任的信息，以及有利于控制者进行审计和核查的信息。

3. 数据处理的安全要求

· 控制者和处理者应当采取包括但不限于如下的适当技术与组织措施；

· 个人数据的匿名化和加密；

· 保持处理系统与服务的保密性、公正性、有效性以及重新恢复的能力；

· 在遭受物理性或技术性事件的情形中，有能力恢复对个人数据的获取与访问；

· 具有为保证处理安全而常规性地测试、评估与评价技术性与组织性手段有效性的流程；

· 在评估合适的安全级别的时候，应当特别考虑处理所带来的风险，特别是在个人数据传输、储存或处理过程中的的意外或非法销毁、丢失、篡改、未经授权的披露或访问。

4. 数据泄露的披露要求

· 向监管机构报告：

在个人数据泄露，控制者在知悉后应当及时（至迟在72小时内）将个人数据泄露告知有权监管机构，除非个人数据泄露对于自然人的权利与自由不太可能会带来风险。对于不能在72小时以内告知监管机构的情形，应当提供延迟告知的原因。处理者在获知个人数据泄露后，应当及时告知控制者。

· 向数据主体的披露：

当个人数据泄露很可能给自然人的权利与自由带来高风险时，控制者应当及时向数据主体传达对个人数据的泄露。

5. 组织及流程要求

数据控制者和处理者应该建立数据保护的评估保障流程，并设立相应的数据保护官。

4.1.5 GDPR处罚

GDPR对数据主体、数据控制者、数据处理者、监管机构等都做了相关的法律权利及诉讼的限定，如申诉权、司法救济权等，这里重点提一下行政处罚的要求：

1. 轻度处罚：施加最高10 000 000欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额2%的金额的罚款，两者取其高的一项进行罚款。
2. 重度处罚：施加最高20 000 000欧元的行政罚款，如果是企业的话，最高可处相当于其上一年全球总营业额4%的金额的罚款，两者取其高的一项进行罚款。

4.1.6 GDPR合规主要关注点

1. 数据本地存储要求

GDPR没有规定数据必须要本地存储，但是对于数据跨境则有着严格的规定。当然，对于一些特定行业，如医疗、金融、政府业务等，欧盟境内需要遵从各所在国的规定。

2. 数据跨境要求

总体而言GDPR关于数据跨境传输的一般性原则是，数据控制者或处理者在全面满足各条款的具体要求时，才能够将个人数据从欧盟转移到第三国或国际组织。GDPR中关于数据跨境传输要求的条款主要是下面五条：

· 充分保护水平：将个人数据从欧盟转移到第三国的活动仅限于欧盟委员会决定具有“充分保护水平”的国家。GDPR同时提供了评估保护程度的充足性时会考虑的相关因素。需要注意的是，中国不被欧盟认为是提供了“充分保护水平”的国家。2023年7月10日，欧盟委员会通过了关于欧美数据隐私框架的充分性决定。美国被正式列入至欧盟数据跨境白名单。这意味着欧盟内个人数据可以自由流动至美国而无需采取额外的保障措施。数据控制者或处理者可以合法地将个人数据传输到这些位于清单中的国家或地区。截止2023年7月10日，被欧盟认可的通过数据充分保护性认证的国家或地区有15个：安道尔、阿根廷、加拿大（仅限商业组织）、法罗群岛、根西岛、以色列、曼岛、泽西岛、新西兰、瑞士、乌拉圭、日本、韩国、英国、美国。

· 受适当保障措施约束：数据控制者或处理者必须对数据提供适当的保障措施，以及为数据主体提供可执行的权利以及有效的救济措施，才能进行数据跨境转移。适当的保障措施包括数据控制者或数据处理者与数据控制者、数据处理者或第三国或国际组织的个人数据接收者之间的合同条款。

· 有约束力的公司规则：GDPR对公司规则是否具有足够的约束力给出了具体的评价标准，同时明确了欧盟委员会可以明确数据控制者、数据处理者和监管机构之间为了约束性公司规则而进行信息交换的形式和程序。该规则要求企业通过内部设置规则的方式实现自我约束，从而满足合规要求，达到数据跨境传输的要求从而可以实现数据跨境。

· 未经欧盟法授权的转移或披露：明确了在经法庭判决、仲裁裁决或第三国行政机构决定的情况下，进行数据转移或披露的条件。

· 特殊情形下的跨境：明确了在不满足前述“充分保护水平”“受适当保障措施约束”以及“有约束力的公司规则”，但仍可以进行数据跨境的情形。

如果要将在欧盟境内收集的个人信息传输到中国，需要采取其他方式证明在中国的接收方采取了足够的措施以保证个人数据安全。从欧盟出境中国的个人数据传输只要能满足下述措施中的一项，就可以被欧盟监管机构认为是合规的：

· 数据输出方与数据接收方签订数据传输协议，并使用欧盟委员会给出的标准数据保护条款；

· 如果是跨国集团内部的数据传输，可以在集团内部制定一套所谓的具有约束力的公司规则 （Binding Corporate Rules），保证集团内部严格遵守，并经欧盟委员会批准；

· 某个行业的协会拟定一套数据保护行为规则，作为数据接收方的行业协会成员声明遵守这套行为规则，该规则要经过欧盟委员会的事先认可；

· 对数据接收方的数据处理流程进行认证，该认证需要每三年更新一次。

3. 个人数据和敏感数据

· 个人信息就等同于个人数据。在GDPR的定义中， 个人数据是指与已识别或可识别的自然人（即数据主体）相关的任何信息。可识别的自然人是能够被直接或间接地识别的人，特别是通过一个标识符实现识别，例如姓名、身份号码、定位数据、在线身份标记，或者是通过自然人的一个或多个物理个性、生理个性、遗传个性、心理个性、经济个性、文化个性或社会个性这样的要素实现识别。

· GDPR把数据分成普通个人数据和敏感数据，比如说肤色，宗教，性取向，政治倾向等都属于敏感数据，企业没有特殊情况是不得收集的。按照GDPR定义，凡是涉及这一种或一种以上类型的个人数据则为敏感数据：种族或民族出身，政治观点，宗教/哲学信仰，工会成员身份，涉及健康、性生活或性取向的数据，基因数据，经处理可识别特定个人的生物识别数据。

· 根据GDPR，敏感数据的处理仅在下列例外情况下才被允许：

（1）数据主体明示同意。该等同意应当是自由作出的，特定的，知情的且明确的。需要注意的是，雇主对员工医疗数据的处理（包括药物或酒精测试）不能以员工的同意为依据。这是因为，考虑到双方的层级关系，这种同意不被视为是自由作出的。

（2）在劳动法、社会保障法或社会保护法领域，雇主对此类数据的处理必须在欧盟或成员国法律或集体协议授权的范围内进行。

（3）在数据主体因为身体上或法律上的原因（紧急情况）不能作出同意时，为保护数据主体或他人的重大利益之目的所必需的处理。

（4）处理是由具有政治、哲学、宗教或工会目的的非营利团体进行的，并且该等处理仅涉及团体成员或前成员，同时，相关数据在未经数据主体同意的情况下不会向第三方披露。

（5）涉及已由数据主体公开的个人数据的处理。

（6）为合法诉求的成立、行使或抗辩或法院行使其司法职能之目的所必需的处理。

（7）根据欧盟或成员国的法律，为重大公共利益所必需的处理。该处理所追求的目的应当是适当的，且包含合理的数据保护措施。

（8）根据欧盟或成员国的法律或与医疗专业人士的合同，为预防医学或职业医学，为评估雇员的工作能力，医疗诊断，提供卫生或社会保健或治疗或卫生社会保健系统和服务管理之目的所必需的处理。

（9）根据欧盟或成员国法律规定以适当的、特定的措施保障数据主体的权利和自由，在公共健康领域中为公共利益之目的所必需的处理。例如抵御严重的跨境卫生威胁，或确保医疗保健和医药产品或医疗器械的高标准。

（10）根据欧盟或成员国法律，为公共利益、统计、科学或历史研究之目的所必需的处理。该处理所追求的目的应当是适当的，尊重数据保护的基本权利，并采取了适当的、特定的措施以保障数据主体的基本权利和利益。

· 个人数据必须与自然人有关。GDPR不适用于法人或已故的人。

4. 其他

· GDPR的适用范围更广：GDPR适用于在欧盟成立的所有组织的行为，也使用于欧盟境外的数据处理者的行为。

· GDPR的义务范围更广：尽职义务（Due Diligence），不仅仅针对数据控制者，也针对数据处理者；通知义务，在了解到违反数据保护的情形时，不超过72小时，需要给到合理、不拖延的通知 。

· 扩大了个人的权利。一是被遗忘权，个人可以要求相关个人数据被删除；二是可携带权，要求数据控制者向另一个数据控制者转移相关个人信息。

4.1.7 GDPR合规建议

1. 阿里云的责任与义务

在 GDPR 的定义下，阿里云既是数据的处理者也是数据的控制者。

· 数据处理者：当客户使用阿里云服务来处理其上传到阿里云服务的内容中的个人数据时，阿里云的角色是数据处理者。

· 数据控制者：阿里云自行收集的个人数据，并且决定处理相关个人数据的目的和方式，比如管理我们的用户信息等，阿里云的角色是数据控制者。

但同时，客户和阿里云需要共担合规的责任。

当客户将IT系统和数据迁移到阿里云时，阿里云对底层基础架构的安全负责，而客户也要对放入阿里云中或连接到阿里云的内容负责。前者称之为云的安全性，后者称之为云中的安全性。这样一种责任划分方式可以帮客户减轻运营负担，也兼顾了灵活性和控制权，以便在阿里云中部署其基础设施。阿里云运行、管理和控制基础设施组件，从托管操作系统和虚拟化层到基础设施的物理安全性。客户负责管理guest OS（包括更新和安全补丁）、应用程序软件以及 阿里云提供的安全组防火墙的配置等。

阿里云在GDPR中提供基础的云安全能力、数据安全与隐私保护能力、GDPR合规轻咨询服务等。

2. 阿里云欧洲境内的资源分布

· 阿里云在欧盟境内有法兰克福region，3AZ架构。

· 由于英国不属于欧盟，阿里云在英国伦敦有region，2AZ架构。

3. 企业在GDPR框架下优先要做的动作建议

· 建立DPO团队，结合所处的行业和国家，帮助组织梳理清楚必须要遵守的法规和标准，评估企业目前的合规水位，创立可行的合规建设总体方案；

· 开展PIA（隐私影响评估）与DPIA（数据保护影响评估），生成评估报告；

· 生成数据资产地图，并记录针对数据的操作行为；

· 在数据处理的各个环节加入合规审计与评估功能，强制其符合合规要求；

· 建立DSR能力（Data Subject Rights Request，数据主体权利请求）；

· 评估SDK、Cookie等三方数据合规风险，进行简化与治理；

· 合规风险可视化能力建设，迅速捕捉合规风险涉及的数据、操作动作与系统，集中管控风险。

4.1.8 常见问题

1. 我的公司既不在欧盟境内成立，在欧盟境内也没有住址，我是否受到GDPR的管辖？

GDPR有域外效力：如果你的公司向欧盟居民提供商品或服务，或者您的处理数据、或者监控（数据）的行为发生在欧盟境内，即使您的公司并非欧盟境内成立，或在欧盟境内有住所的公司，仍然要受到GDPR的管辖。

2. GDPR合规，我们需要做什么？

- 合规实践需要有文件记录（documentation requirement）
- 两大领域的合规实践：隐私卫生与数据主体权利
- 隐私卫生：数据处理池、数据隐私合规产品设计、数据保护评估、72小时数据泄露通知义务、任命数据保护官（DPO）等等
- 数据主权利：访问权、修改权、删除权、获得信息的权利、限制处理的权利、撤回同意的权利、数据可转移的权利
- 熟悉GDPR的内容：注意每个欧盟成员国具体落地GDPR时候，本地的政策法规也会略有不同

3. 在GDPR合规上，阿里云服务能为我们公司带来什么好处？

- 阿里云服务满足行业标准，并提供如何在云上保护个人数据的最佳实践
- 阿里云实时监测政策动态，在出现影响到客户的政策变化时，作出积极响应和应对措施

4. 阿里云对客户的GDPR合规有什么支持？

- 阿里云为客户提供隐私管理建议
- 阿里云向我们的客户分享我们的隐私合规实践
- 阿里云联合生态伙伴提供的业务、技术合规的整体组训服务

5. 阿里云满足GDPR合规的要求吗？

- 是的，从2018年5月25日GDPR生效之日，阿里云满足GDPR合规的要求。

6. 在考虑GDPR合规时，选择欧美的云服务厂商，是否相对于选择中国云服务厂商更有地缘优势？

- GDPR对于合规要求，并不区分云厂商的地区，针对全球的IaaS服务提供者，要求都是统一的：向欧盟境内的客户提供产品或者服务时，必须满足GDPR的要求。

7. 除了购买合规的产品或者服务，企业日常运营中需要做到哪些关键动作？

- GDPR合规不仅仅是“安全”的工作，也不仅仅是“法务”工作，而是一个机构/组织管理成熟水位的整体体现，需要一起合作配合以做到如下三点：

（1）数据保护影响评估 (Data Protection Impact Assessment (DPIA))

（2）72小时内向数据保护机构报告数据违规的情况

（3）任命数据保护管（DPO，Data Protection Officer)

8. 阿里云合规和阿里云客户合规之间有什么关系？

阿里云满足GDPR合规要求，不代表阿里云的客户直接满足GDPR的合规要求。但是如果一家企业使用云厂商来处理业务时，云厂商的合规就是这家企业合规的必要非充分条件。

4.2 东南亚

东南亚我们主要关注新加坡，有三方面原因，一是新加坡的数据合规与隐私保护法律体系较为完整，二是新加坡往往也是中企出海东南亚的首选目的地，三是东南亚各国的数据合规与隐私保护法律体系大体都会参照新加坡的相关立法。因此，对企业来说，选择新加坡作为重点研究对象可以事半功倍，降低学习成本。

但毕竟东南亚国家较多，各国情况也都有自己的独特性和复杂性。由于文化上、地理上、经济上以及行业政策上的原因，不少汽车与新能源、消费电子、电商等行业客户出海到泰国的也很多。因此除了新加坡，我们也会对泰国数据合规进行简单的解读，以供读者参考。

4.2.1 新加坡PDPA简介

在新加坡，个人数据保护委员会（The Personal Data Protection Commission）来管理数据保护事宜。PDPC设立了2012年个人数据保护法（Personal Data Protection Act），这部法律部包括了对于个人数据的收集、使用、披露、保护等规范。

1. 什么是个人数据？

个人数据，是可以从该数据识别到个人身份的数据。

2. 什么是PDPA？

（1）PDPA（Personal Data Protection Act）是新加坡数据保护的基本准则

（2）这部法律部包括了对于个人数据的收集、使用、披露、保护等规范

（3）PDPA也建立了DNC登记机制（Do Not Call Registry），个人可以向DNC登记自己的手机号，选择不接受某些机构的电销信息

3. PDPA的目标

（1）平衡对个人数据的保护和机构收集、使用、披露个人数据的合理目的之间的关系

（2）防止个人数据滥用，维持个人对管理数据的机构的信任

（3）通过管理数据的流程，维持新加坡是值得信任的商业枢纽（Trusted Hub for Business）的地位

4. PDPA适用的范围

（1）PDPA 适用于（保护）所有的电子或非电子形式存储的数据

（2）但是PDPA一般不适用于：

- 个人出于个人或者住所目的所披露的信息
- 个人作为机构的员工所披露的信息
- 公共（政府）机构所收集、使用和披露的信息
- 商业联系信息：姓名、职位、商务电话号码、商务地址、商务邮箱、商务传真电话或其他类似的信息

5. PDPA下的数据保护义务有哪些？

（1）责任义务（Accountability Obligation）

- 数据保护政策、实践、投诉处理机制
- 任命DPO数据保护管 (Data Protection Officer)
- 机构的商务联系方式要公之于众

（2）通知义务：有意收集、使用、披露个人数据的机构需要通知该个人关于数据被收集、使用、披露的目的

（3）同意义务：

- 收集、使用、披露个人数据的前提，必须获得该个人的同意
- 同意是可以撤销的

（4）目的限制义务

- 必须有合理的目的
- 任何机构都不得以提供产品或者服务为条件，要求个人必须同意非合理范围内收集、使用和披露个人信息的行为

（5）准确性义务：应尽可能的保障收集的个人数据是准确的、完整的，特别是会影响到个人或者其他机构做相应决策的时候

（6）保护义务：避免非经授权的访问、收集、使用、披露（个人数据）

（7）保存期限义务：合理、合法的理由，不能超过必要合理的时间期限；

（8）传输限制义务：不能低于PDPA的保护标准

（9）访问和更正义务

- 个人提出要求时，组织必须向个人提供访问其个人数据的权限，以及在请求前一年内如何使用或披露数据的信息。
- 机构亦须在切实可行范围内尽快更正个人资料中的任何错误或遗漏，并将更正后的资料发送至披露个人资料的其他一年内披露该信息的机构（或个人已同意的选定机构）。

（10）数据泄露通知义务

· 如果发生数据泄露，组织必须采取措施评估它是否需要通知，对于个人数据的泄露必须要通知到数据主体。

· 如果数据泄露可能对个人造成重大伤害和/或规模很大，组织必须尽快通知 PDPC 和受影响的个人。

（11）数据可移植性义务：应个人的要求，组织必须以常用的机器可读格式，将组织拥有或控制的个人数据传输给另一个组织。

6. 处罚

若违反PDPA中的数据保护条款，组织或企业将被处以最高达该组织在新加坡年营业额10%的罚款（如果企业营业额超过了1000万新元），或在任何其他情况下最高达100万新元的罚款。

此外根据PDPA第51(2)条，如果未经授权而获取或更正了他人的个人数据，可处以不超过5000新元的罚款或不超过12个月的监禁，或两者并罚。

4.2.2 新加坡PDPA合规主要关注点

1. 数据本地存储要求

PDPA中没有数据本地存储的强制要求。

2. 数据跨境要求

在PDPA的规定中，任何组织或企业不得将任何个人数据转移到新加坡以外的国家或地区，除非能够根据PDPA规定的要求，确保转移个人数据能提供与PDPA相当的数据安全标准。企业或组织只有在采取适当措施确保数据接收方受可强制执行的法律义务约束，保证传输个人数据与本法保护标准相当时，才能将个人数据向第三国转移。

法律要求	具体内容	注意事项
被视为满足跨境传输要求的情况	1.个人同意或被视为同意； 2.对于保护数据主体利益以及国家利益是必要的，并且转移组织已采取合理措施； 3.个人数据是传输中的数据或个人数据在新加坡是公开的。	PDPA对此类视为同意进行严格限制，并列出视为同意的例外。
法律强制义务	1.法律； 2.订立的合约； 3.具有约束力的公司规则（Binding Corporate Rules）； 4.任何其他具有法律约束力的文书。	此外，PDPA规定个人数据的接收方被视为与转移组织“相关”的情形。
提供特定证明	亚太经合组织跨境隐私规则（“APEC CBPR”）体系和亚太经合组织处理者隐私认可（“APEC PRP”）下的认证系统。	

可以采用的可强制执行的法律义务约束包括以下三种：

· 法律

· 合同

· 公司约束规则或其他具有法律约束力的文书。

此外，满足如下四类特定情况下，个人数据也可以跨境传输：

· 个人同意，即数据主体明确同意；

· 个人被视为同意：即数据主体虽然没有实际同意，但经合理推断，数据主体将自愿提供数据，这要求组织或企业明确告知数据主体收集、使用或披露个人数据的目的，给予数据主体拒绝机会，并未遭受拒绝。此外企业或组织还要评估并确认，此处数据处理行为不会对数据主体产生不利影响；

· 跨境传输为数据处理所必须（例如跨境电商订单），并且企业或组织需要确保数据接收方不会基于其他目的处理接收到的个人数据；

· 传输数据属于中转或者已公开的数据。

3. 个人信息、隐私数据和敏感数据

在PDPA中，个人数据，是可以从该数据识别到个人身份的数据。

PDPA不区分个人数据和隐私数据、敏感数据。

4. 其他

PDPA中的处罚不仅包括经济处罚，还包括刑事处罚，这是和GDPR不同的一点。

4.2.3 新加坡PDPA合规建议

阿里云在PDPA中提供基础的云安全能力、数据安全与隐私保护能力、PDPA合规轻咨询服务等。

阿里云服务具备可以帮助客户遵新加坡个人数据保护法（PDPA）的技术和产品能力。帮助企业或组织做好符合PDPA要求的数据安全、数据传输、数据分享等场景。

此外，阿里云在新加坡和东南亚有丰富的节点资源分布，满足东南亚不同国家、区域的合规性要求：

· 阿里云在新加坡有Region，采用3AZ架构。

· 阿里云在泰国首都曼谷有1个AZ架构。

· 阿里云在马来西亚吉首都隆坡有一个Region，采用2AZ架构。

· 阿里云在印度尼西亚首都雅加达有一个Region，采用3AZ架构。

· 阿里云在菲律宾首都马尼拉有1个AZ架构。

企业在PDPA框架下优先要做的动作建议

· 建立DPO团队，结合所处的行业和国家，帮助组织梳理清楚必须要遵守的法规和标准，评估企业目前的合规水位，创立可行的合规建设总体方案；

· 对比PDPA要求，开展在数据安全领域的评估，衡量差距；

· 建立DSR能力（Data Subject Rights Request，数据主体权利请求），满足数据主体请求；

· 优化数据收集能力，根据PIA（隐私影响评估）来最小化数据收集范围；

· 合规风险可视化能力建设，迅速捕捉合规风险涉及的数据、操作动作与系统，集中管控风险。

4.2.4 泰国PDPA合规概览

1. 立法

《个人数据保护法》（Personal Data Protection Act，PDPA）于2022年6月1日生效，是泰国的首部在个人数据保护、数据合规领域的立法。该法包括了个人数据收集、使用、披露等的相关固定，且就违法违规处理个人数据的民事责任、刑事责任以及行政责任作出明确规定。

在《个人数据保护法》的基础上，泰国政府颁布了一系列的二级立法，包括《免除小型企业数据控制者记录》，《个人数据控制者安全措施》，《个人数据处理者个人数据处理活动记录的准备和保存标准和方法》和《专家委员会发布行政罚款和命令的标准》。

2. 监管机构

泰国个人数据保护委员会（Personal Data Protection Committee）负责后续法律的实施与监管。

3. 数据控制者收集处理个人数据的合法性依据

· 取得个人同意；

· 为实现为公共利益准备历史文件或档案有关的目的，或为与研究或统计有关的目的；

· 预防或抑制对自然人的生命、身体或健康的危险；

· 对履行与数据主体签订的合同是必要的，或为了在签订合同之前应数据主体的要求采取措施；
· 符合公众利益或行使授予的官方权力；
· 数据控制者、其他自然人或实体的合法利益，除非此类利益被数据主体关于个人数据的基本权利所凌驾；
· 对数据控制者遵守法律是必要的。

4. 对数据控制者的要求

· 数据收集目的限制：数据控制者收集个人数据应限制在与其合法目的相关的必要范围内；
· 通知义务：数据控制者应在处理个人数据之前告知处理的目的、保留期限等信息；
· 数据保留限制：数据控制者应告知数据主体个人数据的保留期限，如果无法指定此类保留期限，则需要指定数据保留标准所依据的预期数据保留期限；
· 数据安全与保护：数据控制者应提供适当的安全施以防止未经授权的或个人数据的非法丢失、访问、使用、更改或披露等；
· 数据记录准确性：数据控制者应确保个人数据准确、最新、完整以及不具有误导性；
· 数据处理记录：数据控制者应保留个人数据处理活动的记录，以供数据主体和PDPC检查，记录可以是书面或电子形式；
· 数据跨境转移限制：数据接收方应具有足够的数据保护标准，并应执行PDPC规定的个人数据保护规则；
· 数据泄漏通知：数据控制者必须立即通知PDPC个人数据泄露事件，并在可行的情况下，在知道该事件后的72小时内通知，如果个人数据泄露可能对个人的权利和自由造成高风险，数据控制者应及时将泄露事件和补救措施通知数据主体；
· 任命数据保护官：数据控制者在满足法定条件时应指定数据保护官
· 未成年人保护：对于不满十周岁的未成年人，数据控制者应当征得对儿童负有父母责任的人的同意

5. 数据主体权利

与新加坡PDPA类似，数据主体拥有数据知情权、访问权、数据可移植权、反对权、删除权、限制使用权、整改权。在此不赘述了。

6. 数据跨境

与新加坡的数据跨境规定类似，若组织跨境转移个人数据，接收方所在的国家或国际组织应具有足够的数据保护标准，并应按照PDPC颁布的标准或规定执行，但PDPC规定了几种例外情况：

· 为遵守法律规定；
· 已征得数据主体同意，但须告知目的地国家或国际组织的个人数据保护标准不足；
· 为履行数据主体为一方的合同所必需的，或为在签订合同前应数据主体的请求采取措施；
· 为维护数据主体的利益，遵守数据控制者与其他人或法人之间的合同；
· 为防止或者抑制对数据主体或者其他人的生命、身体或者健康的危险，在数据主体不能及时给予同意的情况下；
· 为开展涉及重大公共利益的活动所必需的。

7. 处罚

数据控制者违法违规处理个人数据，需要承担民事、刑事或者行政责任。
刑事处罚方面，企业高管或相关负责人员将面临最高一年的监禁，最高100万泰铢的罚款，或者两者兼而有之。
民事处罚方面，数据主体可要求惩罚性赔偿，但不得超过实际赔偿额的两倍。
行政处罚方面，最高可面临500万泰铢的罚款。

4.2.5 常见问题

1. 企业数据保护合规方案可以如何设置？

（1）基本动作
· 指定数据保护官 DPO
· 数据保护政策、数据保护措施，检查是否有欠缺的地方
· 设计一个合理的数据保护治理框架
（2）建设能力
· 员工教育：每个员工都要知道数据保护的重要性
· DPO能力框架、训练地图
· 内部培训
（3）建立个人数据管理体系问责制
· 获得数据保护信任标志认证（DPTM， Data Protection Trustmark）
· 在官方网站上展示满足PDPA的能力
· 组织内部成立数据保护管理体系

2. 数据库和服务器是不是应该本地部署？

根据PDPA，数据控制者不得将任何个人数据转移到新加坡以外的国家/地区，除非根据PDPA要求，转移组织采取适当的步骤确保个人数据的接收方受法律强制义务的约束，为传输的个人数据提供至少与PDPA相当的保护标准。数据本地化是数据跨境管理的措施质疑，一般要看该主权国家有没有制定相关的法律来限制本国或者本区域的数据向境外流动。新加坡没有禁止数据跨境流动，但对于数据的转移有程序上的要求。因此，建议本地化部署，这会降低潜在的法律风险以及数据处理成本。阿里云在新加坡设有Region，新加坡Region有全线的阿里云数据库与计算类产品，可以满足客户在新加坡本地的数据处理要求。
如果有不得不进行数据跨境处理的要求（例如运维和业务人员在国内，要远程查看或操作新加坡的数据），阿里云也提供了数据传输、存储和加密、安全等合规领域的保障能力。可以满足新加坡PDPA的要求。

4.3 北美

4.3.1 美国数据合规相关立法

1. 美国个人信息保护法概述与特

目前，美国没有统一的个人信息保护法，立法分散而多元化。按照美国联邦制政体规定，各州有权独立进行隐私立法，例如犹他州、弗吉尼亚州、科罗拉多州、康涅狄格州，而又以《加州消费者隐私法》（The California Consumer Privacy Act，简称CCPA）为典型。但分散的隐私法律给在美国经营的企业带来了较大合规成本，也给消费者维权带来了混乱，相关问题亟需联邦层面的解决方案。2022年，美国众议院能源和商业委员会主持了《美国数据隐私和保护法》（American Data Privacy and Protection Act, 以下简称“ADPPA”）的审阅修订工作，目前该法案仍属于众议院修订阶段，向前推进需要美国两党协商一致、经两院表决和总统签署后才能通过。令人关注的ADPPA具有如下特点：
（1）对“大数据持有者”受到额外限制，所谓大数据持有者指总收入超过2.5亿美元且处理500万个个人数据或20万个个人敏感数据的商业实体，而“小企业”享有额外的豁免。
（2）ADPPA通过后，作为联邦法律，效力上明确优于所有州级隐私法案。
（3）数据分类限定： ADPPA规定了各类型数据使用目的，企业在使用这些数据时时不能超出限定的目的。
总体上，美国主张个人信息跨境自由流动，实现经济效益的最大化；美国数据保护的模式，是用“市场调节”和“事后追责”两种手段结合实现国家监管和商业自由的平衡。

2. 立法目的

（1）公共领域：政府部门对个人信息的正确收集和使用；
（2）私有领域：针对不同的行业展开规范

3. 立法层级

（1）以前的联邦法律：
· 1914年《联邦贸易委员会法》
· 1970年《公平信用报告法》：保护公共领域的个人信息
· 1974年《隐私权法》、1978年《金融隐私权法》：保护私人领域的个人信息

· 1986年《电子通信隐私权法》：行业和市场调节
· 1996年《健康保险携带和责任法》（HIPAA）
· 2000年《儿童线上隐私保护法》（COPPA）

（2）新近法律或行政令
· 2018年3月，美国颁布《澄清域外合法使用数据法案》（Cloud Act）：
a)对美国机构获取域外个人信息和外国机构获取美国境内个人信息都予以了规定；
b)直接将数据管辖权从“属地原则”变成了“数据控制”管辖范围——只要美国企业对用户数据具有实际控制或管辖权，无论用户是否在境内，美国企业都有义务按规定保存、备份甚至向美国政府披露用户数据。
· 2018年《外国投资风险审查现代化法案》：凡涉及维护或收集美国公民敏感个人数据的任何投资交易，都必须接受美国外国投资委员会（CFIUS）的调查。
· 总统行政令：2019年发布的《确保信息和通信技术及服务供应链安全行政令》（EO13873）
· 总统行政令：2021年发布的《关于保护美国人的敏感数据不受外国敌对势力侵害的行政令》（EO14304）等

尤其是2019年和2021年的立法，统称ICTS安全审查行政令，这一系列若干行政令旨在针对对手国家（尤其是中国）在信息通讯硬件、软件和服务领域对美国造成的国家安全威胁。重点审查和评估包括外国应用软件程序在内的重点行业敏感数据安全风险。因此在美国开展业务的中国背景的公司尤其需要注意。

（3）州法案：
· 2018年加利福尼亚州颁布的《消费者隐私法案》(CCPA)：目前美国最严格的消费者个人信息保护法案
· 2021年3月，弗吉尼亚州通过《消费者数据保护法》

（4）行业自律规范：
· 建议性的行业指引
· 网络隐私图章认证计划
· 技术平台

4. 处罚

美国没有全国层面的数据保护机构，因此监管机构的执法权将取决于有关的具体法规。有些法律只允许联邦政府执法，有些允许联邦或州政府执法，有些允许受害消费者通过私人诉讼权维护法律权益。处罚的细则，取决于相关适用法律法规的具体要求。

4.3.2 美国数据合规主要关注点

1. 数据本地存储要求

美国的联邦立法层面没有规定数据必须要本地存储，但是对于一些特定行业，如医疗、金融、政府业务等，需要遵从各所在行业的特殊规定，可能会有数据本地存储的要求。如：
· 美国国防部要求向其提供服务的云计算服务提供者将相关数据存在美国境内；
· 美国国内收入署规定联邦机构必须将接收、处理、存储、传输联邦税务信息的信息系统的位置限制在美国境内、大使馆或军事设施；
出口管制领域下特定类型数据的本地化规则：美国政府可以禁止某些竞争国家可能带来国家安全风险的交易，比如涉及处理美国人敏感个人数据的硬件或者软件的交易。

2. 数据跨境要求

美国各项数据安全与合规方面的立法一定程度上是鼓励数据的自由流动，以实现商业利益的。美国签署了多种国际合约，禁止包括数据本地化措施在内的歧视性条款。例如，美国与日本的数字贸易协定和美国与墨西哥、加拿大的三方协定都明确禁止将限制数据存储和处理位置的数据本地化措施作为在相关地区开展业务的条件。这两个协议都提到亚太跨境隐私规则体系可以作为一个有效的机制在保护个人数据的基础上促进数据跨境传输。

3. 个人信息、隐私数据和敏感数据

由于美国各项立法的分散和混乱，具体如何区分并区别对待个人信息、敏感数据，目前需要遵从具体所在的州和所在行业的规定。在美国，与个人有关的信息通常被称为个人信息，而不是个人数据。个人信息的定义在所有州或所有法规中并不统一。
· COPPA：禁止从13岁以下儿童的在线和数字连接设备中收集任何信息，并要求在收集儿童信息时发布隐私通知并收集可核实的父母同意书。
· CCPA：个人信息是指与已识别或可识别人员相关的任何信息。CCPA中的定义与GDPR中关于个人信息的定义基本一致。但CCPA还包括了对家人和家庭数据的保护。
ADPPA：ADPPA定义的敏感数据比各项州立法更宽泛，包括收入水平、语音邮件和文字消息、日历信息、与17岁以下儿童有关的数据、以及对个人“穿着内衣”等的描述。

4. 其他

美国在个人数据保护立法方面是非常碎片化的，但随着美国各州关于个人数据保护法相关的法律越来越多，越来越杂，对联邦层面统一立法的需求将会越来越强烈。在美国经营的企业需要时刻关注ADPPA的立法进展，对一些很大可能会通过的条款做好提前应对，以争取有利的市场先机。

4.3.3 数据合规建议

虽然美国鼓励数据要素的自由流动，但数据要素的自由流动并不完全等同于数据的随意跨境。阿里云建议在美国开展业务的中国企业，如果数据来源是美国公民且服务对象也是美国企业或美国个人，则推荐数据本地存储，避免不必要的跨境传输。这和中国企业在美国的身份有一定的相关性，尤其是数据从美国往中国传输，将面临更高的合规风险以及更高的合规成本。实际上，随着全球范围内各主要经济体对数据合规与安全的越来越重视，以及对数据资产的意识越来越强，全球范围内的数据跨境流动成本和风险将会越来越高。此外，数据在美国的本地存储既能降低数据跨境的费用，也能提升在本地的服务体验。
阿里云在美国有两个region：
· 西海岸硅谷Region，采用2AZ架构；
· 东海岸弗吉尼亚Region，采用2AZ架构。

企业在美国的合规框架下（以CCPA为例）优先要做的动作建议
· 建立一个集中的合规中心，详细拆解CCPA各项要求；
· 评估消费者消费各环节的合规差距，主要是消费者进入、消费者识别、数据发现、数据删除以及安全响应；
· 给消费者提供可行途径，以拒绝基于行为的营销与广告的；
· 匹配映射消费者数据流，对每个环节的数据进行打标；
· 合规风险可视化能力建设，迅速捕捉合规风险涉及的数据、操作动作与系统，集中管控风险。

4.3.4 常见问题

1. 企业在美国经营必须使用美资云吗？

不是。可以使用阿里云。在法律层面上，除了一些特殊的行业规定（如为美国政府或军方提供服务），没有限制企业在美国经营必须选择美资的云服务厂商。

2. 企业保存的用户信息是否可以被政府获得？

政府数据调取需要走正规法律调查流程，数据征用和调查，需要符合美国法律法规的规定。

3. 阿里云在美国本地的实体怎么运营的？

阿里云在美国运营云业务的主体最终由阿里巴巴集团在美上市公司全资所有，在美国有当地履行供应链、产研、法务、市场、服务、业务等职能的团队，足以保障阿里云服务美国客户的能力。如果客户是注册在美国的公司，一般阿里云对应的签约主体可以是美国公司Alibaba Cloud US LLC，也可以是阿里云新加坡公司 ALIBABA CLOUD (SINGAPORE) PTE LTD.这是阿里云国际站的通用规则，官网成员协议（Membership Agreement）上可以看到。

4.4 日韩

4.4.1 日本数据合规相关立法

1. 日本关键的个人信息保护和安全法律法规

《个人信息保护法》(APPI)
《保护个人信息的基本政策》
《APPI 的实施条例》
《APPI 的执行令》
《个人信息保护法准则：一般规则》
《个人信息保护法准则：向海外第三方传输》
《个人信息保护法准则：针对第三方传输的确认和记录义务》
《个人信息保护法准则：匿名信息》
《关于个人信息保护法的公告：数据泄漏后的行动措施》
《个人信息保护法关于依据充分性决定处理从欧盟传输出的个人数据之补充规定》

4.4.2 日本数据合规主要关注点

1. 敏感/特殊个人数据

（1）按照日本法律，敏感/特殊个人数据包括：

- 揭示种族民族本源的个人数据
- 揭示政治观点的个人数据
- 揭示宗教或哲学信仰的个人数据
- 遗传数据
- 关于健康/医疗信息的数据
- 关于个人刑事定罪或记录的个人数据
- 其他

（2）收集或处理敏感个人数据需要明确的法律依据

- 数据主体已明确同意个人数据处理
- 数据处理是数据控制者或数据主体在就业、社会保障和社会保护法领域履行相应义务和行使特定权利所必需
- 数据处理是保护数据主体或其他自然人的切身利益所必需（如果数据主体在实际上或法律上无法给予许可）
- 数据处理涉及数据主体明确公开的个人数据
- 个人数据处理是保护公共卫生领域的公共利益所必需

2. 收集或处理未成年人的个人数据时，需要由由未成年人的父母/监护人同意或授权。APPI没有明确规定与未成年人有关的规则，民法典中有关成年人保护的特殊要求在一般情况下都适用。

3. 数据主体的权利包括：

- 数据主体访问本人的个人数据的权利
- 数据主体纠正/更正本人的不准确或不完整个人数据的权利
- 删除个人数据的权利
- 限制数据处理的权利

4. 数据控制者的义务：

日本的法律中并没有定义数据控制者和处理者的概念。但是，数据控制者必须：

（1）对处理者进行尽职调查，以确保其能提供恰当的安全保障并处理个人数据；
（2）控制者只能使用已签订书面协议（符合特定要求）的处理者。

5. 数据本地存储要求

目前日本个人数据保护法中没有针对数据本地化的法定要求，但是部分行业指南（如医疗保健/医疗行业）有数据本地化的相关规则。

6. 数据跨境传输限制

按照APPI的规定，原则上不允许个人数据的跨境传输，除非获得数据主体的同意。此外，还需向数据主体提供接收国个人数据保护制度，且第三方需要采取与日本个人信息保护措施同等的保护措施。日本PPC具有监督、要求第三方提供报告、实地检查等权力。在APPI统一规定的基础上，数据处理/传输者在有法律依据且以下情况之一适用的情况下，允许向第三国家/区域传输个人数据：

- 经充分核准/列入白名单的区域
- 特定资质的持有者或特定行为守则计划的参与者，且均已获得相关数据保护和安全机构（例如，欧盟/美国隐私保护框架）的批准。
- 豁免情形，例如同意、合同履行或者确立/行使/保护法律主张所必须的情形

其他解决方案总体来说，日本倾向于促进数据的跨境自由流通，日本是通过三个和数据跨境传输有关的区域协定来达到这个目的的，这帮助日本扩大了数据流通的范围。

- APEC-CBPR：APEC Cross-Border Privacy Rules System，于2011年11月被APEC领导人批准。CBPR通过由政府支持、第三方验证机构评估的数据隐私认证以及跨境隐私执法安排（CPEA），确保参加CBPR体系的组织实施符合CBPR要求的隐私政策和做法。企业或组织获得CBPR体系的认证，是日本PPC允许个人数据跨境传输的合法路径之一。目前这一框架内的国家/地区有9个：日本，美国，加拿大，澳大利亚，墨西哥，新加坡，韩国，菲律宾，中国台湾。
- CPTPP：全面与进步跨太平洋伙伴关系协定。2018年12月30日生效，CPTPP要求缔约方允许包括个人数据在内的跨境数据自由流动，同时给予缔约方在不构成对其他缔约方贸易歧视和变相限制的情况下基于“合法公共政策”的豁免；允许缔约方对计算机设施的使用根据安全保障和机密保护设有不同监管要求，同时不得将数据本地化作为市场准入条件的强制性要求以及相应的例外情形。目前加入CPTPP协定的国家有11个：日本、加拿大、澳大利亚、智利、新西兰、新加坡、文莱、马来西亚、越南、墨西哥和秘鲁。
- RCEP：区域全面经济伙伴关系协定，Regional Comprehensive Economic Partnership。在金融服务信息传输部分，RCEP要求缔约方不能阻止金融服务提供者进行其金融服务活动必需的相关信息传输；在电子商务章节中，RCEP要求缔约方不得将计算机设施必须置于境内的规定，作为进入该缔约方内部市场的前提条件，不得阻止正常经营活动中的信息跨境传输活动，同时为以上约束提供了实施“合法公共政策”和保护“基本安全利益”两种豁免情形。RCEP成员国包括15个国家：东盟10国（文莱、柬埔寨、印度尼西亚、老挝、马来西亚、缅甸、菲律宾、新加坡、泰国、越南）与中国、日本、韩国、澳大利亚、新西兰。

4.4.3 日本数据合规建议

日本的法律对于敏感数据有界定，因此，应该根据法律的规定，对数据进行分级分类处理。机构在处理个人数据时，应当建立数据保护机制，确保数据的收集和处理遵从最小必要原则，以及获得了数据主体的充分的授权。

日本法律对于数据跨境传输有一定限制，因此在选择数据处理的节点时，应当考虑接受地是否有充分的数据保护水平，或者是否是在传输白名单内。有条件的情况下，仍建议数据留存本地处理。

企业在日本数据合规的建议动作可以参考GDPR部分。

4.4.4 日本数据合规常见问题

1. 涉及数据跨境传输时，应该如何满足日本APPI合规遵从？

- 对于数据传输行为需要通知数据主体
- 任何任命第三方数据处理者之前，需要对这些供应商做充分的尽调工作

- 数据传输协议的内容需要满足APPI的要求
- 引入审计和监督的组织，来监督传输协议的正确履行

2. 违反APPI将会面临何种处罚？

- 针对不遵守区域内关键数据隐私和安全法的行为，APPI对某些违规行为最高处以六个月监禁（附带劳役）或300,000 日元（将近2万人民币）罚款。

4.4.5 韩国数据合规主要立法

在韩国，2020年8月生效的《个人信息保护法》（PIPA），管理个人信息的采集、使用和处理。同时，2020年10月，韩国政府也制定了PIPA执行令，对PIPA进行补充和增强。

2021年1月6日拟议的修正案引入了数据可携带权和拒绝自动化决策的权利，增加了向海外传输个人数据的方法，并将假名数据纳入要求销毁的范围。

2023年7月30日，韩国PIPC发布《个人信息保护法》规范解释和《2023年个人信息保护法标准解释例》：在线平台向海外传送信息需信息主体同意。

2023年8月3日，韩国个人信息保护委员会（PIPC）发布了《人工智能时代个人信息安全使用指南》（《指南》）。这是 PIPC 发布的首份人工智能领域指南，旨在帮助降低人工智能在隐私和数据保护方面的潜在风险，同时促进数据的安全使用与人工智能生态系统的进一步创新和发展。

其他具体的行业内也有关于处理个人信息的相关法律规定，例如：

- 信息和通信：IC Network Act规定网络服务商需要承担的信息保护责任
- 金融行业：UPCIA（Utilization and Protection of Credit Information Act）
- 交通：保护和使用地理位置信息法案
- 劳动法：保护工作场所和雇员的个人信息
- 健康行业：生物道德和安全法案、医疗服务法案保护医疗相关个人信息

数据合规监管机构：PIPC个人信息保护委员会。

4.4.6 韩国数据合规主要关注点

1. 根据韩国PIPA的要求，数据控制者需要承担以下责任：

- 必须明确定义处理个人信息的目的
- 收集个人信息遵从最小必要原则
- 获得数据主体的授权
- 仅仅在明确目的的范围内处理个人信息，避免超范围将个人信息用于其他目的，包括转移给第三方
- 数据存留期限到期后要及时删除销毁个人数据
- 保证个人数据的准确、完整和更新
- 在数据处理方式、数据类型选择上，考虑将风险最小化
- 数据泄露时及时通知数据主体
- 提供面向公众的隐私政策，保障个人的隐私权利
- 可行的条件下，使用匿名或者假名来处理个人信息
- 遵守PIPA和其他法律的规定
- 必须任命数据保护合规官（Data Protection Officer，简称DPO）

- 在可行的情况下，向PIPC注册个人信息档案
- 监督雇员、合同工、第三方对于数据处理的工作符合PIPA的要求

2. 韩国数据保护法律对于数据跨境的规定

PIPA要求个人信息控制者，在向位于韩国境外的第三方传输个人数据时，必须获得授权。然而， 个人信息控制者，如果是将个人数据分包（outsource）给韩国境外的机构处理，则不需要单独授权，但是必须：

- 遵守PIPA的披露要求
- 根据PIPA的要求征得数据主体的同意
- 与第三方数据处理者签订合理的数据处理协议

但需要注意的是，虽然韩国是APEC的成员国，也遵守APEC（亚太经济合作组织）跨境隐私规则CBPR，但在处理数据跨境传输时，仍需要遵守韩国的数据保护法律。

3. 韩国没有数据必须本地存储的要求

4.4.7 韩国数据合规建议

可以看到，韩国数据合规对于个人信息控制者的责任要求，与GDPR的要求从框架上较为类似。我们推荐，能建议一套通用的数据合规制度，以节省公司的运营成本。另外，韩国没有本土存储个人数据的明确要求，但在数据跨境这一块区分了转移和分包处理两种情况。在韩国运营的公司，如果涉及到跨境的业务，应当根据PIPA的要求，按照分包处理的情形，签订数据处理协议，明确数据保护机制。

企业在韩国数据合规的建议动作可以参考GDPR部分。

4.4.8 韩国数据合规常见问题

1. 涉及数据跨境传输，是否需要监管部门批准数据传输协议？

一般来说，不需要。但是，如果某个行业的数据保护法律适用时，可能会需要相关监管部门的批准（主要是要关注信息通信行业和金融行业）。

2. 违反韩国数据保护法有什么法律后果？

（1）行政处罚

a) 重大PIPA违法行为，个人信息控制者，将会面临：

- 最高十年监禁；或者
- 最高1亿韩元的罚款

b) 一般PIPA违法行为， 个人信息控制者，将会面临：

- 责令改正，或者
- 最高5000万韩元的行政罚款，或者
- 年周转金额的3%

（2）民事侵权赔偿：最高三倍损失的赔偿金

4.5 印度

4.5.1 印度数据合规相关立法

印度2021年引入的数据保护法案。

2008年IT修正法案有提到一些关于个人数据保护的内容，但这部法案主要还是关注信息安全。有一些行业性的规范管理相关个人数据保护问题，例如：

· 金融行业：Aadhaar Act of 2016：允许金融机构使用个人生物信息识别开户自然人的身份；Credit Information Companies (Regulation) Act, 2005： 对于银行客户信息保密和保护要求
· 保险行业：要求保险公司保护用户信息
· 通信行业：IT Act, IT Amendment Act，IT Rules 2021，Indian Telegraph Act.

4.5.2 2023年8月，印度《2023年数字个人数据保护法案》获得上议院和下议院批准。该法案对数字个人数据的处理进行了规范，旨在保障数据主体的权利并确保个人数据被合法处理。该法案适用于在印度境内，以数字形式收集或处理的个人数据。如果数据处理行为与向印度境内的数据主体提供的产品或服务相关，则该法案同样适用。印度数据合规主要关注点

1. 印度法律下，数据处理者的责任
（1）合理的安全措施和程序
（2）合理的目的：仅仅在必须、合法、仅限于目的范围内使用和收集信息、保存合理的期限
（3）处理敏感个人数据（SPDI）时，必须获得数据主体的事前书面授权，且该授权是可以撤回的
（4）向第三方转移敏感个人数据时，无论是在印度境内还是境外啊，必须：
· 数据接收方必须有同等水平的隐私保护
· 数据转移是为了与数据主体订立合同之必须，且数据主体已经同意了该项转移
（5）机构必须要提供完备的隐私政策，说明讲如何处理个人敏感数据
（6）机构必须要任命一位申诉官，将他的联系方式公之于众，申诉官负责处理数据主体的投诉，且必须在一个月内回复

2. 印度法律下，数据主体的权利
（1）被知会的权利
（2）访问权
（3）修正和更新全
（4）撤销同意授权的权利
（5）需要注意的事情是，印度法律没有认可数据主体的其他权利，例如，反对处理权、数据转移权、以及要求机构删除某些特殊数据的权利

3. 印度法律下，关于个人数据保护的安全措施的要求：
（1）满足IS/ISO/IEC 27001认证要求
（2）达到其他政府认可的认证机构的安全认证

4. 收集个人数据需要数据主体的明确同意。需要告知数据主体数据收集的目的和用途。用途需要合理合法，包括：个人出于自愿而提供指定用途的数据、政府服务或福利目的需要的数据、紧急医疗情况需要的数据、出于就业目的。这些目的是无需个人同意的，其他的目的需要个人同意。

5. 未成年人保护：对于18岁以下的未成年人，将由其父母或法定监护人提供同意书。

6. 数据跨境限制：
（1）如果接受地的数据合规能够满足印度法律的要求，则跨境传输没有特别限制；
（2）法律要求，数据传输需要满足与数据主体订立合同所必须，并且需要得到数据主体的授权认可；
（3）印度政府有权限制个人数据传输到指定的国家。

4.5.3 印度数据合规建议

虽然印度法律没有命令禁止数据的跨境传输，但是敏感个人数据向第三方转移，都需要满足两点原则：1）与数据主体履行合同之必须 2）获得数据主体的授权。因此，如果收集印度用户的个人信息，需要明确，是否属于法律规定的敏感个人数据，且需要明确的隐私政策机制，获得用户的明确授权。

企业在印度的数据合规的建议动作可以参考GDPR部分。虽然印度尚未有全国统一的数据安全或隐私保护相关法规，但印度目前在审核的草案是参考GDPR拟定的。企业可以未雨绸缪准备起来。

4.5.4 常见问题

1. 违反印度的数据保护相关法律，会有何种法律后果？
· 侵权赔偿：以违反IT法案“合理安全措施”，造成自然人损失的，承担侵权赔偿责任
· 刑事责任：违反合同或者不经数据主体同意泄露个人信息的，最高处三年监禁，罚款50万INR
· 刑事责任：公司拒绝向CERT-In(计算机应急小组)提供信息，或者不遵守CERT决定的，处最高1年监禁或罚款10万INR，或并罚

2. 是否有数据本地存储的要求？
· 特定行业的数据有本地存储的要求，例如：支付信息、公司账目财务信息、保险理赔案件信息等

4.6 南美

南美国家众多，其中巴西无论从经济体量还是文化影响力，都是南美当之无愧的第一。不仅如此，中国企业出海南美，选择最多的国家也是巴西。因此本节主要对巴西的数据合规进行解读，并简要概括下阿根廷的情况。

4.6.1 巴西数据合规主要立法

《巴西通用数据保护法》，The General Data Protection Law（LGPD）是巴西的主要个人数据保护立法。LGPD于2018年8月颁布，并于2020年9月18日生效，LGPD规定的行政处罚相关条款于2021年8月生效。LGPD较多地借鉴了欧盟GDPR的相关内容和指导思想。

除了LGPD，与数据合规、个人隐私保护相关的法规还有：

· 《巴西信息获取法》，2011年颁布，用于指导巴西公共信息的获取。
· 《巴西消费者保护法》，1990年颁布，规定如果数据库记录消费者信息，需要告知消费者。同时数据库中不能记录任何超过五年的负面信息。同时消费者必须被允许访问收集到的关于他们的信息，也有权要求任何被认为必要的修改。
· 《巴西互联网法》，2014年颁布，规定了适用于应用程序提供商的规则，例如应用程序登录访问日志信息需要存储六个月。
· 《巴西民法》，2002年颁布，保证个人有权寻求司法介入以保护其隐私权免受侵犯、有权要求对由此产生的所有损害索求赔偿。
· 银行和医疗卫生行业的行业立法，如《巴西良好数据法》（2011年颁布）、《巴西银行保密法》（2001年颁布）、《巴西网络安全条例》（2021年颁布）

巴西合规监管机构：巴西国家数据保护局（The Brazilian National Data Protection Authority，简称"ANPD"），2018年12月28日成立。

总体来说，巴西LGPD和欧盟GDPR高度类似。

4.6.2 巴西数据合规主要关注点

1. 关键定义：LGPD中对于个人数据、数据控制者、数据处理者、敏感个人数据的定义和欧盟GDPR类似。

2. 管辖范围：LGPD有治外法权，无论企业在哪个国家成立或用于数据处理的服务器在哪个国家，它适用于三类情形，三者是“或”的关系：

（1）数据处理的行为发生在巴西境内；

（2）处理活动旨在提供产品或服务，或处理位于巴西境内的个人数据；

（3）所处理的个人数据产生于巴西境内；

3. 数据主体权利保障：高度类似欧盟GDPR中关于数据主体权利的保护，保护数据主体的数据可携带权、删除权、撤销同意权、拒绝营销权、遗忘权等。

4. 营销场景：巴西消费者保护法》规定了适用于营销行为的广告商和供应商的若干义务。 营销信息应该有一个退出选项，让消费者可以选择停止接收直接营销信息。

5. 数据跨境：只有在符合LGPD规定的情形下，巴西个人数据才允许出境。

（1）数据目的国提供与LGPD规定的同等水平的充分保护；

（2）情报、调查和起诉机构之间的国际法律合作所必需的转移；

（3）为保护数据主体或其他人的生命或身体安全必需的转移；

（4）国家当局批准的转移；

（5）根据国际合作协议的转移；

（6）为执行或实施公共政策或公共服务所必需的转移；

（7）经数据主体单独同意的转移。

（8）数据控制者通过使用特定的合同条款、标准合同条款、全球公司条款或行为准则来确保个人数据保障措施。

但金融行业有特殊规定，巴西央行对巴西个人金融数据的境外存储有约束和限制。

需要注意的事，巴西虽然有跨境数据白名单制度，但是还没有数据跨境的具体白名单国家。

6. 数据泄露通报义务：数据控制者尽量在48小时向ANPD和受影响的个人通报数据泄露事件。对于一些特殊行业，还需要根据情况向某些指定机构通报。如巴西央行、巴西证券委员会等。

7. 处罚：

（1）警告，并明确采取纠正措施的时限；

（2）处以上一个财政年度在巴西的法人实体总收入不超过2%的罚款（不含税），最高上限为5000万雷亚尔（约58万元人民币）。

（3）对外披露和公布违规行为；

（4）阻止违规行为涉及的个人数据处理活动，直到对其进行规范化；

（5）删除违规行为涉及的个人数据；

（6）部分暂停对涉违规数据库的操作，最长不超过六个月，可再延长同样的时间，直到数据控制者将处理活动正常化为止；

（7）暂停与违规行为有关的个人数据处理活动，最长不超过六个月，可以再延长同样的时间；

（8）部分或全部禁止与数据处理有关的活动；

4.6.3 巴西数据合规建议

可以看到，巴西LGPD对于个人信息控制者的责任要求，与GDPR的要求从框架上较为类似。因此企业在巴西数据合规的建议动作可以参考GDPR部分。相对来说，巴西的LGPD的条文规定是较为严格的。

4.6.4 阿根廷数据合规概览

1. 立法

阿根廷的个人数据保护法（PERSONAL DATA PROTECTION ACT，"DPA"）和1558/2001号法令条例都于2000年11月生效。最近一次DPA的修订草案于2022年11月生效。

2. 监管机构

阿根廷的数据合规监管机构为APPI（Agency for Access to Public Information），APPI可以发布行政禁令。

3. 数据控制者收集处理个人数据的合法性依据

在阿根廷收集需要得到数据主体的明确同意，必须以明显和明确的方式说明获取同意的性质和数据的用途。但DPA不强制要求任何固定审批手续的来获得个人同意。

如果是姓名、国民身份证号码、税务或社会保障身份、职业、出生日期和地址的清单这样的个人数据，且这些数据来源于公共领域，或者是为国家履行政府职能或法定义务而收取，则无需获得个人同意。

如果个人数据产生于合同关系或金融实体进行的交易，或出于科研目的做个人数据的收集与统计，也无需获得个人同意。

获得处理敏感个人数据的同意必须是明确和知情的，采用书面形式或类似形式来获得个人同意。敏感数据指揭示种族和民族血统、政治观点、宗教、哲学或道德信仰、工会会员资格的个人数据，以及有关健康状况或性习惯或行为的信息。

4. 对数据控制者的要求

· 数据泄露通知：DPA中没有强制规定数据泄露通知的义务，但APPI有这方面的建议，企业在阿根廷最好主动履行通知义务，以长期可信、持续经营；

· 数据安全与保护：DPA中的安全义务要求数据控制者和数据处理者使用措施来检测任何未经授权的对个人数据的访问或修改；

· 任命数据保护官：不强制要求设立数据保护官；

· 未成年人保护：对于18岁以下未成年人的个人数据收集需求，必须由父母或法定监护人明确同意给予。

5. 数据主体权利

阿根廷对数据主体权利的维护并不像巴西那么严格。数据主体有知情权，数据获取权（如果数据主体的个人数据被纳入公共数据库或私人数据库，那么数据主体有权查阅其个人数据，如果个人数据涉及到一个已故的人，他们的继承人有权代表遗产行使这一权利），但对数据可携带权和数据遗忘权没有规定。

6. 数据跨境

DPA禁止向未提供充分保护水平的国家或国际或超国家实体转移任何类型的个人信息，除非获得数据主体的明确同意。此外，阿根廷有一系列白名单国家，白名单中的国家被认为提供了足够的保护水平，这些国家包括欧盟和欧洲经济区的成员国、瑞士、根西岛和泽西岛、马恩岛、法罗群岛、加拿大（仅限私营部门）、新西兰、安道尔和乌拉圭。

7. 处罚

数据控制者违法违规处理个人数据，需要承担刑事或者行政责任。

刑事处罚方面：如果故意在个人数据库中插入虚假信息，最高可判处两年监禁；(ii若故意向第三方提供个人数据库中的虚假信息，最高可判处三年监禁；若侵入个人数据库或泄露数据库中的机密信息，最高可判处三年监禁。如果对数据主体造成伤害，或者犯罪行为是由公职人员在行使其职责时实施的，则会加重处罚。

行政处罚方面：行政处罚可由APPI实施，包括警告、暂停、关闭数据库或最高金额为500万阿根廷法郎的罚款。

4.6.5 常见问题

1. Q：巴西个人数据要本地存储吗？

A：一般来说不需要，除非特殊行业有自己的规定。

2. Q：巴西的数据合规违规处罚有哪些参考案例?

A：2023年7月电话营销公司Telekall Infoservice收到警告和两张罚单，每张罚单的金额为7200雷亚尔，这是巴西首次实施对违法LGPD的判罚。Telekall因违反数据保护法的三条规定而受到处罚。这三条分别是：未在公司内部指定数据保护负责人、处理个人数据缺乏法律依据以及未配合监管程序。

4.7 澳新

澳新指的是澳大利亚和新西兰。由于澳大利亚经济在大洋洲具有压倒性的优势，绝大部分中国企业出海大洋洲首选都是澳大利亚，因此本节仅着重解读分析澳大利亚的数据合规情况。

4.7.1 澳大利亚数据合规主要立法

联邦层面：

《隐私法》，The Privacy Act是澳大利亚联邦层面的主要个人数据保护立法，于1988年颁布。《隐私法》适用于 "APP（Australia Privacy Principles）管辖实体"，包括联邦政府机构和私营部门组织（个人、法人团体、合伙企业、非法人组织和信托机构 （individuals, bodies corporate, partnerships, unincorporated associations, and trusts））， 除非它们是小企业经营者 small business operator、注册政党或州或地区当局。小企业经营者是指在一个财政年度内年营业额在300万澳元或以下的组织。

Do Not Call Register Act 2006 (Cth)（DNCR法），规定了对未经请求的电话的限制，于2006年颁布。

Anti-Money Laundering and Counter-Terrorism Financing Act，包含了有关根据该法获得的信息需要遵守澳大利亚隐私原则的规定，2006年颁布。

州层面：

Workplace Privacy Act 2011（澳大利亚首都地区）；

Privacy and Personal Information Protection Act 1998（新南威尔士州）；

Information Privacy Act 2014（澳大利亚首都地区）；

Information Privacy Act 2009（昆士兰州）；

Invasion of Privacy Act 1971（昆士兰州）；

Privacy and Data Protection Act 2014（维州）；

Personal Information Protection Act（塔州）。

澳大利亚的个人数据保护的监管机构也比较分散，主要包括如下几个机构（以下关于监管机构的信息来自公众号“Compliance Geeks合规小组”）：

· 澳大利亚信息专员办公室（The Office of the Australian Information Commissioner，OAIC）负责《隐私法》规定的数据保护工作；

· 澳大利亚通信和媒体管理局（The Australian Communications and Media Authority ，ACMA）依据《国家版权法》（DNCR Act ）和《垃圾邮件法》（Spam Act）负责保护公民个人隐私；

· 澳大利亚竞争和消费者委员会（The Australian Competition and Consumer Commission，ACCC）负责根据《2010年竞争和消费者法案》（The Competition and Consumer Act 2010 (Cth)）（Cth）保护CDR；

· 澳大利亚金融审慎监管局（Australian Prudential Regulation Authority，APRA）负责根据CPS231和CPS234赋予的监管权力执法；

· 澳大利亚总检察长根据《1979年电信（拦截和访问）法》（Telecommunications (Interception and Access) Act 1979 (Cth)）对数据隐私方面负有保护责任和执法权力；

· 澳大利亚金融交易报告和分析中心（AUSTRAC）有责任去保护根据《2006年反洗钱和反恐怖主义融资法》（Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)）获得的个人信息。

4.7.2 澳大利亚数据合规主要关注点

总体来说，澳大利亚的个人数据保护法体系和欧盟GDPR有较大差别，澳大利亚不像大部分国家，没有照搬GDPR的原则和逻辑。

1.关键定义：在澳大利亚《隐私法》中，没有区分数据处理者与数据控制者，而是统一用APP Entity（Australia Privacy Principles Entity）来指代。此外，《隐私法》中也不使用“数据主体”这样的指代，而是使用“个人”，即自然人。对于敏感数据，《隐私法》是有明确的规定的，它指的是：个人种族或民族血统信息、个人的政治观点、政治或党派成员信息、宗教信仰信息、哲学信仰、工会成员信息、专业类协会的成员信息、性取向或性行为信息、犯罪记录、有关个人的健康信息、不属于健康信息的个人遗传信息、将用于自动生物识别验证或生物识别的生物识别信息。

2.管辖范围：无论某家企业是否位于澳大利亚境内，只要这个APP Entity有澳大利亚联系（Australia Link）就会收到澳大利亚个人数据保护法的管辖。所谓Australia Link指的是此APP Entity收集或处理了澳大利亚人的个人数据（除非是持有护照或其他再限定时间内必须离开澳大利亚的人，否则其他在澳大利亚土地上的人都是“澳大利亚人”），或者向澳大利亚公民进行营销推广的离岸实体或网站。

3.营销场景：原则上禁止以直接营销为目的使用或披露个人信息。此外，将数据发送给另一家公司，接受个人信息的公司利用这些信息来进行营销也是不被允许的。除非得到个人的明确同意。但政府机构、政党和慈善机构向个人发送电子信息属于例外豁免的情形。2023年7月26日，澳大利亚联邦法院对Meta旗下两家子公司脸书（Facebook Israel）和Onavo（Onavo Inc）分别处以1000万澳元罚款，理由是两家公司在Onavo Protect应用程序的数据使用方面存在误导消费者的行为。在未向消费者披露的情况下，将消费者的个人活动数据，包括使用应用程序时的位置、应用程序访问记录和使用时间等数据以匿名汇总形式提供给Meta以实现其他商业目的，例如广告和营销活动、改进产品和服务以及制定商业战略等。

4.数据跨境：澳大利亚不禁止数据跨境，根据1988 年《隐私法》，要求“海外接收者”需满足两个条件：一是接受者位于澳大利亚及其附属领地外；二是接受者不能是数据披露主体。如果个人数据仅仅因为路由缘故短暂存储于澳大利亚境外，却没有被访问的话，可以不受《隐私法》关于跨境数据流动原则的约束。澳大利亚分散立法，对于政府数据、健康数据和个人隐私数据的出境都有不同的规定。对于数据出境行使监管的主要机构是澳大利亚信息专员办公室（OAIC）。

5.数据安全：澳大利亚《数据安全标准》规定了关于数据存储、保密性、完整性以及可用性等各个方面的标准，以保证数据隐私得到充分保护。澳大利亚的网络安全响应中心（Australian Cyber Security Centre），制定了详细的网络与数据安全事件响应指南，以保证对网络与数据安全事件的快速响应和处理。同时政府也建立了相关的网络安全信息共享和协作机制，以及网络与数据安全事件报告制度，以便快速掌握和了解网络安全事件的情况。

6.数据泄露通知：澳大利亚对所有“符合条件的数据泄露”进行了强制性通知。在实体发生数据泄露后尽快通知OAIC和所有受影响的个人。

7.处罚：澳大利亚隐私保护法的域外条款的范围扩大后，使更多的组织面临新的拟议处罚制度。对于法人团体，罚款将从220万澳元增加到不超过以下两项中较大的数额：

· 10,000,000澳元；

· 如法院能确定法人团体和任何相关法人团体直接或间接获得的、可合理归因于构成违反行为的利益的价值，则处罚金额为该利益价值3倍；

如法院不能确定该利益价值，则该法人团体在截至该法人团体从事或开始从事构成违法行为的月份末的12个月期间的相关营业额的10%。

4.7.3 阿里云数据合规建议方案

对于在澳大利亚经营的或有 “Australia Link” 的公司，需要认真遵守澳大利亚监管当局关于数据安全保护与营销等场景的相关规定。澳大利亚遵从判例法，各项合规相关的规定虽然比较分散，但能够组成一个完整的拼图且并不互相冲突。分散的立法有助于企业在面对不同场景和处理不同数据时都能有较为切实可依的法规。

由于澳大利亚并不禁止数据出境，企业可以既可以将澳大利亚的数据在澳大利亚境内的云厂商进行处理，也可以将数据传到云资源更为丰富的一些区域去处理，如美国、新加坡等。

阿里云建议在澳大利亚开展业务的中国企业：对数据进行分类标识；对于个人健康数据必须本地存储，严禁数据跨境传输；对于政府数据添加保护性标识，标识包括数据需要保护的机密性，以及数据使用、存储、传输和销毁需要满足的保护性措施；建立政府数据风险评估机制；当设立数据中心时，制定适用于整个政府数据外包过程的风险评估流程。同时，每家企业都需要根据不同业务要求和操作环境，确定自身风险承受水平，并采用相应的保护措施以减轻数据合规风险。

阿里云在美国、悉尼、新加坡都有region，在各个区域也都有开展云业务相关的合规认证，足以满足企业在澳大利亚开展业务的合规性要求。

企业在澳大利亚的合规框架下（以个人健康数据为例）优先要做的动作建议：

- 建立数据合规评估流程，识别数据分类并盘点个人健康数据；
- 评估涉及个人健康数据的数据流各环节的合规差距，包括数据采集、存储、处理、传输是否跨境，数据安全保护及数据权利行使；
- 发生数据泄露事件的应急响应流程，建议一次应急演练消除潜在风险点；
- 对患者数据流转场景的存在数据风险场景，逐一进行数据安全保护设计及数据合规管控；
- 建立数据合规体系建设，建议通过安全技术工具或系统，例如SIEM系统，迅速采集与分析安全日志事件进行事件预警。

4.7.4 常见问题

1. Q：澳大利亚个人数据要本地存储吗？

A：一般来说不需要，除非特殊行业有自己的规定。

2. Q：澳大利亚的数据出境白名单国家都有哪些？

A：澳大利亚的暂时没有拟定数据出境的白名单。但有不少国家对澳大利亚是提供白名单待遇的，其中有英国、马来西亚、阿联酋、俄罗斯等。

3. Q：澳大利亚个人数据出境需要报备或申报吗？

A：绝大部分场景下，没有任何登记、通知以及事先批准的规定。但澳大利亚信息专员办公室（OAIC）期望双方可以制定可执行的协议。根据《隐私法》规定，澳大利亚实体对境外接收方违反《隐私法》的违约行为负有法律责任，因为澳洲实体有理由相信外国接收方会遵守《隐私法》的规定而进行跨境传输个人数据。

4. Q：企业在澳洲开展业务必须注册实体公司吗？

A：大部分情况不需要，但是对于医疗健康行业，需要实体公司注册获得营业执照，才能开展行业相关业务活动。

5. Q：企业在澳洲存储的个人数据哪些可以跨境传输？

A：除了个人健康数据外的其他个人数据，在做好数据安全和合规管控情况下可以跨境传输。

6. Q：中国企业在澳洲开展业务如有信息系统处理个人健康数据怎么样合规？

A：公司在处理健康相关数据前，必须建设本地化的数据中心，或将相关服务外包至澳大利亚境内服务商。如需要从海外访问相关数据，则必须建立数据跨境传输管控机制，例如避免从澳洲境外直接访问澳洲本地化存储的健康数据。

4.8 中东区域

中东比较有代表性的两个国家是沙特和阿联酋。总体上来说，两国对于个人数据定义、数据主体权利等方面的定义差别不大，但在数据本地存储、数据跨境方面则有着较大区别。沙特较为严格，阿联酋相对自由宽松。

4.8.1 沙特数据合规主要立法

沙特和《个人数据保护法》(the Personal Data Protection Law, PDPL)和《沙特阿拉伯境外个人数据传输规定》是沙特在数据合规层面的主要立法。这两项法规在2023年9月14日正式生效。PDPL超越了一般伊斯兰教法对于隐私和个人数据的规定，该法律旨在规范数据传输并确保个人数据的隐私。除此之外沙特还有一些适用于特定部门和行业的立法。

沙特的数据合规监管机构为沙特数据和人工智能管理局(Saudi Authority for Data and Artificial Intelligence)。

4.8.2 沙特数据合规主要关注点

1. 适用范围：适用于在沙特境内处理与个人相关的个人数据，包括由沙特以外的任何实体处理居住在沙特的个人的个人数据。

2. 数据保护官任命：在沙特境外经营并处理沙特公民个人数据的控制者必须在沙特王国任命一名代表,以便主管当局在遵守适用法律方面可以进行询问监管。

3. 个人数据处理的原则：总体来说和GDPR类似。

（1）处理数据并向数据主体发送营销材料需要获得数据主体的书面同意。如果是儿童或无行为能力的个人数据，则需要获得法定监护人的同意；

（2）控制者必须制定隐私政策，在收集个人数据之前让数据主体查看，规定收集的目的，收集的个人数据的类别，收集的方式，存储的方式，处理，删除，以及数据主体权利和如何行使这些权利；

（3）控制者不得在未采取足够措施检查个人数据是否最新、准确、完整和符合收集目的的情况下处理这些数据；

（4）控制者必须保存其处理活动的记录，并在行政法规规定的期限内保存；

（5）控制者需要根据其处理活动的性质，对处理个人数据的后果进行评估，并指出执行条例应规定此类评估的相关要求。

4. 数据泄露通知：如果违规行为会对数据或数据主体造成严重损害，控制者应在意识到违规行为和数据主体后立即通知监管机构。

5. 企业内部责任：必须指定隐私政策，建立内部审查机制、最小化处理数据原则、为数据处理活动建立保障、记录数据以符合监管机构所需要的策略、程序和操作等。

6. 数据跨境：个人数据不得转移到沙特阿拉伯境外（履行公约规定的义务或服务于沙特阿拉伯王国的利益除外），除非满足以下条件：

（1）转移不会损害国家安全；

（2）为保护所转移数据的机密性提供充分的保证，因此保护级别与数据保护法中规定的相同；

（3）为履行数据主体义务；

（4）转移仅限于所需的最低个人数据；

（5）监管机构根据条例批准转移。

总体来说，沙特既对数据本地存储有要求，而且对于数据出境有着严格的限制。

7. 营销：未经收件人同意或使用选择退出机制，个人数据不得用于营销目的。

8. 特种数据保护：PDPL中规定了适用于健康数据处理的额外要求。控制者在处理个人健康相关数据时必须采取的一定的额外措施。其中包括：遵守沙特卫生部和沙特卫生委员会实施的政策和要求、在员工行为准则中反映《防止歧视法》的要求、PDPL执行条例中和所有其他有关适用的要求。对数据控制者的这些要求也必须被纳入与数据处理者的合同中

4.8.3 沙特数据合规建议

由于沙特对于数据本地存储有要求，企业在沙特经营，凡是涉及到处理沙特公民个人数据的，尽量选择对这些数据进行本地存储。阿里云在沙特利雅得有region分布，其中有两个AZ，在沙特经营的企业可以选择阿里云利雅得节点来承载业务。

如果要做沙特的数据出境，则数据控制者须向主管部门申请并获得批准之后，才可以将个人数据传输到沙特之外。申请必须在传输前至少30天提出，保护部门最初有 30天时间审查申请，并可酌情延长这一期限，批准的请求将被保护部门逐一评估。如果这些例外都不适用，企业则必须要建立本地的数据中心。

4.8.4 阿联酋数据合规主要立法

2021年9月《阿联酋联邦个保法》获得阿联酋内阁通过并生效。该法既遵循属地原则也遵循属人原则，即：既适用于位于阿联酋联邦的数据控制者或数据处理者的个人数据处理行为，也适用于虽在阿联酋境外但对阿联酋境内的数据主体进行处理活动的每个数据控制者或数据处理者。

阿联酋对于数据安全、个人数据保护方面的立法还是比较完善和成体系的。除了个保法之外，《阿联酋消费者保护法》、《阿联酋刑法》、《阿联酋民事交易法》、《阿联酋网络犯罪法》和《阿联酋劳动法》中都有对个人数据相关的保护要求和规定。

每个酋长国还有权通过适用于其管辖范围内实体的法律。迪拜酋长国在这方面最为积极，增加了两项关键的隐私规则：《迪拜酋长国数据传播和交换法》和《迪拜酋长国统计中心法》（Law on Data Dissemination and Exchange & Dubai Statistics Centre Law）。其规定相关当局在执行其任务和权限时，应采用的与数据传播有关的政策、机制、规则和标准。以及从事统计活动或研究时，收集的个人数据的保密性要求。这些数据的任何交换或转让都只允许通过迪拜统计中心进行，前提是它事先获得了数据主体的同意。

除了酋长国自己的立法，阿联酋各行业还有自己的立法。包括：《阿联酋中央银行法》、《阿联酋中央银行消费者保护条例》、《电信消费者保护条例》《电信部门监管法》《阿联酋卫生数据法》/《信息通信技术卫生法》《阿联酋储值工具条例》。这些特定行业的法律会对这些行业的企业以及与之相关的数据类型进行监管，一家企业是否收到监管并不取决于它本身所处的行业，而是取决于它的数据处理行为是否触及到了上述各行业立法的相关规定。

由此可见，阿联酋的个人数据合规相关立法是比较全面和立体的，也带来了一定的复杂性。企业在当地开展商业活动时需要认真对待。

阿联酋的数据合规监管机构是阿联酋信息技术部（United Arab Emirates Telecommunications Regulatory Authority，TRA）。

4.8.5 阿联酋数据合规主要关注点

1. 适用范围：既适用于位于阿联酋联邦的数据控制者或数据处理者的个人数据处理行为，也适用于虽在阿联酋境外但对阿联酋境内的数据主体进行处理活动的每个数据控制者或数据处理者。

2. 数据保护官任命：阿联酋法律允许组织的DPO为员工或外包给具有专业知识的第三方。并非所有组织都需要一个DPO，但有一个可以向监管机构表明企业对待隐私合规的认真态度，增强信任。如果进行高风险、高度机密或私人性质的处理，或如果处理过程包括对敏感的个人信息进行的系统评估，如剖析或自动处理，或如果需要大规模并行处理敏感个人信息，则必须要任命DPO。

3. 如果处理过程包括对敏感的个人信息进行系统评估，如剖析或自动处理；和/或

4. 数据控制者的义务：
（1）采取技术和组织措施，对个人信息实施适当的数据安全标准，维护其机密性并保证其完整性，同时考虑到处理的性质和目的以及对信息安全可能带来的风险。
（2）在确定处理方式或处理过程中采取适当的措施，以遵守法律的规定，包括假名化、匿名化处理措施等。
（3）实施适当的技术和组织措施，以确保个人信息的处理仅限于其目的。

（4）需要保持一份数据处理记录，必须应要求提供给办公室，包括：控制者和DPO的详细信息、对处理的个人数据类别的描述、与被授权访问个人信息的人员有关的信息、处理的时间段和限制、删除或纠正信息的方式、处理的目的、任何与信息的跨境转移或处理有关的信息以及与用于保护个人信息安全的技术和组织措施有关的信息。
（5）指定一个（多个）处理者，并充分保证执行符合法律及其执行条例规定的技术和组织措施。

5. 数据控制者义务：
（1）根据控制人的指示和双方的协议进行处理活动，确定处理的具体内容，包括其范围、目的、性质和个人信息的类型。
（2）结合成本、范围和目的，确定数据的处理方式和处理过程，在设计阶段实施适合保护个人信息的技术和组织措施（隐私设计）。
（3）根据指定的目的进行处理，如果在目的达到后仍继续处理，则向控制人寻求指导。
（4）一旦处理过程结束，需要删除个人信息，或将其返还给控制人。
（5）除非得到法律授权，不能披露个人信息或所处理的信息。
（6）维持一份代表控制者进行处理的数据处理记录，必要时向数据保护办公室提供。

6. 数据泄露通知：数据控制者如果意识到任何违反合规的情况下应该通知数据保护办公室。通知应该包括合规违约的性质、原因和违约的程度，指定的DPO的详细信息，违约的可能或预期风险，为减轻违规行为的后果所采取的措施，违规事件和所采取的缓解措施的文件；以及办公室的任何其他要求。此外，数据控制者应该在数据主体的隐私遭受侵犯的情况下通知数据主体。

7. DPO责任：必须指定隐私政策，建立内部审查机制、最小化处理数据原则、为数据处理活动建立保障、记录数据以符合监管机构所需要的策略、程序和操作等。

4.8.6 阿联酋数据合规建议

1. 所有个人数据的处理需要取得授权同意书。非经授权，企业或组织只有在出于保护公共利益、司法或安全程序、保护公共健康等一些有限目的的需要时才被允许处理数据。

2. 数据的跨组织共享，需要有合同的约束。企业如果外包了某些功能，它仍然最终负责确保其提供商也根据阿联酋法律处理数据，无论数据处理器位于世界的哪个国家。需要对共享个人数据的所有第三方的数据保护合规性进行彻底审计，合同应更新以反映数据隐私合规性要求和责任。

3. 制定数据保护影响评估、供应商评估问卷和隐私影响评估材料，以支持三方审计。同时为法务、合规、IT和数据安全等团队提供一套标准，用以评估新技术和合作伙伴。

4. IT团队要与数据团队一起建立强大的数据安全和访问控制机制，以确保数据不泄露。

5. 要周期新检查数据传输到的所有外部国家和区域。如果某个国家或区域被认为不能提供足够或同等水平的保护，将需要特殊的控制和文件来保证转让数据跨境照常进行。

6. 加强内部关于数据安全、合规以及隐私保护的培训和教育。应持续进行培训，以强化合规文化，并让员工了解法律和政策的最新变化。

4.8.7 常见问题

1. Q：中东其他国家的数据可以存在沙特吗？存在沙特之后还能不能再自由地出来？
A：中东各国，除了沙特，其他国家并没有数据本地存储的要求和对数据跨境的严苛要求。其他国家的数据不在PDPL的管辖范围内，所以在数据安全的前提下，可以将数据流转到其他国家。

2. Q：为什么我在控制台上看不到沙特资源？
A：沙特利雅得节点只有开通国际站账号才能看得到。

4.9 海外各国数据本地化与DPO要求小结

基于以上各国法律法规解数据本地化与数据保护官DPO要求如下：

序号	国家或区域	是否需要本地化	对DPO要求
1	欧盟	允许跨境传输的情况： 1.传输向欧盟充分性认定的第三国； 2.遵循标准合同范本签署相关传输协议； 3.约束性公司规则，集团公司内部订立的数据传输协议； 4.经过个人专门同意的数据传输	DPO需要向服务的企业和企业员工提供GDPR数据保护方面的信息和建议； 向服务的企业和企业员工提供GDPR数据保护方面的信息和建议； 向服务的企业和企业员工提供GDPR数据保护方面的信息和建议； 向服务的企业和企业员工提供GDPR数据保护方面的信息和建议； 客观独立的履行自己的职责； 有权限可直接向企业最高管理决策层汇报工作； 参与和管理数据保护影响评估等工作
2	澳洲	个人健康信息禁止跨境传输	政府机构需要设立DPO，为机构提供隐私保护建议； 处理机构内外部关于隐私问题地问询、投诉等工作。
3	新加坡	允许数据跨境	任命一位或多位确保组织合规地DPO； 确保与新加坡PDPA法律合规工作。
4	美国	允许数据跨境	根据HIPAA法规要求，制定并执行该实体地政策和流程。
5	俄罗斯	要求数据本地化存储	法律实体需要任命DPO负责个人信息处理地组织管控； 从事内部控制个人信息相关法律合规方面工作； 为操作者和员工提供与个人数据要求有关培训； 处理数据主体请求。
6	日本	允许数据跨境	
7	印度	要求在境内数据本地化存储，只有为满足特定服务所必须，敏感数据才能跨境，针对支付信息、物联网收集数据、社交数据等禁止出境	任命一名数据保护官员，以回应数据负责人的询问和建立申诉补救机制；
8	韩国	允许数据跨境	任命隐私保护官DPO管理数据处理工作； 制定数据保护计划、调查和完善数据处理流程、解决数据处理投诉、控制与预防个人数据误用； 为员工提供数据保护培训； 保护、控制和管理数据文件； 制定隐私保护政策，发现违规行为提供纠正建议，向组织负责人汇报。
9	巴西	允许数据跨境	对数据处理者而言，DPO是必须要有的。DPO被定位为数据控制者、数据主体和ANPD之间的沟通渠道。DPO需要在促进和传播组织内的数据保护文化方面发挥重要作用，如当收到数据主体和国家政府当局的请求并采取措施时、在收到数据主体的请求时、在指导员工和承包商有关个人数据保护的实践时。

阿里云出海能力中心&德勤中国
ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

出海企业数据合规体系化能力建设

5.1 数据合规体系建设基础
5.2 管控内外部数据使用
5.3 数据生产与采集
5.4 数据分类与分级处理
5.5 数据存储与传输
5.6 规范数据加工与开放
5.7 合规审计与风险度量
5.8 使用数据合规工具与技术

05 出海企业数据合规体系化能力建设

以近两年的形势来看，企业面临的最大挑战以数据合规为主。无论是欧盟的GDPR，还是中国的个人信息保护法、数据安全法，还是美国、德国等各自的隐私保护法的轮番实施，都对数据合规、开放、跨境等做出了明确规定。因此，数据合规成为合规的重中之重。

数据合规是企业确保数据在其全生命周期各环节满足法律法规和企业规则的过程。数据的全生命周期包含了数据从采集、传输、存储、使用、共享、销毁等环节。法律法规和企业规则通常涉及数据的合法性、公正性、透明性、安全性、准确性、数据最小化等要求。

过去企业做数据合规，面临的问题少且小，只需要点状的解决问题即可。但今天，数据合规面临的挑战非常大，从组织、流程、管理，到技术、产品、架构等，需要进行体系化地设计。这样不仅可以满足各国合规监管的需求，充分覆盖各合规场景下的问题，还能在这个越来越数字化的世界让合规能力成为企业的内功之一，充分利用好数据这个新时代的石油，取得市场竞争优势。

5.1 数据合规体系建设基础

以下是我们总结的数据合规体系化能力建设的基础建议。

5.1.1 强化全员合规意识

强化全员合规意识，需要从三个方面来开展：

· 一是对公司全员进行数据合规相关培训，告诉大家在日常工作中应该要重点关注那些合规方面的问题，强制参加考试并通过。培训内容需要结合企业的业务特点进行定制。一般来说，最起码要有专门针对企业的销售、产品技术、市场、财务税务、采购等较大的职能角色的责任和义务清单，要明确这些角色在自己的工作中应该遵守什么样的法条和规定。要将数据合规的高频、高危场景穷举出来，明确红线与相关处理流程，明白无误地周知所有人。

· 二是要尽量依靠工具和自动化方式在事前和事中及时提醒，避免无心之过，避免绕过内部风控流程。例如使用钉钉进行企业内外部沟通时，可以有防止截屏，以及向外部传输文件前提醒走脱敏流程；使用类似阿里云无影一类的云桌面产品进行办公，保障员工办公环境的数据安全和IT安全；IM类以及云笔记类软件严控使用等。

· 三是划清合规红线，明确违规后果，用制度来约束合规行为。

5.1.2 理解数据全生命周期

数据全生命周期合规管理（Data Lifecycle Management）是一种政策导向的数据管理方法，用于管理数据在整个生命周期内的流动，即某个集合的数据从产生到销毁的过程。

对企业来说，以生命周期的视角来管理自己的数据有如下四个方面的收益：

1. 流程改进：能够在数据的整个生命周期中保证和维护数据的质量，进而改进流程和提高数据流向的效率；

2. 控制成本：数据生命周期管理通过检测不同阶段的数据价值，可以通过一系列解决方案来降低成本，包括数据备份（冷热存储）和销毁等；

3. 数据易用性：借助数据生命周期管理的战略和工具，可以对不同的数据制定不同的政策和规程，确保一致的方式标记所有元数据，以便组织内部使用，共享和运营；

4. 合规和治理：数据生命周期管理是基于每个行业的自身政策所需，使组织和企业能够以更高的效率和安全性来处理数据，同时确保遵守个人数据和组织记录的数据隐私法律。

数据全生命周期合规治理整体框架如下：

5.1.3 定期进行风险度量

风险度量基于审计数据及合规制度落实情况，可以及时数字化地反馈合规水位，用以度量合规的变化趋势，有利于呈现合规管理运营结果。

度量在合规规则结构化基础之上，抽离出来能够反映合规水位的指标体系，并且能够针对不同区域或者国家要求有所体现。所以度量水位需要基于不同的规则体现。

一般来说，有以下五种合规度量的方式：

1. 合规问题发现的平均时间：通过“问题发现时间”总和除以事件总数来计算。可以通过被动告知（例如在被用户投诉其数据被泄露）或数据取证（例如监控到数据违规跨境）等方式来确认问题发现时间。通过这一指标可以验证企业内部是否有公开透明的合规问题透传机制，以及是否具备水平之上的数据监控能力。

2. 合规问题平均解决时长：用来衡量合规问题发现后的解决速度。在此要注意个性问题个性分析，不要把太多问题混为一谈。因为这个指标的用意是用来发现是流程问题、资源问题或者是技术问题。如果混为一谈是无法明确具体问题在哪里的。

3. 合规问题平均解决成本：可以通过将总合规预算除以计划管理的合规问题数量来计算此指标。它可以帮助企业高层了解有效的合规治理消耗了多少资金，也可以帮助企业了解为什么有些合规问题的解决成本要高于其他一些问题。如此一来就可以帮助决策者将钱花在更明智的地方。

4. 预测风险与实际风险之间的差值：需要在财务上和操作层面上来衡量这一差值。举例来说，可以在财务上，衡量预计的合规花费与实际的合规花费之间的差值；在操作上，衡量预测的隐私数据被窃取数量与实际的被窃取数量之间的差值。这个差值可以提现企业自身风险评估能力的强弱，进而能够比较实事求是地制定企业的合规治理计划与方案。

5. 风险缓冲时间：从发现风险到实施任何必要的整改措施以减轻该风险之间的时间。这个指标显示了实施合规变更的能力。该时间越长，企业就越有操作空间来从容应对风险，可以低成本、高质量地治理好合规问题。但如果该事件比较短，那么就要想办法避免这类合规问题的出现。

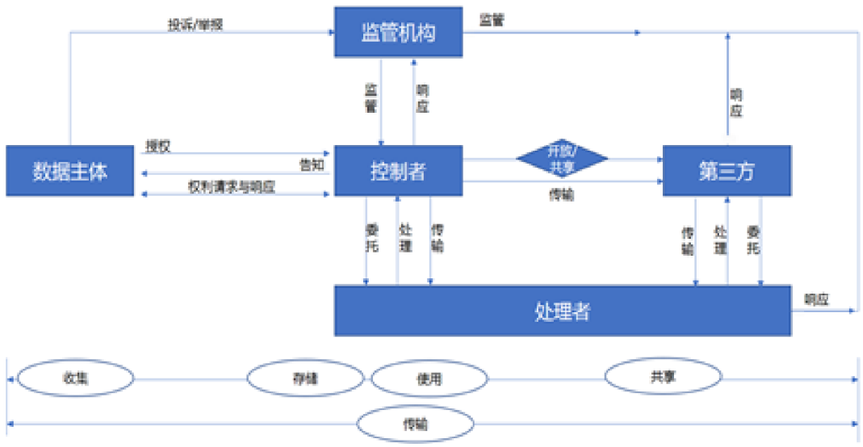
以上度量方式并非适用于所有的企业，在企业具体的合规能力建设过程中，可以有合理的指标体系和度量手段。

5.2 管控内外部数据使用

首先要明确都是哪些角色在使用数据。然后所谓管控内外部数据使用即按照角色去进行相应数据使用授权。

5.2.1 明确数据使用角色

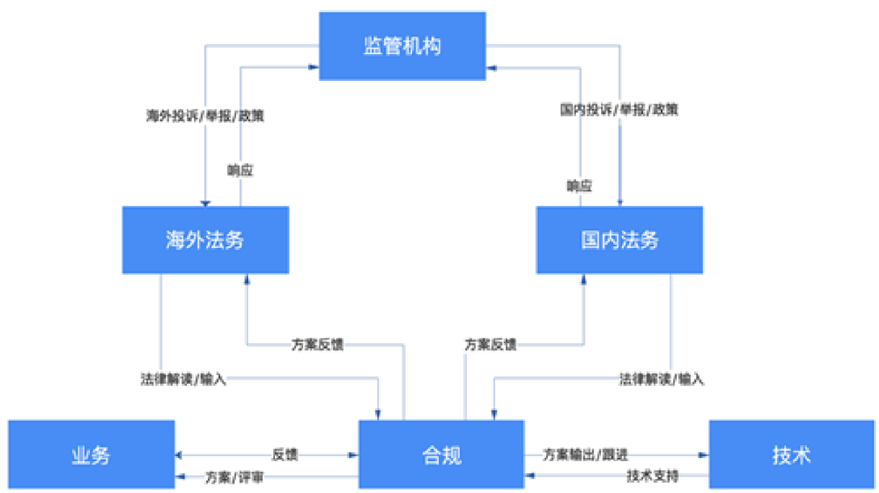
外部角色：按照数据生命周期角度，国际数据合规立法相关要求通常涉及如下角色，角色之间的权利/责任关系如下图：



其中：

- **数据主体：**个人数据所标识或者关联的自然人，简单来说就是平台的用户。
- **控制者：**单独或与其他主体一起决定数据处理目的和方法的自然人、法人。
- **处理者：**代表控制者处理数据的自然人、法人。
- **监管机构：**业务属地所在的国家或区域为数据安全或隐私数据保护而设立的独立性公共机构。
- **第三方：**指数据主体、控制者、处理者以及根据控制者或处理者的直接授权处理个人数据的主体之外的自然人、法人、公共机构、行政机关或其他实体。

内部角色：数据合规通常涉及组织内部的法务、合规、技术、业务等角色。法务负责对法律法规的解读和外部案例解读输入；合规协同各方制定企业合规方案并持续跟进方案的落地；技术团队提供技术支持并负责技术的执行；业务团队遵循合规方案并反馈业务诉求。



- **监管机构：**合规相关法律法规的制定以及舆情和问询函的下发实体（与外部角色中的监管机构是同一个角色）。
- **海外法务：**集团内部支持海外业务实体的法务，具有专业的海外法律专业知识，给出相关国家或者区域法律法规的解读和后期咨询。
- **国内法务：**集团内部支持国内业务的法务，具备国内法律专业知识和经验，用于给出国内法律法规的解读和相关案例的分析解答。
- **合规：**集团内部负责协同各方角色跟进推动合规方案的执行，提升集团的合规水位。
- **技术：**基于法务和合规产出的合规诉求，产出和落地对应的合规方案。
- **业务：**集团内面向客户的业务场景，业务场景需要满足合规制定的规则规范。

管理角色，要按照最小够用原则授权，并在运行时做数据权限管控，不得访问和管理超出授权范围的数据。典型的如按照成本经营单元、业务管理团队、项目组等进行授权。个人操作功能，按照实际身份，只能访问自身的敏感信息及公开的信息。

5.2.2 设计数据使用授权

数据访问控制是数据安全的核心要素，用于管理和限制用户或者系统对特定数据资源的访问权限，它是确报数据安全性、隐私保护、合规性和业务连续性的关键步骤。数据访问控制通过做好权限管理、过程追踪与记录以及事后审计，从而降低数据风险，提高数据管理的整体质量。根据GDPR 第 25 条的规定，控制者“应实施适当的技术和组织措施以确保在默认情形下，仅处理为实现特定目的而必需的个人数据。”以下阿里云访问控制体系仅允许得到授权的管理员、用户和应用程序访问阿里云的资源和客户数据，从而能够帮助客户符合此要求。如下是数据访问控制所涉及的产品，场景与方案映射示意图：

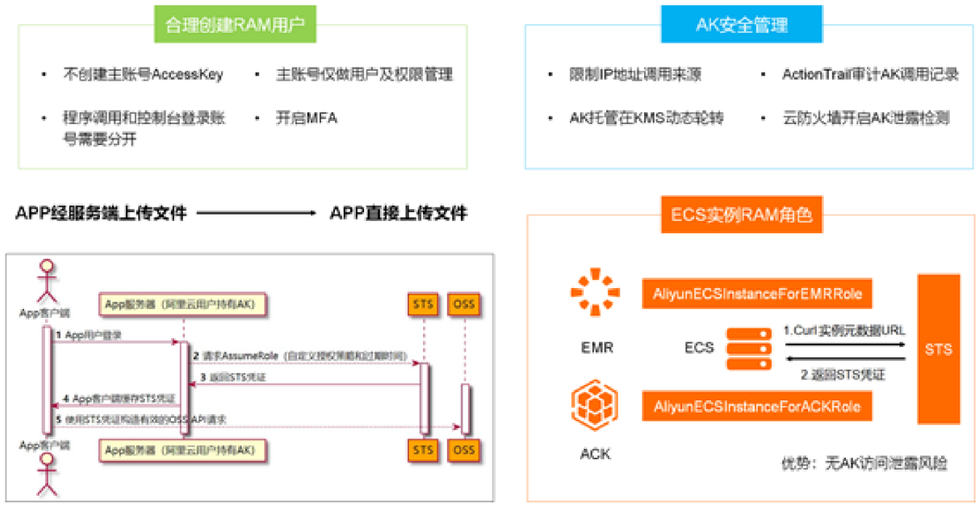
按照数据权限授权的角色，运行时需要校验数据权限。

5.2.3 业务数据访问控制

数据访问控制是数据安全的核心要素，用于管理和限制用户或者系统对特定数据资源的访问。

1. 云平台秘钥AK/SK安全管控

关于数据访问控制的一个常见场景是AK/SK的使用治理，防止AK/SK使用不当引起的数据泄露。GDPR 第 25 条规定，控制者“应实施适当的技术和组织措施以确保在默认情形下，仅处理为实现特定目的而必需的个人数据。以下是场景的实现图：



2. 隐私数据访问控制

隐私数据应该集中在统一的隐私数据库，并提供统一服务。然后需要对原有使用隐私数据的场景进行重新梳理。任何需要继续使用隐私字段的服务、程序、角色等都需要重新申请。

申请需要按字段进行，并需有充足理由使用该字段。因此需要有数据使用的申请平台控制读写权限的申请和审批流程，同时还需要将这些权限逻辑融入到所有读写服务中，提供高性能的鉴权能力。综上，数据服务管控由三部分组成：数据权限的维度设计、数据权限申请与审批、数据权限鉴权。

为了满足最小化使用原则，所有隐私数据的使用应当通过合理审批流程，获得授权后读写隐私数据。可以将管控的数据分为两类，一类是通用隐私数据，称为公域；一类是某个业务独有的隐私数据，称为私域。对于公域的通用隐私数据，比如一个会员的手机号码，按需申请读写的授权码即可。对于私域隐私数据，其归属和使用还需经过此数据写入方授权。该方案具有较好的隔离性， 可由业务自定义私域字段, 不同业务的私域字段可重名；同时具有较细的管控粒度, 区分写入的业务场景, 当申请某字段读权限时, 需要先选定是哪个业务场景, 然后筛选业务场景下写入的私域数据

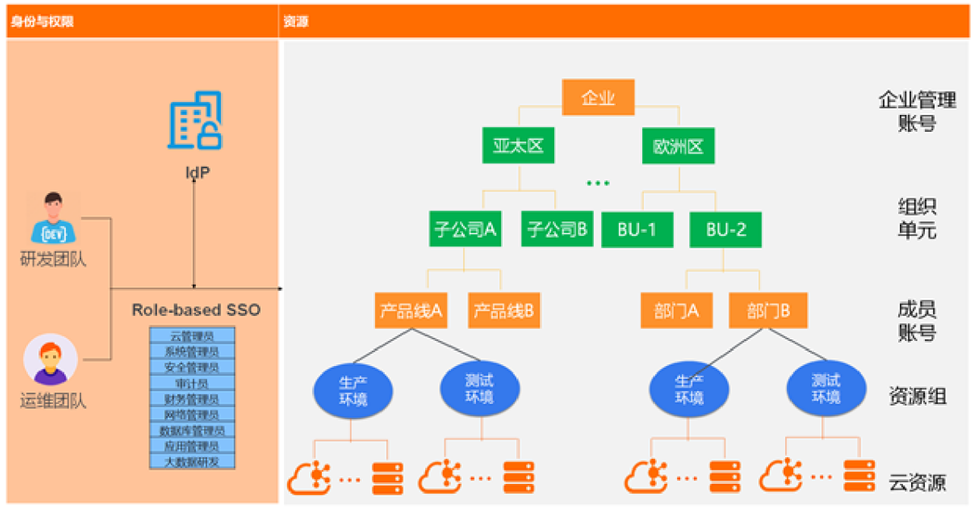
为了更好的管理合理使用场景，建议设计企业内部的合规管理平台，将权限申请与审批流程线上化。申请过程中，业务方需要提供足够的信息让法务合规的同学了解业务场景，并解答补充性问题。申请按字段进行。将全域通用数据定义为公域数据，将业务线或业务场景自身维护的隐私数据定义为私域数据。公域数据申请字段权限后即可使用，也是用户默认的隐私数据值。私域数据因存在场景区分，需要使用方和写入方达成一致后方可使用，故申请时还需要对方的业务授权码。权限申请提交后，合规官将详细审查调用合理性，并与业务方和技术方深入访谈，确保申请内容真实有效、描述准确，且相关人员对数据的使用有清楚的规划。

在完成数据权限申请和审批后，使用获得的授权码，通过数据服务中心提供的接口即可读写隐私数据。根据公私域特点，权限校验方式有所区别。在公域数据中，读写接口只需根据授权码和字段名进行判断，对于未授权的字段不予返回。对于私域数据，双方的授权码都需要填写，权限平台需要校验双方授权码和字段名，以决定是否有权限。特别的，如果是数据写入方读写自己的数据，双方授权码使用同一个即可。

3. 基于阿里云的账号体系进行权限治理

从权限管理的角度来说，不同的数据、业务最好匹配不同的账号，充分使用阿里云的多账号管理体系来构建数据边界。

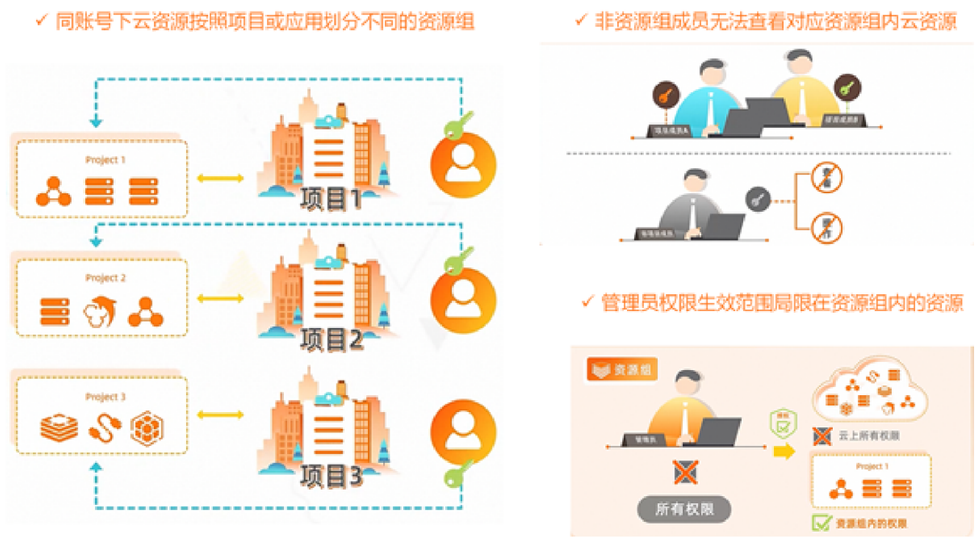
首先，可以利用服务目录来进行账号体系与公司组织的映射，以吻合实际业务中的数据边界。方案图如下：



阿里云的服务目录可以统一创建各个账号的control policy，高效地统一约束账号的统一行为，如不能创建公网IP、云上磁盘必须弃用加密等。

更多细节可参考链接：https://help.aliyun.com/document_detail/2340495.html

但毕竟很多时候会有在同一个阿里云账号中进行资源的精细化权限管控，此时可以利用资源组进行资源的权限划分：



然后在不同的资源中生效不同的RAM（resource access management）账号，并通过开启多重身份验证，来进一步保障安全性。

· **资源管理服务：**阿里云资源管理服务包含一系列支持企业IT治理的资源管理产品集合。其中主要产品为资源组和资源目录。资源管理服务支持您按照业务需要搭建适合的资源组织关系，使用资源目录、资源夹、账号、资源组分层次组织与管理您的全部资源。详情可参考官网链接。

· **服务与资源访问控制（RAM）：** 访问控制 RAM 使您能够安全地集中管理对阿里云服务和资源的访问。您可以使用 RAM 创建并管理子用户和用户组，并通过权限管控他们对云资源的访问。RAM可以以更精细的粒度（eg. 资源对象级、API操作级）授予对云端资源的访问权限，帮助您的公司实施最小授权原则；可以通过请求STS临时安全凭证 （可自定义时效和访问权限），使您的移动版和基于浏览器的应用程序安全地访问阿里云资源；可以通过配置计算型实例角色（如ECS实例角色），使您的应用程序安全地访问阿里云资源，避免 AccessKey 泄露带来的安全风险；同时可以与企业目录做集成，支持两种身份联合能力，通过设置单点登录(SSO)，使企业本地身份系统中的用户直接登录到对应的RAM用户身份或RAM角色身份。详情可参考官网链接。

· **多重身份验证：** Multi-Factor Authentication (MFA) 是一种简单有效的最佳安全实践方法，它能够在用户名和密码之外再额外增加一层安全保护。启用 MFA 后，用户登录阿里云网站时，系统将要求输入用户名和密码（第一安全要素），然后要求输入来自其 MFA 设备的动态验证码（第二安全要素），双因素的安全认证将为您的账户提供更高的安全保护MFA 设备可以基于硬件也可以基于软件，目前阿里云官网支持基于软件的虚拟 MFA。详情可参考官网链接。

关于详情，可参考：https://help.aliyun.com/document_detail/110036.html

5.2.4 通过云产品实现数据权限管理

对一个云上组织来说，核心数据往往放在数据库、大数据等产品中。阿里云的这些产品有自己的账号与数据权限管理体系。以RDS产品为例，可以通过RDS控制台或者API来创建普通数据库账号，并设置数据库级别的只读、读写、DDL、DML权限。如果需要更细粒度的权限控制，例如表、视图、字段级别的权限，也可以通过控制台或者API先创建高权限数据库账号，然后登录数据库创建普通数据库账号。高权限数据库账号可以为普通数据库账号设置更细粒度的权限。

这套数据管理体系，和上面通过账号进行数据边界治理的体系不同，属于更细粒度的授权。

以下是部分常用产品的账号权限管理指导信息：

· **RDS：** https://help.aliyun.com/zh/rds/apsaradb-rds-for-mysql/accounts-and-permissions-1/

· **PolarDB：** https://help.aliyun.com/zh/polardb/polardb-for-mysql/user-guide/database-accounts/

· **MaxCompute：** https://help.aliyun.com/zh/maxcompute/user-guide/permissions

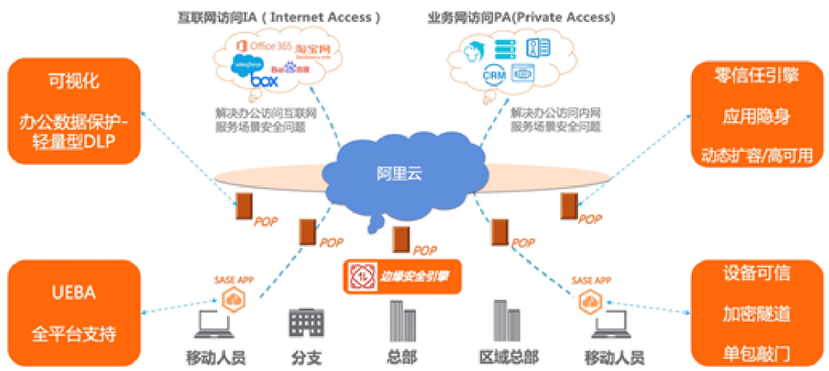
更多产品的访问控制、权限管理，可以根据您使用的具体产品到阿里云官网找到相关说明。

5.2.5 办公数据访问与保护

办公场景的数据合规是合规监管的重点之一。办公场景有较强的人为因素，增加了合规监管的难度。

1. 使用SASE实现远程访问控制

结合阿里巴巴集团多年的办公安全与合规管理经验，阿里云提供了基于零信任机制的SASE（Secure Access Service Edge）服务。



它可以提供三类场景的数据访问控制与管理能力：外发文件检测、外接设备管理、水印管理。

企业需要检测员工在日常办公中，通过多种渠道（例如即时通讯、邮件通道等）传输内部文件。该企业接入了SASE办公数据保护功能，通过检测员工传输的所有文件，帮助企业识别敏感文件及用户行为，避免业务遭受重大损失。SASE敏感文件检测功能通过自定义的关键字作为敏感文件的特征进行敏感内容的自动化识别，通过特征、数据类型、敏感定级组成敏感数据模板，再结合处置动作等条件形成检测策略帮您识别企业员工外发的文件是否为敏感文件。

通过配置外接设备的策略，管控企业员工的外接设备的数据访问权限，帮助企业识别是否存在敏感文件外发的行为。企业需要杜绝企业员工在日常办公中，通过外接设备传输企业内部文件，造成业务重大损失。接入SASE办公数据保护功能，通过配置策略检测外接设备的数据访问，可以识别是否存在敏感文件外发的行为，避免业务遭受重大损失。

企业也可以开启员工屏幕水印和打印水印能力，避免业务遭受重大损失，保障企业的办公数据安全。

2. 使用无影实现代码开发与核心数据的访问控制

企业经常会碰到使用外包、跨国协同开发、远程数据访问等面临较大合规风险敞口的场景。在这些场景中，不仅会涉及企业自己的机密运营数据，也会设计企业承载的个人数据。这些数据的跨主体访问，跨境访问，跨域访问一直是合规治理的主要目标。可以使用阿里云的无影，来一定程度上降低上述风险。如通过制作已安装软件的镜像来批量创建云桌面，保持环境的一致性，以方便统一合规基线。通过无影和管控策略，实现云桌面的只进不出，内网访问以减少后端服务的暴露面等等。

实习生外包开发

核心数据安全访问

关于无影的更详细信息请参考官网：https://help.aliyun.com/document_detail/214461.html

5.3 数据生产与采集

数据的生产与采集是由人工、应用程序、传感器等产生以及从不同的源头进行采集和获取。这里主要涉及数据采集时对敏感数据、隐私数据的自动识别。数据采集可能发生在企业系统平台对外的接口界面上，也可能发生在企业内部不同模块之间，从企业内部采集的数据一般我们也称之为数据的生产，比如从企业内部数据库、日志等存储介质中获取一些数据来实现某个需求。以下是数据采集与生产所涉及的产品，场景与方案映射示意图：

5.3.1 数据采集与生产合规

数据的采集途径主要有三个：客户端、网络爬虫、采购的商业数据。

· 对于从客户端采集的数据，应当遵循最小必要原则，并获得用户授权同意。涉及采集敏感信息时，必须要有合理业务场景，且需单独明示收集使用规则并获得用户授权同意。

· 对于网络爬虫获取的数据，须经法务评估以确保符合网络及数据安全、著作权、不正当竞争等法律要求，遵守相关自律公约，禁止通过攻防对抗方式爬取数据。

· 对于采购而来的商业数据，业务方责任人须确保数据采集来源、渠道的合法性，采集目的及流程的正当性，并通过采购合同协议等明确采集数据的目的和用途，并保留相关记录，确保符合相关法律法规要求。

5.3.2 场景举例

核心的支撑产品是阿里云的数据安全中心、App隐私保护等，支撑了以下合规场景：

场景1：App隐私合规检测

阿里云的DataWorks数据安全合规服务可对App进行隐私安全合规分析，支持敏感权限风险识别、个人信息采集行为检测、三方SDK风险检测、隐私政策合规检测等多项检测，助力企业和开发者全面、准确、高效地规避合规风险。详细功能信息可以参考官网链接。

场景2：Cookie合规检测：

根据各国法律，扫描各网站cookie对数据的采集是否符合当地的数据采集要求。例如欧盟《GDPR》要求网站cookie默认不存储,需要用户手动同意；但美国等国家的要求则是默认存储,需要用户手动拒绝。在Cookie合规检测领域阿里云并没有成熟产品，在阿里云市场有合作伙伴的相关产品，例如由浙江爱橙技术发展有限公司打造的八鲸合规产品，面向国内出海商家，专为云上用户和企业打造的海外合规解决方案服务提供围绕完整数据生命周期，同时满足面向消费者、商家、平台、监管机构多方的合规解决方案/最佳实践。经过速卖通（Aliexpress）、Lazada、Daraz、天猫海外等业务验证，具有扎实的技术架构基础，以及卓越的产品设计表达能力，助力中国企业在海外市场能够安全高效的实现合规方案落地。

具体可以参考阿里云市场链接：https://market.aliyun.com/products/205811101/cmfw00061879.html

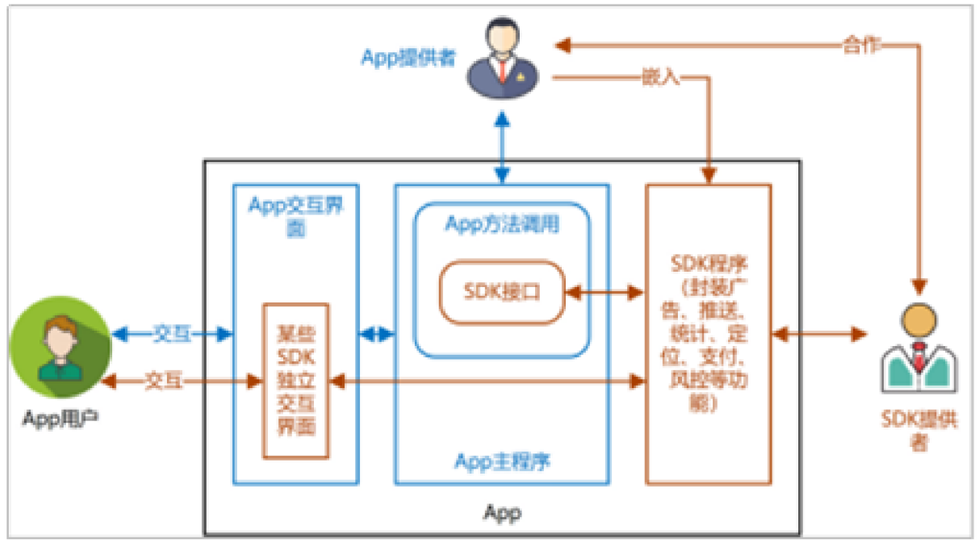
场景3：三方SDK检测

SDK主要类型有以下几类：框架类、广告类、推送类、统计类、地图类、第三方登陆类、社交类、支付类、客服类、测试类、安全风控类、Crash监控类、人脸识别类、语音识别类、短信验证类、基础功能类等。各类App平均使用第三方SDK的数量在10个以上。SDK本身不具备运行能力，必须等待宿主App调用才能被执行，完成特定功能。第三方SDK无疑给App开发者带来了极大便利，但与此同时SDK的安全与合规问题也逐渐漏出水面，SDK收集个人信息和安全问题也已得到了各方的关注。主要来说，三方SDK存在以下三类合规风险：

· 第三方SDK隐瞒收集个人信息，有些第三方SDK能够收集个人信息标识、行动轨迹、个人偏好、网络设备信息等，并上传至远程服务器，甚至是境外服务器；

· SDK借助合法App执行恶意操作，例如恶意开发者能够利用后门对用户手机进行远程静默安装应用、静默添加联系人、获取用户隐私信息等；

· 绝大部分第三方SDK缺乏安全审核环节，造成代码存有未知安全漏洞。目前，已经发现的SDK安全漏洞包括HTTP误用，SSL/TLS不正确配置、敏感权限滥用、通过日志造成信息泄露等；



解决上述问题，需要具备SDK合规检测的能力。可以参考阿里云市场上合作伙伴提供的产品，详情可以参考官网链接。

5.4 数据分类与分级处理

无论是欧盟的GDPR还是国内的《数据安全法》都要求数据分类分级管理。一般把数据分为4类：**重要数据、个人信息、公共数据、业务或其它数据**。重要数据指那些一旦泄露或非法利用，可能影响国家安全、经济运行、社会稳定、公共健康等的数据。这是从整个社会的角度上划分的，定义数据分级和分类要结合不同的行业和业务特点来进行。

除了某些特定行业（如医疗、金融）各合规条款会有相对明确的分级分类标准，其他行业的数据分级分类主要要靠企业自己划定标准来完成。

5.4.1 数据分类

数据分类通常有三种模式：

- **基于内容的分类：**取决于数据内容是否包含敏感数据；
- **基于来源的分类：**比如由人创建的数据，由程序产生的数据，位置数据等；
- **基于用户的分类：**即用户手动分类。

需要说明的是，以上三种模式并不是唯一的分类方法。如阿里云在实践过程中经常参考的一套数据分类标准如下：

1. 第一类：用户数据。用户数据即公民个人信息类，这类数据在全球已经有了比较清晰的规范要求和说明，各国比较类似。个人识别信息是“由代理机构维护的有关个人的任何信息，包括（1）任何可用于区分或追踪个人身份的信息，例如姓名，社会保险号，出生日期和地点，母亲的姓氏或生物特征记录； （2）与个人连接或可连接的任何其他信息，例如医学，教育，财务和就业信息。 PII的示例包括但不限于：名称，例如全名，娘家姓，母亲的娘家姓或别名；个人识别号，例如社会安全号（SSN），护照号，驾照号，纳税人识别号或金融帐户或信用卡号。

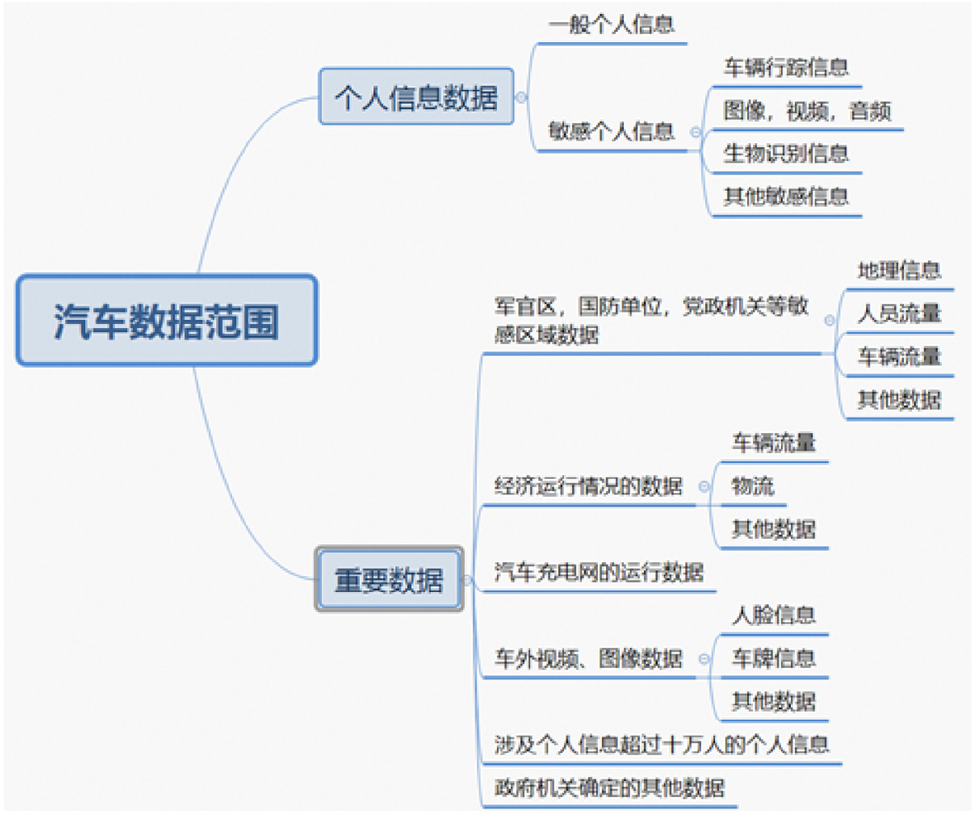
2. 第二类：业务数据。业务相关的数据，与组织的业务形态息息相关，比如：淘宝京东更多的是订单物流、商品详情数据等；爱奇艺优酷更多的是视频类数据等；除此之外，还有一些通用类数据，比如市场数据、业务分析数据等。

3. 第三类：公司数据。公司数据主要包含人事数据、财务数据、法务数据、采购数据、日志数据、代码数据、制度数据等二级数据分类，二级数据可以分为两类，一类为通用数据类，如日志、制度等；一类为定制数据类，如人事、财务等。

在实施和扩展数据分类策略时，请牢记这些规则：

- 确定哪些合规或隐私法律适用于你的公司，并根据该信息制定分类计划。
- 从有限的范围和定义明确的模式（如 PCI-DSS）开始进行分类。
- 要快速处理大量数据，尽量使用自动化工具。
- 必要时创建自定义分类规则，但不要重新发明轮子。
- 根据需要，更改分类规则/级别。
- 一定要检查分类结果的准确性，并迭代。
- 将数据分类应用于具体的业务场景，如数据跨境、BI分析、营销推广等。
- 数据分类是综合数据安全策略的重要组成部分。一旦确定了哪些数据是敏感数据，您就需要确定谁有权访问它以及它在什么时候发生了什么。要对数据的变化有掌控。

以车联网场景为例，如下是常见的一种数据分类：



5.4.2 数据分级

数据分级时，我们常常需要考虑以下问题：
数据泄漏或破坏相关的合规风险是什么？组织经济风险是什么？软件成本和硬件成本是什么？组织品牌及舆论影响成本是什么？

依照上述问题，对数据进行分级对待和处理。
将数据和系统分为三个风险级别是一种常见的做法：

- **低威胁：**如果数据可供公众访问且不易丢失（例如，恢复更简单），则此数据收集和包含它的系统可能比其他系统危险性低。
- **中等风险：**数据不公开，仅供公司或其合作伙伴内部使用。也不太可能因为操作过于关键或过于敏感而被视为“高风险”。中等风险包括专有操作程序数据、货物成本数据和部分公司文件。
- **高风险：**包括任何敏感或对安全至关重要的数据。极难恢复的数据（如果丢失），个人隐私数据，公司财务明细数据等都属于高风险数据。

在某些行业，有成型的数据分级标准，如2020年版的《金融数据安全数据安全分级指南》，将金融行业涉及的客户、账户、合约、交易、渠道、营销、影像、监管报送等信息分为四个层次五个敏感性等级。但由于企业业务形态的复杂性，企业需要基于成熟的分级标准，结合自己的具体业务建立自己的分级评估体系。

同样以车联网数据为例，数据分级的参考矩阵和处理要求如下：

数据类型	是否包含个人信息	是否包含敏感个人信息	是否包含重要数据	数据存储要求	数据跨境要求
车外数据	是	是	是	车外保存不超过14天	否
座舱数据	n/a	是	n/a	n/a	否
运行数据	否	否	是	n/a	n/a
位置轨迹数据	是	是	是	车外保存不超过14天	否

5.4.3 数据分类分级建议

数据分类过程根据项目目标略有不同。大多数数据分类项目都需要自动化来处理企业每天生成的海量数据。总的来说，有一些最佳实践可以使数据分类项目取得成功：

1. 定义数据分类过程的目标
（1）关注的数据有哪些？为什么是这些数据？
（2）初步分类阶段包括哪些系统？
（3）在合规方面，必须遵守哪些规则？
（4）还有其他的商业目标吗？（例如风险管理、存储优化或BI应用）。

2. 数据类型分类
（1）确定企业拥有的数据类型（例如，客户名单、财务记录、源代码、产品计划等）。
（2）区分私有数据和公共数据。
（3）确定是否受到 GDPR、CCPA 或其他监管标准。

3. 确定分类级别
（1）需要多少分类级别？
（2）记录每个级别，并提供示例。
（3）教用户如何对数据进行分类（如果计划进行手动分类）。

4. 定义自动分类的过程
（1）确定应首先扫描哪些数据以及如何确定优先级。
（2）动态数据处理优于静态数据，数据的开放比数据保护优先级更高。
（3）确定多久使用一次自动数据分类以及需要投入多少成本（时间、算力）。

5. 定义类别和分类标准
（1）为高级类别（例如，PII、PHI）定义并提供示例。
（2）定义或启用适当的分类模式和标签。
（3）创建用于审查和验证用户自定义的结果和自动分类结果的程序。

6. 定义分类数据的结果和使用场景
（1）应定义风险缓冲和自动化流程的步骤：例如，如果180天未使用的数据，则可以将其移动或存档；全局访问权限应该从包含敏感数据的文件空间中移除。
（2）定义一种使用分析来改进分类结果的方法。
（3）确定分析的结果是否符合预期。

7. 观察和维护
（1）创建用于对新数据或更新数据进行分类的例子和流程。
（2）根据优于业务变化或新法规应用需要的数据审查流程，并更新数据分类流程。

对于大部分云上的企业来说，需要进行管理的数据大都存放在数据库或大数据平台中。以下两节将从数据库和大数据系统的视角简要介绍其中的数据分级分类实践。

5.4.4 敏感数据监督

在数据分类分级的基础上，对敏感数据进行全方位的审计，全面掌握敏感数据的来源、存储分布、数据数量、数据去向，从而在其中发现安全问题或安全薄弱环节并加以治理，以确保敏感数据的安全合规。这里面主要包含以下部分能力的建设：

1. 权限管控
基于前文提到的内容，管控内外部数据使用的同时，针对重点关注敏感数据访问。

2. 风险告警
对于账号、权限、程序的动态跟踪与维护是进行风险告警的基础之一。需要周期性扫描人员组织、权限基线、应用架构等方面的变化，变化前后是否会对敏感数据的使用有影响，这些变化是否遵循了合规性的保证。对于数据的授权确权等要有明确的记录以及统计分析，及时将异常情况以告警的形式呈现出来。
对于数据访问行为的跟踪、记录与监督是进行风险告警的基础之二。可以基于网络流量分析、高性能数据库入库技术、大数据分析技术以及可视化展现技术等对数据访问进行检查。对于异常行为可以通过两种方式来识别，一种是人工的方式，一种是对日常行为模式进行动态的机器学习与建模，通过AI的方式来监督。

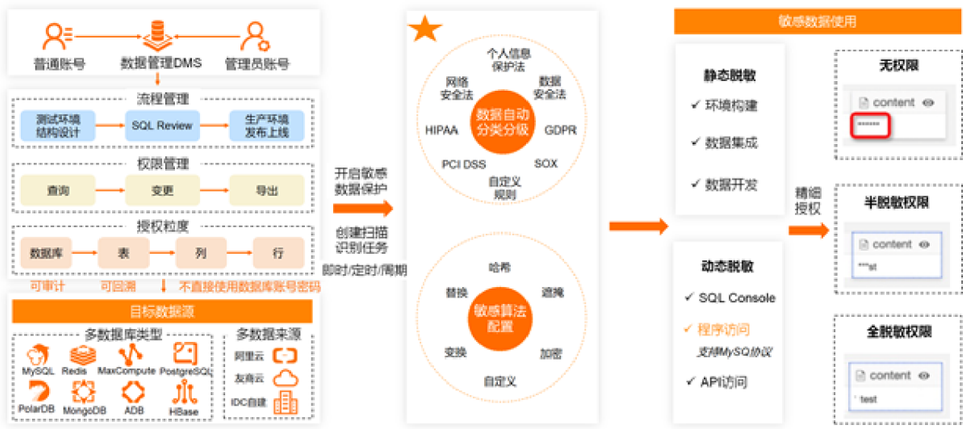
3. 追溯问责
敏感数据域合规相关各项处理活动必须可以进行过程追溯，还必须以各种可举证的形式证明所进行的数据处理活动符合相关法律法规的要求。同时，遵守处理个人数据的基本原则是法定义务而非最优选择，若违反数据处理基本原则的要求即会受到相应的处罚。

5.4.5 云产品实现数据分类分级

1. **使用阿里云DMS进行数据分级分类**
阿里云数据管理DMS（Data Management）是一款支撑数据全生命周期的一站式数据管理平台。DMS提供全域数据资产管理、数据治理、数据库设计开发、数据集成、数据开发和数据消费等功能，致力于帮助企业高效、安全地挖掘数据价值，助力企业数字化

转型。基于流程审批的全方位精细化安全管理DMS支持全域数据的实例、数据库、表、字段以及数据行级权限管理，可按需分配查询、导出、变更等不同操作权限。根据系统内置的行业和法案等识别规则对数据库元数据进行扫描，识别、脱敏和管理，实现敏感数据保护。

使用DMS进行数据分级分类的参考方案图如下：



DMS中有数据分类分级模板功能。它从模板维度为数据提供自动分类分级能力。给实例绑定模板后，系统会根据模板内的识别规则对实例中库表的字段进行分类分级扫描，判断是否有符合该规则的敏感字段并且给字段打上分类分级的标签，还可以保护（例如：敏感列权限访问控制、使用过程进行脱敏等）敏感等级高的字段，并将敏感字段直观地展示在识别结果中。模版功能可以大大简化数据分级分类的工作，提高数据管理效率。

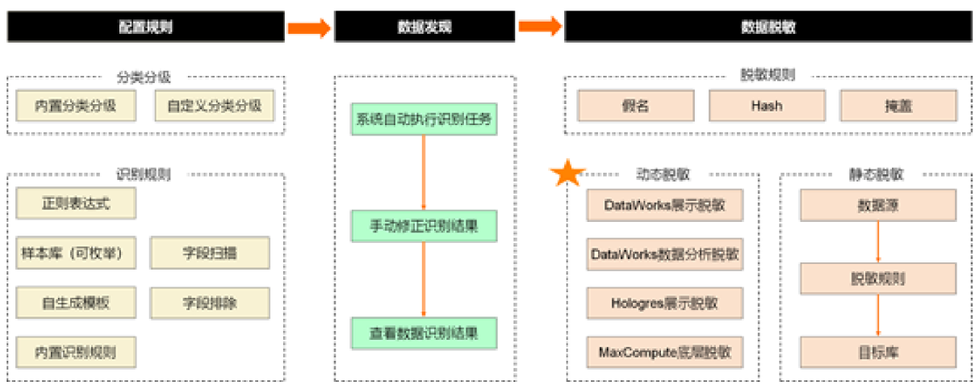
更多细节内容参考官网：https://help.aliyun.com/document_detail/159254.html

2. 使用阿里云Dataworks进行数据分级分类

阿里云DataWorks基于阿里云ODPS/EMR/CDP等大数据引擎，为数据仓库/数据湖/湖仓一体等解决方案提供统一的全链路大数据开发治理平台。作为阿里巴巴数据中台的建设者，DataWorks从2009年起不断沉淀阿里巴巴大数据建设方法论，同时与数万名政务/金融/零售/互联网/能源/制造等客户携手，助力产业数字化升级。

MaxCompute提供数据保护伞数据安全管理服务，支持数据发现、数据脱敏、数据水印、访问控制、风险识别、数据审计、数据溯源等功能，有效识别组织内的敏感数据，通过动态脱敏和静态脱敏对敏感数据进行保护。

使用Dataworks进行数据分级分类的参考方案图如下：



更多细节请参考：https://help.aliyun.com/document_detail/72799.html

3. 使用阿里云数据安全中心自动识别敏感数据

阿里云数据安全中心（DSC）提供对数据源中敏感数据的自动识别能力，且支持OCR技术，对图片中保存的敏感信息进行提取和识别；同时内置深度神经网络和机器学习等先进技术，通过样本扫描、特征萃取、特征对比和文件聚类等算法，可以识别结构化数据、非结构化文本、图片文件，并可以自定义识别规则，提供基于关键词、正则表达式、数据表列名的敏感数据识别能力，为企业进行重要数据资产管理提供定制化方案，便于企业实现数据资产统一化管理。DSC的详细功能信息可以参考：官网链接。

DSC接入数据库的方式大致罗列如下，更详细信息可以参考：DSC接入数据库方式step by step。

连接类型	说明	支持的数据资产类型
一键连接	指通过控制台按钮一键连接数据库的方式。 在连接过程中，数据安全中心会针对目标数据资产添加只读账号，数据安全中心通过该账号连接目标数据库，从而进行数据识别任务；由于该账号为只读权限，一键授权的数据库无法作为脱敏任务的目标数据库。	RDS、PolarDB、PolarDB-X 1.0（原DRDS）、OSS
一键连接	指通过手工输入数据库的账号、密码进行数据库连接的方式。 通过只读账号进行数据库连接后，该数据库可正常进行敏感数据识别、脱敏及审计任务，但无法作为脱敏任务的目标数据库；通过支持读写的账号进行数据库连接后，该数据库可作为脱敏任务的目标数据库来存储脱敏后的数据。	结构化数据： RDS、PolarDB、PolarDB-X 1.0（原DRDS）、Redis、MongoDB、OceanBase、自建数据库 大数据： TableStore、MaxCompute、ADB-MySQL、AnalyticDB for PostgreSQL（即ADB-PG）

5.5 数据存储与传输

数据存储是指将数据保存在计算机系统或其他电子设备中的过程。这包括将数据存储到硬盘、固态硬盘、内存、数据库、云存储等介质中。存储的数据可以是各种类型的信息，如文档、图片、音频、视频、应用程序等。数据存储的目的是为了在需要时能够随时访问、处理和使用这些数据。

以数据库为存储介质的数据，可以以数据模型作为选型依据，如选择关系型数据库（如MySQL、Oracle）或非关系型数据库（如MongoDB、Redis）；可以以数据量和负载作为选型依据，如根据数据量的大小和负载的性质，选择适合的数据库。

对于大规模数据或高负载的情况，可以选择分布式数据库。而一些数据库提供了缓存层、索引优化、数据分区等功能来提高性能，提供了加密、访问控制、审计等安全功能来提高安全性，也是选型的重要依据。

- 除了数据库产品，阿里云还提供了丰富全面的云存储来存储数据。如：对象存储OSS：海量、安全、低成本、高可靠的云存储服务；
- **文件存储NAS：**一个可共享访问，弹性扩展，高可靠，高性能的分布式文件系；
- **块存储：**基于多副本分布式技术，提供99.9999999%数据持久性；
- **表格存储：**主要满足海量结构化数据的存储需求；
- **日志服务：**提供实时数据的采集/清洗/分析/可视化服务。

企业可以根据自己的数据特性和服务要求来选择合适的阿里云存储产品。具体可以参考官网链接：阿里云存储产品系列。

5.5.1 数据存储合规

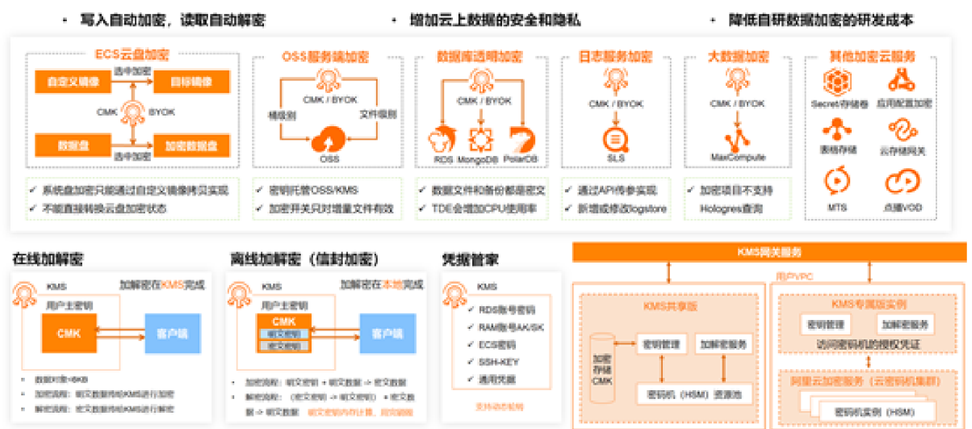
企业在数据存储环境应当遵循一定的合规原则，包括但不限于：

- 不应当存储未经过用户授权的个人数据；
- 应保证数据的机密性，敏感数据默认应进行加密或哈希存储；
- 应保证数据的可用性、完整性，按需建立必要的数据灾难备份、恢复和演练验证机制；
- 法律或相关安全标准要求的数据应设置有效的存储周期；
- 遵循特定国家特定场景的数据本地化存储要求；
- 敏感数据相关页面展示应进行脱敏处理和日志打点，并接入水印；
- 脱敏规则原则上应保持一致或不得低于基线脱敏要求，避免通过技术手段反推出真实的数据。

在数据存储环节，如何基于阿里云的数据库与存储产品落实合规的存储设计，可以参考以下场景：

- **场景1：通过KMS加密存储敏感数据**

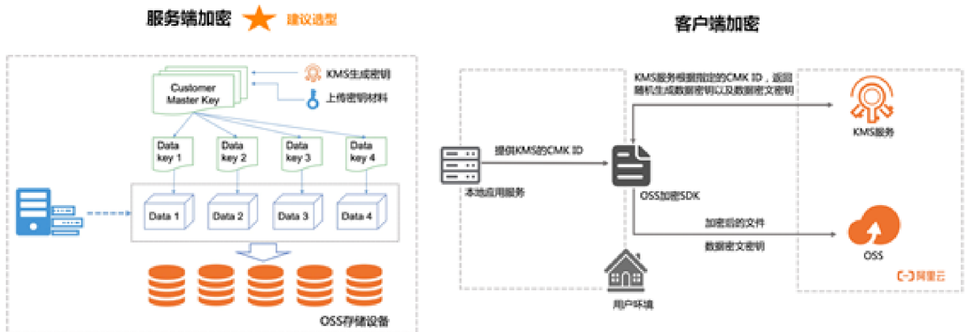
密钥管理服务KMS提供简单、可靠、安全、合规的数据加密保护能力，极大的降低密码基础设施和数据加解密产品上的采购、运维、研发开销，为凭据提供托管加密、定期轮转、安全分发、中心化管理的能力，降低传统IT设施配置静态凭据带来的安全风险。



- **场景2：OSS敏感数据保护与加密**

敏感数据主要包括个人隐私信息、密码、密钥、敏感图片等高价值数据，这些数据通常会以不同的格式存储在您的OSS Bucket中。企业拥有大量数据，但无法准确获知这些数据中是否包含敏感信息，以及敏感数据所在的位置。OSS的敏感数据保护能从海量数据中快速发现和定位敏感数据，精准区分敏感数据与非敏感数据。通过内置算法规则和敏感数据识别规则，对OSS存储的海量数据进行扫描、分类和分级。您可以根据扫描结果做进一步的安全防护，例如通过加密、设置访问权限等方式对数据进行安全审计或保护，从而满足数据安全、个人信息保护等相关法规的合规要求。这是OSS的一项产品附属功能，详情可参考官网链接：https://help.aliyun.com/zh/oss/user-guide/sddp

而OSS也可以通过服务器端加密或客户端加密的方式来为其中的数据提供加密保护，方案如下：



由于服务端加密可以实现写入自动加密，读取自动解密，所以较为推荐。客户端加密需要先加密再上传，先下载再解密，使用起来不是很方便。详细信息可以参考官网链接：https://help.aliyun.com/zh/oss/user-guide/data-encryption-6/

5.5.2 数据非跨境传输

数据传输就是按照一定的规程，通过一条或者多条数据链路，将数据从数据源传输到数据终端，它的主要作用就是实现点与点之间的信息传输与交换。

非跨境场景下，需要使用安全协议进行加密传输，其中敏感数据单独进行加密或混淆，并对两端的主体身份进行鉴别和认证，确保数据传输双方可信。跨网络安全域传输数据应当遵循网络安全相关规范，默认只允许低等级数据单向流入高等级网络安全域，并经过可信的中转程序或安全管控服务。原则上禁止高等级网络安全域向低等级写入数据。阿里云提供了一系列加密能力与证书服务，确保数据不会被窃取和泄露。数据的跨组织传输合规，会在“数据开放”章节展开。

- **传输层链路加密：**阿里云所有云产品的客户访问数据（包括读取和上传），都默认提供了SSL/TLS协议来保证数据传输链路的安全。
- **传输层应用加密：**阿里云通过加密服务（Cloud HSM）和密钥管理服务（KMS）对传输层应用数据进行加密。应用系统通过代码层的集成完成数据加密，加密后再传输数据，这样即使是开放的互联网网络，客户的数据也可以得到安全保证。
- **证书服务：**数字证书管理服务（Certificate Management Service）是由阿里云联合全球多家数字证书颁发机构，在阿里云平台上直接提供数字证书申请、管理、部署等的服务。数字证书管理服务同时支持SSL证书和私有证书，帮您以较低的成本将数据传输协议从HTTP转换成HTTPS，实现网站或移动应用的身份验证和数据加密传输。
- **智能网关：**阿里云的网关产品也提供传输链路的加密功能。VPN网关（VPN Gateway）服务，可通过传输链路加密通道将企业本地IDC和阿里云VPC安全可靠的连接起来。VPN网关可建立IPsec-VPN，将本地IDC网络和云上VPC连接起来；也可建立SSL-VPN，将本地客户端远程接入VPC。阿里云也提供智能接入网关（Smart Access Gateway，简称SAG）服务，企业客户可通过智能接入网关实现就近加密接入，并在传输过程中使用IKE和IPsec协议对传输数据进行加密，保证数据安全。
- **数据防泄漏：**主要由阿里云的数据安全中心（原版名称叫做敏感数据保护）来提供，通过收集和分析数据访问日志，基于各维度自动生成行为基线，目前总共内置27种异常行为检测，在发现某些访问行为和流转过程中出现潜在的疑似风险时，进行及时的告警，提供相关修复建议，协助客户分析异常产生的原因并进行处理，以便对云平台中保存的数据进行整体运行态势的评估。

5.5.3 数据跨境传输

数据跨境传输的场景下，跨境传输应当遵守传输地所在国家或地区的法律法规，若传输地所在国家或地区的法律法规禁止特定类型数据跨境传输的，不得对该类数据进行跨境传输。若传输地所在国家或地区的法律法规限制特定类型数据跨境传输的，应当在符合其法律法规要求的情况下进行特定类型数据跨境传输。跨境数据接收方运营主体或使用场景发生变化时，应立刻停止跨境传输，并重新进行评估。在跨境场景下，不仅需要上述一系列传输加密能力，还需要对跨境场景提供额外的能力。

· **数据传输服务：**DTS（Data Transmission Service）支持关系型数据库、NoSQL、大数据(OLAP)等数据源，集数据迁移、订阅及实时同步功能于一体，能够解决公共云、混合云场景下，远距离、秒级异步数据传输难题。其底层基础设施采用阿里双11异地多活架构，为数千下游应用提供实时数据流，已在线上稳定运行6年之久。DTS默认仅支持非跨境的同步任务。若您需要创建跨境（跨国家或地区）的同步任务，如从中国内地同步至非中国内地地域，您需要申请开通同步的权限。

· **全球网络互联：**云企业网（Cloud Enterprise Network，简称CEN）是阿里云提供的一款能够快速构建混合云和分布式业务系统的全球网络服务，为用户提供优质、高效、稳定的网络传输环境，帮助用户打造一张具有企业级规模和通信能力的云上网络。适用于集团企业、全球网络等场景。

· **敏感传输数据识别：**在数据被跨境传输前，使用阿里云数据安全中心的能力可以对数据进行扫描和检测，识别其中的个人数据、隐私数据和敏感数据，以便客户以根据最小必要原则进行筛选排除不必进行跨境传输的数据。具体可以参看阿里云官网链接。

5.6 规范数据加工与开放

5.6.1 数据加工合规

数据加工的目的是提取有用的信息、发现规律和趋势，以支持决策和业务需求。它通常涉及数据清洗，数据转换，数据集成，数据聚合，数据分析和可视化等步骤。在合规语境下，在数据加工环节，主要是指数据的分级分类，敏感数据发现与数据脱敏。此外，还包括权限的精细化控制。

在数据加工环节，还应该注意以下原则：

· 应在限制访问网络域进行，如需在其他网络环境中进行，应按照跨网络安全域要求执行数据流动传输；

· 数据应当在审批确定的范围内加工使用，不得未授权超范围使用或商业化；

· 加工数据如涉及非活跃数据应禁止加工输出；

· 数据或数据产品必须明确负责人，如涉及敏感数据必须有安全保护措施；

· 数据加工输出的分析成果或数据产品必须有权限控制，不允许超越原始数据授权范围使用，不得侵犯商家的商业秘密；

· 如涉及个人数据，应在上线前开展必要的DPIA/PIA数据风险评估，并按需提供必要的安全控制措施；

在数据加工环节，企业要关注加工行为的合规性，不能在不经过客户授权的情况下，做超过合理范围的行为。如何基于阿里云的数据库与存储产品落实合规的存储设计，可以参考以下场景，场景举例：

· **场景1：数据脱敏能力：**

阿里云提供数据在交换、处理过程中的静态脱敏和动态过敏能力，与几乎所有的合规法案相关。在阿里云的大数据、数据库等数据产品中都有数据脱敏能力的功能模块。静态脱敏适用的场景，将数据抽离生产环境并进行分发和共享的场景，例如生产环境向开发测试环境的数据脱敏导出；动态脱敏适用的场景，主要用于直接访问生产数据的数据脱敏使用场景，例如前端页面展示或在应用使用数据的过程中进行脱敏。

· **场景2：基于DMS的数据库管理**

数据管理服务DMS支持多法律法规覆盖，数据分类分级全面覆盖中华人民共和国网络安全法、GDPR、SOX、PCIDSS、HIPAA等法律法规；精细分类与脱敏，内置40多项分类识别规则，支持用户自定义；支持哈希、遮掩、替换、变换、加密等常用脱敏算法。

· **场景3：号码隐私保护**

号码隐私保护是一套专注保护客户通信隐私、信息安全防护服务的解决方案，在提供优质、稳定通信服务的同时，隐藏用户真实号码，进而有效保护企业通信、服务号码、客户资料等信息安全。适用于快递、外卖、网购、租赁等多种业务场景。同时可以通过录音来对其服务质量进行分析，提升产品安全性及平台价值。

· **场景4：日志服务数据脱敏**

在日志服务的采集、存储和加工环节，对敏感数据进行脱敏处理。使用敏感数据包括手机号、银行卡号、邮箱、IP地址、AK、身份证号网址、订单号、字符串等场景中，您需要为敏感数据进行脱敏操作。在日志服务数据加工服务中，常见的脱敏方法有正则表达式替换（关键函数regex_replace）、Base64转码（关键函数base64_encoding）、MD5编码（关键函数md5_encoding）、str_translate映射（关键函数str_translate）、GROK捕获（关键函数grok）等。以下是几种常见的方式：

更多详细信息可参考官网链接：https://help.aliyun.com/zh/sls/user-guide/mask-sensitive-data

5.6.2 数据开放

数据开放主要指组织内以及跨组织之间的数据访问与共享，充分发挥数据的流动性，放大数据的价值。数据开放的主要应用场景包括：

- **商务智能BI：**典型场景如使用阿里云的dataV，QuickBI进行数据展示与分析等；
- **分析与应用：**人工智能和学习，智能推荐，图像搜索，智能对话机器人等；
- **数据集市：**数据交换平台包括数据访问控制，数据交换，数据交易等；

如果在数据加工环节中，数据脱敏、数据过滤、数据打标签等前置能力已经做好，那么数据开放环节主要解决的问题就是可信计算和可信环境的问题。在可信的大语境下，数据的开放，也就是数据的交换才具备可行性。

5.6.3 构建可信计算

在很多情况下，我们是希望数据可用不可见的，可信计算同样需要可证、可度量。这里的数据是非集中式的，也有两种模式，一种是去中心化模式，数据提供方，也是计算参与方。另一种是介于集中式和去中心化模式之间的联合计算模式，在联合计算模式里，每方都会参与到模型计算，同时我们引入了中间层，也就是一个中心化模块的概念，这个模块可协调相应计算、模型训练，比较具有代表性的是联邦学习，包括拆分学习、差分隐私等，都属于联合计算学习框架。在这个框架里，通过差分隐私来加密各个模块与中心化模块之间的通信。以信息论为基础，我们可以度量任何一个信息交互所可能带来的个人隐私风险，称之为可度量模式，也就是个人隐私在联邦学习环境中计算，所带来的一系列风险是可度量的。

- **联合计算模式-阿里云隐私增强计算：**阿里云的隐私增强计算产品DataTrust是行业领先的基于可信执行环境（Trusted Execution Environment，TEE）、安全多方计算（Secure Multi-Party Computation，MPC）、联邦学习（Federated Learning，FL）、差分隐私（Differential Privacy，DP）等隐私增强计算（Privacy Enhancing Technique）技术打造的隐私增强计算平台，在保障数据隐私及安全前提下完成多方数据联合分析、联合训练、联合预测，实现数据价值的流通，助力企业业务增长。详细信息可参考官网链接。
- **去中心化模式-可信计算服务：**阿里云的可信计算服务 C3S（Blockchain Confidential Computing Service）为链上应用提供链上链下数据交叉核验，保证链上流转数据可信扩展，并提供通用的、隐私保护的数据分析能力，支持多方业务数据融合和治理，适用于金融风控、数字物流等场景。详情可以参考官网链接。

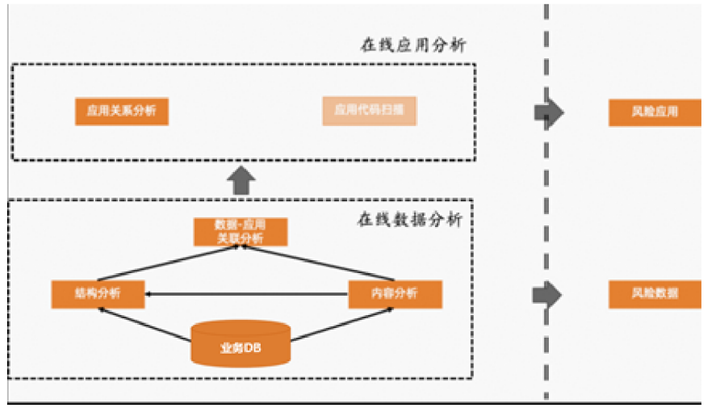
5.7 合规审计与风险度量

合规审计可以确定数据的生产、存储、使用、销毁等全流程的情况，一方面可以保证合规落地，另一方面也可以在前期评估合规改造的范围和成本。合规审计既可以在线实时进行，也可以离线事后进行，目前以离线方式为主，着重于事后审计。合规审计可以对当下的数据使用情况、目前的资源配置情况、历史的产品与数据操作行为等各类数据记录进行全局扫描，从而识别出合规分享，这是合规水位评估以及合规改进的重要手段。

无论哪种审计，都会包含两部分：静态内容审计，即包括内容，结构及代码等的审计；关联分析，即通过数据库日志、监控日志、调度日志、访问日志等分析，盘点合规数据的影响面。合规的关联分析需要企业根据自己的业务、组织情况设置好规则，结合具体场景来实现。

5.7.1 在线审计

数据库是所有在线业务数据的存储载体和数据的最初来源，因此，在线合规审计以数据库为基础，关联获取相关应用，最终覆盖所有日志、数据流及离线数据。



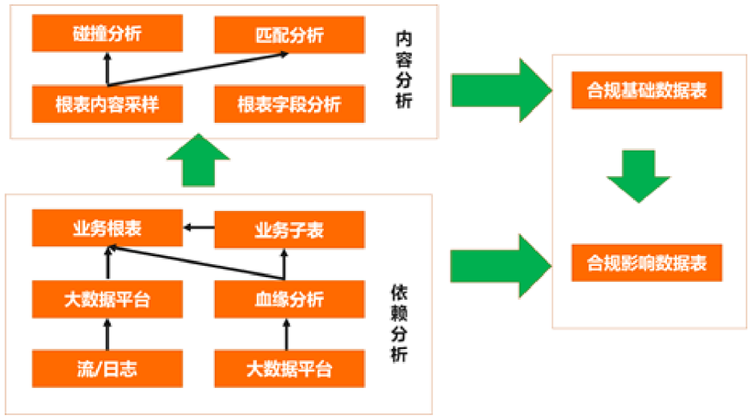
DB数据分析主要包含如下三个步骤：

- **内容分析：**扫描DB内容，随机采样部分数据，如1000条；按照字段内容同步到大数据平台，对比字段内容与敏感字段信息库，进行文本匹配分析，识别潜在的隐私内容；最后，关联到内容的来源DB表及字段。
- **结构分析：**离线获取所有DB表的表结构，识别对比DB表的字段名称，判断风险结构；
- **“数据-应用”关联分析**：以DB访问日志为基础，通过DB的相关操作；DB操作的目标IP， 整合IP与应用关系，最终获得影响相关应用信息。

除了上述的审计方案外，阿里云的数据库产品也提供了在线升级的功能。以RDS MySQL为例，其具备SQL洞察和审计的能力。SQL洞察和审计由数据库自治服务DAS提供，在全量请求和安全审计的基础上，融合了搜索、SQL洞察、安全审计以及流量回放和压测等功能，帮助您更好地获取SQL语句的具体信息、排查各种性能问题、识别高危风险来源、验证实例规格。具体可以参考：
https://help.aliyun.com/zh/rds/apsar-adb-rds-for-mysql/use-the-sql-explorer-and-audit-feature-on-an-apsaradb-rds-for-mysql-instance-6
其他各数据库产品也各自具备审计功能，数据库审计的功能已经与操作审计集成，可以在操作审计中查询用户操作云数据库产生的各管控事件。详情请参考：
https://help.aliyun.com/zh/actiontrail/product-overview/audit-events-of-supported-cloud-services/

5.7.2 离线审计

离线数据以大数据平台的离线表分析为主。通过大数据血缘分析，即分析表之间的依赖关系，分析得到根表及根表产出的子表；然后再进行根表的内容分析和结构分析，从而掌握隐私数据的来源去路；流数据等日志类数据，接入到大数据平台中，进入根表分析流程。



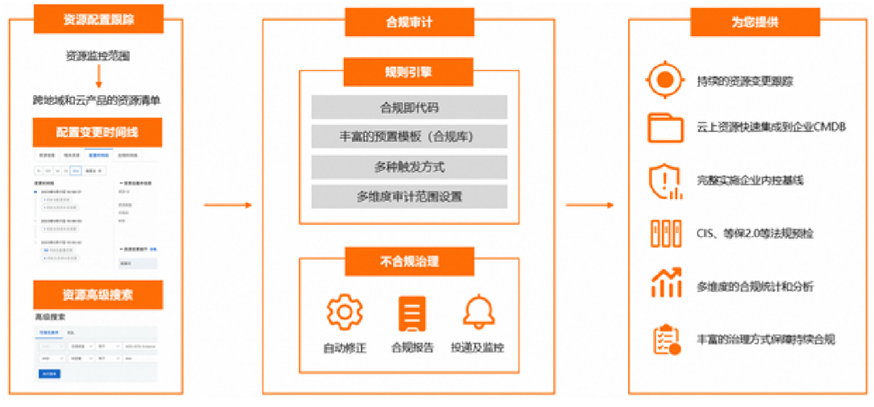
离线内容分析的基本方法有：

- **根表内容采样：**通过采样的方式，提取根表的内容信息；
- **碰撞分析：**直接进行内容碰撞分析，判断内容一致性；
- **匹配分析：**字段内容的模糊匹配和token匹配；
- **字段分析：**分析表字段名称信息

此外，也可以根据数据库的Binlog日志来进行离线审计。Binlog日志会准确记录数据库所有的增、删、改操作信息以及恢复用户的增量数据。Binlog日志先暂存在实例中，系统定期将实例中已经写完数据的Binlog日志转移至OSS保存7天。如果之前已经做好了数据的分级分类打标，则可以从Binlog中定位出针对敏感数据的不合规操作，从而达到离线审计的目的。

5.7.3 配置审计

阿里云的配置审计（Cloud Config）是一项资源审计服务，为您提供面向资源的配置历史追踪、配置合规审计等能力。面对大量资源，帮您轻松实现基础设施的自主监管，确保持续性合规。其实现远离如下图：



配置审计记录监控中资源的配置历史，并保存为配置时间线，即资源配置随时间推进的演变记录。用户可以查询与配置变更相关的操作事件列表和事件详情。配置审计也支持从模板创建规则和自定义创建规则。规则创建成功后，用户可以查看资源的评估结果和合规时间线，并对不合规的资源重新审计。对不合规的规则，可以执行修改、删除和停用操作。配置审计的合规库提供了丰富的合规包模板和规则模板，用户可以启用相应的合规项，对资源进行持续的检测。

关于配置审计，更详细的信息请参考阿里云官网：https://help.aliyun.com/document_detail/127374.html

5.7.4 操作审计

阿里云的操作审计（ActionTrail）能帮助用户监控并记录阿里云账号的活动，包括通过阿里云控制台、OpenAPI、开发者工具对云上产品和服务的访问和使用行为。这些行为事件可以下载或保存到日志服务SLS或对象存储OSS，然后进行行为分析、安全分析、资源变更行为追踪和行为合规性审计等操作。操作审计的实现原理如下：

5.8 使用数据合规工具与技术

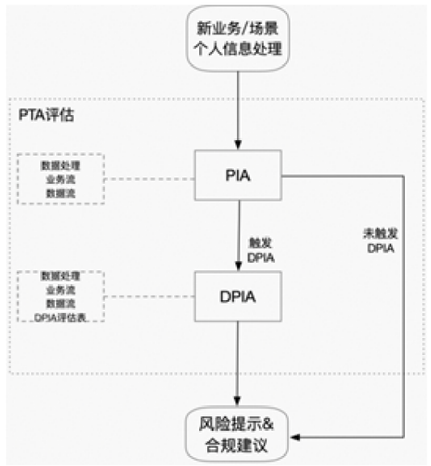
在传统法律行业和合规审计中，我们常见的是合规专业人士们手动对账，手动审核风险，对于互联网时代的海量数据，这个效率是很低的，所以需要有一些工具能在一些关键的方面帮助我们解决合规问题。合规工具需要围绕数据流转来设计，和数据本地存储跨境传输的流向基本保持一致。首先需要考虑的是如何对数据做审计和管控，只有从源头做好合规评估和管控才能应对后面复杂的合规场景，理想情况下我们需要对源头产生的每一个数据能了解它的产生来源、业务含义、使用方式等，才能对后续数据的传输、在不同国家地区法律政策限制下的使用策略做到比较全面的掌握。其次合规工具重点需要考虑的是跨境传输中数据的管控，业务场景下的数据传输是否符合合规，传输目的是什么，一般对于个人数据来说，经济目的是主要的，但不排除政治或者其他因素。另一个是接受国家或地区对数据的保护水平如何，如果保护水平较低，就需要考虑在工具层面做到数据限制和风险控制。

5.8.1 源头审计

对于一些新项目或者新流程来说，带来的必然会有一些新数据的产生，这些新数据是如何搜集的，搜集过程中是否涉及隐私合规，数据使用过程中涉及到影响面有哪些，这些都是需要我们考虑的，也是工具需要来解决的。欧盟的GDPR中已经对这部分有了比较规范的定义和实践，也就是合规中需要做的PTA、PIA以及DPIA。

- **PTA：**隐私阈值分析。新项目或者新流程前针对隐私阈值的分析，以帮助项目和相关人员明确在隐私方面的影响和风险。
- **PIA：**隐私影响评估。从业务和合规性角度考虑，明确何时启动隐私影响评估（PIA）。同时，明确触发启动PIA评估的原因，原因包括该项目是否收集了新的用户信息、是否进行了新的隐私数据处理、是否涉及与其他服务提供商共享数据。
- **DPIA：**数据保护影响评估。依据PIA评估的结果，从隐私数据敏感处理的角度考虑，明确何时启动数据保护影响评估（DPIA）。同时，依据PIA评估的报告，明确触发DPIA评估的原因。

常见的源头审计流程如下：



可以看到，PTA是整体的一个评估手段，而PIA和DPIA是这个手段中的两个阶段，且逐渐严厉和精细。针对以上这个流程，我们可以工具化来实现，在新项目和流程中设置卡口接入，进行PTA的评估。

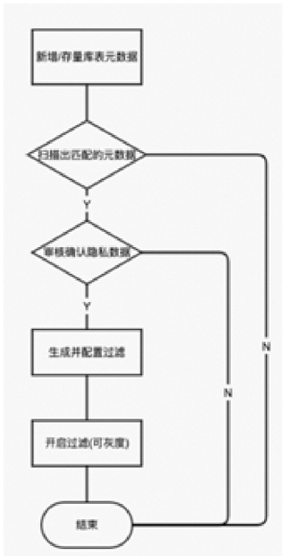
5.8.2 跨境过滤

源头数据有了比较好的管控后，接下来就是对于数据传输过程的管控，这也是传统合规中比较难覆盖的一块，大部分情况下，只能做到对源头数据产生方和目标数据接收方的管控，中间过程传输通常是管控不到的，也就意味着源头最终待传输数据和经过跨境传输到目标端接收到的数据是一致的。这个特别对于源头和目标数据政策不一致的情况比较难处理，所以我们需要能在中间传输过程进行管控。

对跨境过滤阶段的工具设计原则是对数据做切面，通过对常见的数据传输渠道进行卡口，具体在下面数据过滤章节会展开说明。如果当前技术受限，对于渠道的卡口无法做到技术上的限制的话（例如封闭的传输渠道无法进行切面卡口），可以考虑从流程管控上做一些卡口。

5.8.3 流程管控

需要在数据流通的每个环节做好管控，可以是工具层面的强管控，也可以是审批流程层面的弱管控。



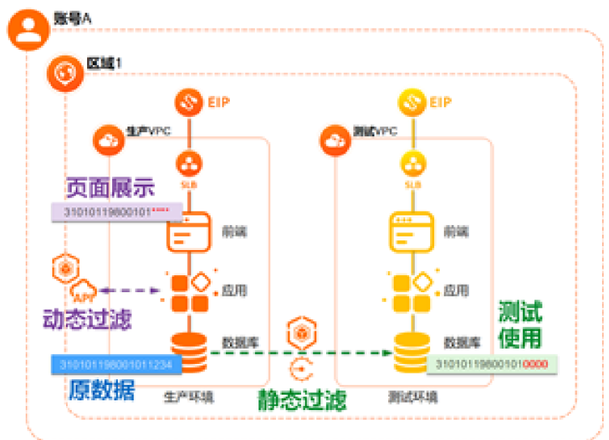
5.8.4 数据过滤

数据过滤是合规中非常重要的一部分，这部分也是工具方面最能助力的一块，对于庞大的数据和复杂的传输链路，如果想像人工审核一样处理，无异于天方夜谭，所以这块我们需要有一个合适的工具来协助我们完成。数据过滤和数据的分级分类所依赖的原理和产品类似，所以在这个领域，阿里云的数据安全中心（DSC）、大数据开发治理平台（DataWorks）、数据库产品族中的数据管理服务（DMS）都可以比较方便快速地帮助企业搭建起数据过滤的能力。

数据过滤主要用在数据跨境和数据跨主体共享场景中使用较多。无论是什么场景，首先要明确场景进一步细分下去的各种技术实现方式。以数据跨境场景为例：

数据源	过滤	说明
数据库RDS	binlog解析判断	通过binlog同步，可以解析binlog，根据合规条件判断是否接收binlog
大数据平台MaxCompute	copytask弱管控	copytask任务流程上卡点管控
消息中间件MetaQ	消息消费订阅判断	新增加一个消息消费管道

明确了具体的细分场景之后，再援引相应的技术方案来实现。例如如果通过DSC来实现数据过滤：



阿里云DSC产品详细介绍可以参考链接：阿里云数据安全中心（DSC）

5.8.5 数据删除与恢复

2020年3月Google被瑞典处罚700万欧元，因未能充分履行GDPR赋予用户的数据“遗忘权”。

在数据的正常运行过程中，数据热度从热、温、冷和冰的依次降温的转化作为归档过程，在销毁前需要有归档管理，再根据当地法律法规和数据的关键性价值把归档为“冰”之类的进行删除。数据销毁是指完全从存储设备、数据库、文件系统或其他数据存储介质中删除数据的过程。它不仅仅是简单地将数据从设备中删除，还包括确保数据无法被恢复，以防止数据泄露，保护隐私，遵守法规，并帮助企业有效地管理数据资源。

存储数据的物理介质，因故障无法读写需要报废时，对应负责部门或数据介质所属部门应进行物理销毁，并保留操作记录。因业务下线，机房裁撤等留存的物理介质，对应负责部门或数据介质所属部门应进行不小于三次的安全擦除，并保留操作记录。因监管规定，用户权利主张申请删除的数据，对应负责部门或数据owner应进行逻辑数据字段删除。长期不使用的公司物理介质，虚拟资源、数据库、报表，应用服务如Web、App、API、SDK等应进行资源释放或下线处理，对应负责部门或数据owner应进行安全的数据清理和管控，并保留操作记录。

这里重点需要关注的是数据销毁的合规以及数据销毁的管理。阿里云数据库产品系中的数据管理服务DMS和大数据产品系中的DataWorks都提供了合规的数据销毁与管理能力。

合规中涉及的另一个要考虑的方面是数据删除和恢复，在数据过滤后，过滤的只是增量新数据，对于存量数据，需要有一个解决方案来处理，否则对于这些存量数据还是会有合规风险，另一方面，对于一些识别为合规风险的数据，可能过了一段时间或者有新的合规政策出来后又是非合规风险数据，需要对这些被过滤删除掉的数据做一个恢复。

1. 数据删除

对于正常业务系统来说，数据删除是一个重要但技术上没那么复杂的事，评估好业务场景和风险，联系DBA或者自行删除即可，数据量大的情况分批低峰删除，但对于合规场景下的数据删除就没有那么简单了，前文提到，合规场景必然是关联到全球部署的，对于数据来说，也是全球存储，通过同步来实现数据一致性，这也意味着一个地区机房下的数据删除会连带着同步到其他地区机房，最终数据全部被删除，这显然不是我们的目的。所以数据删除需要解决的是如何在确保指定地区机房的数据删除情况下其他地区机房的数据还保留。

以MySQL为例，MySQL数据的主从同步和跨地区的数据同步一般都是基于binlog来完成的，读取源库的binlog，解析并写入目标库，这个就给了我们数据删除的一个切入点，如果源库的数据改动不产生binlog那就可以避免影响到目标库。基于这个特点，针对MySQL库的数据删除我们就可以有一个初步的解决方案，就是在对库操作数据删除时不产生binlog，当然这里只是针对符合合规删除条件的数据，正常数据还是需要开启binlog的。

2. 数据恢复

数据恢复是另一个场景下的需求，对于那些被识别为具有合规风险需要删除的数据，可能在政策变动，或者一些误识别为合规风险而被删除的数据，我们需要有一个恢复的方案来保证数据能重新传输到目的库中。

同样以MySQL为例，对于过滤掉的数据，如何快速恢复，主要可以考虑如下几种方式：
第一是从其他库同步过来，可以做到行数据级别，但这个需要考虑新老数据的实时性，以及同步后这些数据的后续更新是否正常。
第二是通过binlog转存恢复的方式，对于过滤的数据，将这些binlog转存，恢复时解析对应的binlog并写到目标数据源中。

阿里云出海能力中心&德勤中国 | 76

阿里云出海能力中心&德勤中国
ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

阿里云
全球合规生态能力

6.1 阿里集团合规实践方案
6.2 全球合规生态资源
6.3 德勤咨询服务

06 阿里云全球合规生态能力

企业如果需要出海数据合规的服务，不仅可以使用阿里云的云服务，也可以充分使用阿里云生态的解决方案与服务。阿里云的生态能力中，不仅有基于阿里集团全球最佳实践的合规轻咨询方案，也有与三方生态合作伙伴共建的能力，如Accenture，Deloitte等。企业可以通过阿里云进行咨询。

6.1 阿里集团合规实践方案

阿里集团在全球有着丰富的业务布局，基于Lazada、ICBU、Arise、AliExpress、菜鸟等海外业务的实践经验，阿里云进行了沉淀，可以给企业提供方案层面的参考，旨在帮企业快速建立海外合规能力。其中包括：

- 最小成本本地存储合规解决方案；
- 数据分级分类合规指导；
- 多用户身份权限统一管理方案；
- 办公数据安全保护方案；
- 远程开发与核心数据访问安全合规方案；
- 全球合规架构设计服务；
- 端到端cookie合规方案；
- 数据全链路加密方案；
- 跨境存储与访问管控合规方案。

6.2 全球合规生态资源

企业自己无法也没必要将合规问题全部解决的。逻辑上来说，正是因为有了外部监管的存在，所以才有了企业内部合规治理的需求。所以企业要善于充分利用外部的合规资源来帮助自身做好合规。具体来说，外部合规资源有如下五类，企业可以视自己的具体情况择用合适的外部资源。

1. 监管机构

监管机构除了进行执法监督之外，也会给出企业部分合规整改要求和建议，而且并不收费。因此企业的合规团队需要与监管机构进行密切沟通，一般来说，监管机构给出的合规要求是最低要求。企业最好的做法是主动与监管机构沟通，以及时获知与本行业以及所在国相关的监管信息。以GDPR为例，GDPR的监管机构是在国家一级设置的，是数据控制者或数据处理者所在成员国所指定的一个独立的公共主管机构，如法国的国家信息技术与自由委员会。

2. 评级机构

全球有诸多合规领域比较有权威性的评级机构与评级标准，如ISO27001，ISO27701，BSI，COBIT 5等。但以GDPR为例，目前还没有任何可证明GDPR合规性的认证。例如获得ISO 27001认证的组织有可能会满足许多在“适当的技术和组织措施”方面的安全要求，可以作为已实施适当的技术和行政控制的证据。在这种情况下进行差距分析，有助于确定组织需要怎么做才能使符合ISO 27001标准的系统达到GDPR的要求。

也因此，做过相关领域认证的企业或组织没必要重起炉灶，可以基于已有的能力进行补足，这是最具性价比的做法。

3. 法律服务外部供应商 （律师事务所、翻译机构）

对于全球布局业务的组织来说，有一个密切合作的律所是非常有必要的。法务服务外部供应商不仅可以提供及时、专业、全面的法律条文的解读与翻译，也能为海外当地牌照申请、资质认证提供助力。 此外，在发生合规风险紧急应对这一块，律师也能帮助企业找到

解决问题的最佳途径。从成本和效率的角度考虑，覆盖海外众多国家和地区，需要企业法务团队和外部供应商联合推进，帮助公司建立完善的、可落地的合规制度。

4. 咨询机构

主要指以德勤、埃森哲、毕马威、普华永道、安永等为代表的专业咨询服务机构。这些咨询机构将更细致地渗透到企业的业务流程和细分业务场景中去，根据企业的业务类型、数据生命周期以及技术系统结构，通过访谈、调研、现状评估与差距分析、合规建议以及合规治理技术落地等服务动作，帮助企业达到合规目标。

5. 云服务厂商

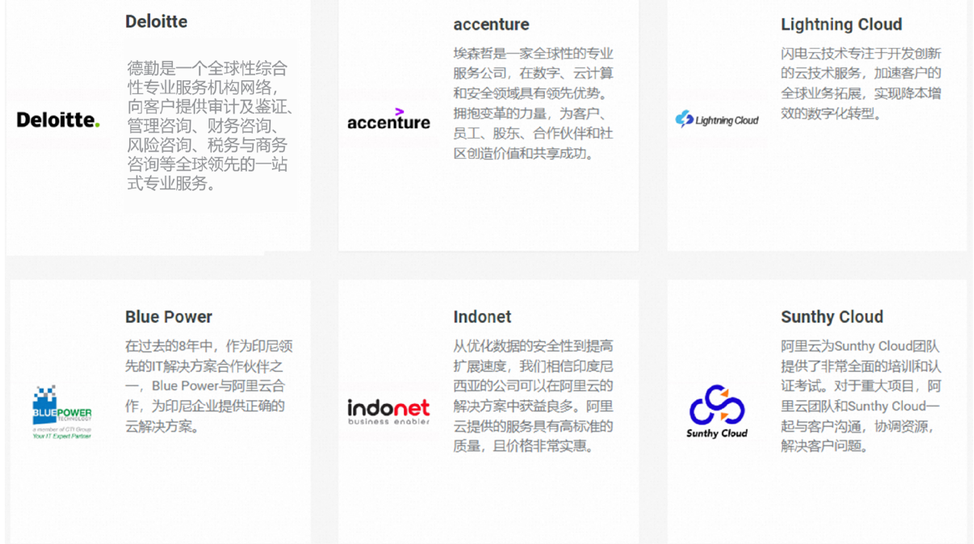
由于云的很多产品本身就收敛了一定的合规能力，而且云计算厂商由于服务客户的广度和深度，积累了众多其他企业做合规建设的案例参考。此外，以阿里云为代表的云服务厂商还有阿里集团海外诸多业务数据合规的最佳实践加持，因此云服务厂商提供了一条从产品和咨询视角出发的非常不一样的合规能力。如果企业能善用云厂商的力量，那么合规能力建设将事半功倍。

上面简要介绍了企业可以寻找的五类合规资源。合规的体系化能力建设是个长期且复杂的过程，而且随着所在国的法律法规的变化，这个建设过程是没有尽头的。阿里云基于阿里集团的最佳实践，与生态合作伙伴一起提供整体的咨询方案。可以初步从阿里云市场上进行了解，链接如下：合规产品解决方案

对于很多企业来说，由于数据不止局限于用阿里云来处理，也会有异构的云供应商乃至用自建IDC来处理，所以落地数据全生命周期的合规治理需要往上抽象一层。

如上图所示，在这方面阿里云基于阿里集团的最佳实践，与生态合作伙伴一起提供的整体咨询服务。具体可以联系阿里云。

阿里云庞大的全球生态体系中有很多生态伙伴可以为出海企业在全球业务开展提供端到端的合规服务。此外阿里云在海外当地也有繁荣的技术咨询伙伴体系，除了合规，在营销、销售、售后等关键环节也可以帮助出海企业快速扎根当地市场，降低业务拓展成本，提高业务成功率。

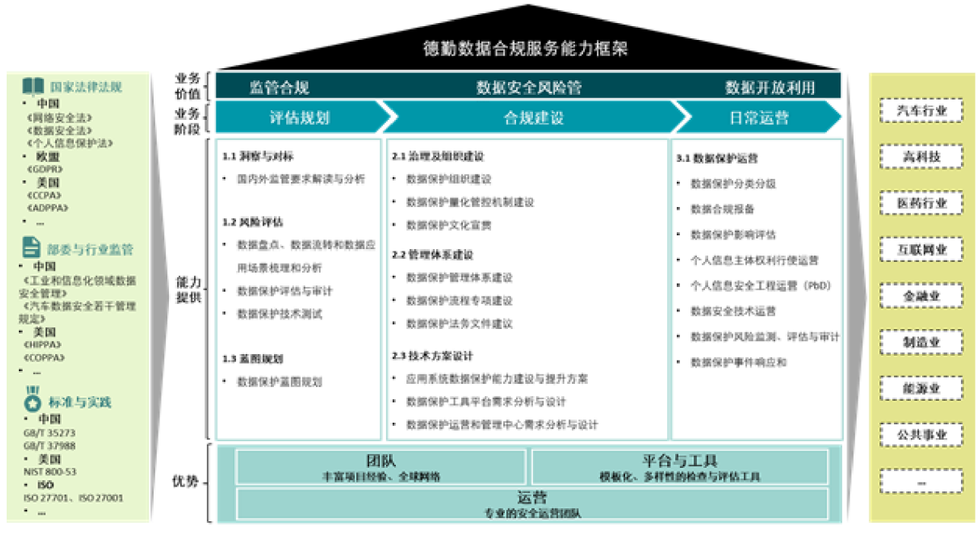


6.3 德勤咨询服务

德勤是一家全球领先的综合性专业服务机构，在数字化、云计算与网络安全领域拥有全球领先能力，根据Gartner报告，德勤连续十二年蝉联全球安全咨询服务市场份额排名第一，并且连续多年被Gartner评为全球数据管理与分析领域的领导者。凭借丰富的业内经验与专业技能，以及翘楚全球的卓越技术中心和智能运营中心，德勤为客户提供战略和咨询、技术和智能运营等全方位服务，业务服务逾150个国家或地区，为财富全球500强企业中的80%提供专业服务，协助客户应对极为复杂的商业和技术挑战。德勤以“因我不同，成就不凡”为宗旨，为资本市场增强公众信任，为客户转型升级赋能，为人才激活迎接未来的能力，为更繁荣的经济、更公平的社会和可持续的世界开拓前行。在数据合规咨询领域，德勤拥有完善的数据安全治理框架，从数据安全战略、数据安全流程、数据安全技术、数据安全运营等多个领域为企业提供端到端的全方位数据安全服务。我们的服务包括数据安全咨询、实施和运营的全过程，并且能够根据企业的业务特点和需求提供定制的数据安全解决方案，帮助客户实现长期可持续的数据安全与合规。我们的业务阶段包括：

在数据合规咨询领域，德勤拥有完善的数据安全治理框架，从数据安全战略、数据安全流程、数据安全技术、数据安全运营等领域为企业提供全方位、端到端的数据安全服务，覆盖数据安全咨询、实施、运营全过程，并能针对企业的业务特点和需求制定专项数据安全解决方案，帮助客户实现长期可持续的数据安全与合规，业务阶段包括：

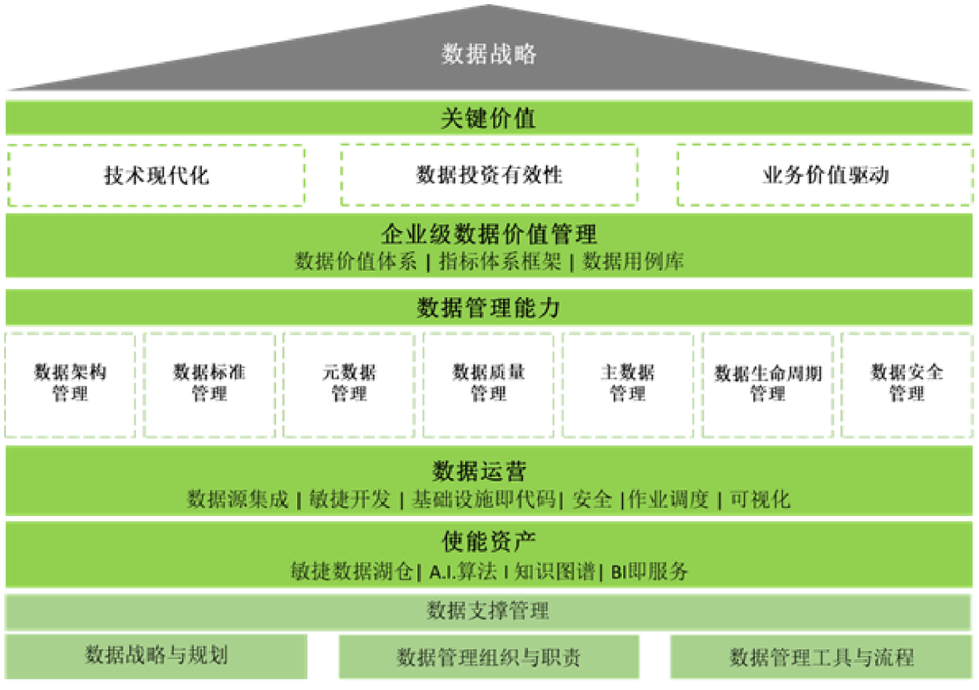
- **评估规划**：德勤整合了自身在数据安全咨询、技术能力整合和安全落地运营的端到端交付能力的经验和优势，采用Plan-Do-Check-Action的持续改进理念，通过解读与分析国内外监管要求，对企业数据做盘点、做数据流转、数据的应用场景进行梳理和分析，对企业数据保护流程和技术的评估分析和对企业的数据保护做蓝图规划，不断推动企业数据安全合规，持续地为企业的跨境业务保驾护航。
- **合规建设**：德勤数据安全治理体系建设以“数据”为中心，从组织、管理体系和技术这三个维度，通过构建全流程、可闭环的完整链条，确保数据资产可视、数据威胁可管、数据风险可控。德勤数据安全风险管理服务从企业数据安全合规建设的痛点出发，协助企业高效、敏捷、低成本地实现全生命周期数据安全风险管理服务。
- **日常运营**：德勤可以帮助客户对所有数据存储库中的数据类型进行自动数据发现和分类分级，对等级保护定级、整改、测评、备案和持续改进提供全流程技术的技术咨询服务，对向第三方传输数据的数据处理活动进行第三方风险评估，帮助企业管理和运营个人信息主体权利、个人信息安全和数据安全技术，建立数据清单和数据安全评估申报材料，评估和部署适当的数据安全解决方案，构建基于事件的应急响应机制以满足监管部门的合规要求等。



不仅限于数据全生命周期的合规治理的咨询服务，德勤还能够针对企业自身的需求，提供企业在海外市场实现数字化的一体化服务，例如数据治理、数据湖建设、数据可视化、决策分析、预测分析、以及AI应用等数据增值服务。根据德勤长期以来在企业转型和数字化方面的深入研究，基于在5G、大数据、人工智能、云计算、区块链等最新数字化转型技术的多年积累，企业可以通过德勤咨询服务从海量数据中获得关键数据洞察，实时帮助管理者制定有效策略，帮助企业降本增效。德勤的数据咨询服务包括以下几个方面：

- **数据支撑管理：**德勤可以协助企业制定长期的数据战略规划，明确企业内部数据管理组织结构与职责，帮助企业做数据管理工具选型和建立完善数据管理体系和流程。
- **数据资产使能：**德勤可以指导企业如何将数据资产赋能组织，比如湖仓一体，人工智能算法，知识图谱，BI即服务等。
- **数据运营服务：**德勤可以为企业构建一套完整的数据资产运营体系，通过数据资产识别、数据资产维护、和数据资产服务，更好地促进数据价值的释放，以体系化的方式实现数据的可得、可用、好用。
- **数据管理服务：**德勤支持企业全域数据资产管理，包括数据架构管理、数据标准管理、元数据管理、数据质量管理、主数据管理、数据全生命周期管理、数据安全管理等。
- **企业级数据价值管理：**德勤针对企业业务发展、数据资产价值体系、客户服务、组织激励等管理领域，通过建立完善和有效的价值管理体系和用例库，为企业管理层以及各个业务部门提供高效透明的数据服务，实现企业的精准评价、精准投资、精准激励，不断提升企业的数据洞察能力和高效决策能力。

在业务全球化拓展领域，德勤拥有丰富的洞见和全面的专业服务：中国企业出海二十多载，经历过泡沫般的快速增长和严格的政策调控，重回了业务发展本质驱动。近年，往外走的中国企业来越来越注重海外供应链整合与品牌建设，运营也逐渐开始本地化，而其全球运营能力也愈发受到关注。



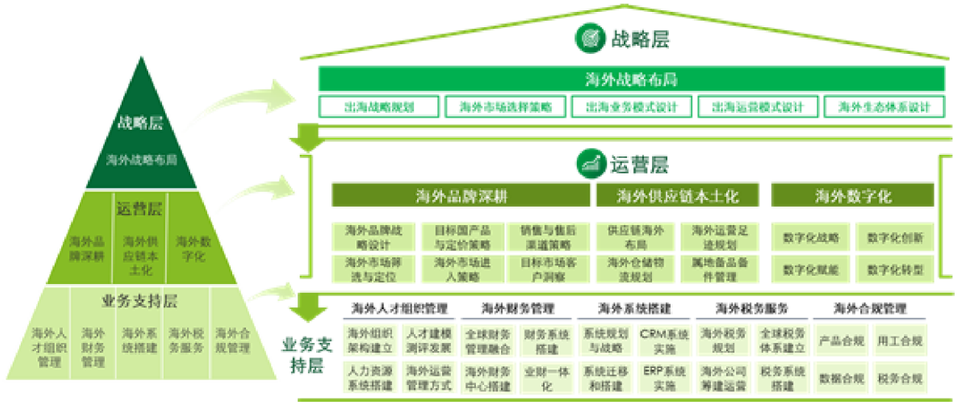
在业务全球化拓展领域，德勤拥有丰富的洞见和全面的专业服务。中国企业出海二十多载，历经了快速增长和严格政策调控等阶段，重回了业务发展的本质。近年来，往外走的中国企业越来越注重海外供应链整合与品牌建设，运营也逐渐开始本地化，其全球运营能力也备受关注。

中国企业全球化的机遇伴随着挑战。德勤认为，中国企业出海模式可以分为出口贸易、海外营销、海外运营及全球化运营四大类。然而，无论企业采取何种模式，都面临着风险多、管理难、差异大、韧性差四种共性挑战。对此，德勤认为可以从战略、运营和能力底座三个视角进行考量和规划。

首先，从战略角度看，中国企业通常没有充分认识到全球业务的复杂性和不确定性，难以有效梳理发展重点和脉络，缺乏自上而下的顶层设计。其次，从运营角度看，中国企业通常对于海外业务管控过于僵化，导致其难以迅速扩张并及时调整。随着业务走向国际化，企业缺乏具有前瞻性的全球化供应链战略体系和布局，影响了企业全球运营的效率。最后，从能力底座角度看，数字化已经成为国际化进程中愈发重要的一个环节，各市场的数据割裂导致许多中国企业无法对全球业务和运营情况进行有效的数据分析和洞察，数据合规性与安全性也仍有待提升。

为了帮助中国企业持续应对海外经营的不确定性，真正实现价值提升，推动境外经营的持续运作，跨国经营发展管理能力的不断完善和提升正是企业后续属地化经营发展的关键引擎。德勤的“跨国经营能力成熟度模型”，涵盖了从战略到运营再到人才管理以及基础体系共十个维度。

“跨国经营能力成熟度模型”是德勤对于企业经营发展管理领先实践的总结，基于全球领先企业的实践经验提炼而成，能切实帮助探索全球化发展的中国企业识别评估其能力现状并提供可行的能力建设建议。与此对应的是德勤出海服务全景图，依托在各行业的深厚咨询经验，德勤为中国企业出海路上提供“战略-运营-业务支持”一站式解决方案，为中国企业出海赋能，并助力中国企业全球化运营。



德勤认为，在中国企业出海的能力组成中，主要有三大主题：一是从业务蓝图设计到落地，二是结合组织和人力方面的需求到变革以及最终的实施，三是供应链的整体设计、落地及属地化运营。而这三大主题离不开两大底座的支撑：一是数据安全及数字化，二是职能/管理能力的提升和全球化。同时，搭建企业跨境税务管理体系（包括海外新公司筹建运营）、管理海外合规与风险（包括数据安全、ESG、运营等领域）以及资本规划，也是企业出海时必要的考量因素。

在出海实操中，德勤发现中国企业通常面临三大关键矛盾：

1.不确定性环境与安全发展底线之矛盾：例如，某清洁能源解决方案供应商在人力资源应用系统建设中，面临着全球合规风险挑战、组织协同效率较低等问题。德勤通过合规性机制设计，确保满足全球人力资源管理的数据要求，降低合规性风险，并突破业务链接点，极大地提高员工和企业的协同效率。

2.产品技术实力与国际化品牌形象之矛盾：例如，某手机品牌在海外面临着打造品牌影响力的挑战。德勤通过Service Cloud技术实现新平台的构建，高效优化内部运营流程以提升服务效率，从而实现客户满意度提升，打造更高的品牌影响力。

3.国际化业务布局与属地化经营管理之矛盾：例如，某生物生产制造企业收购美国某工厂后遇到如何将国际化经营变得长期化、全面化和深度化，以属地化布局增强发展韧性的挑战。德勤通过收购的投后整合与赋能提升咨询服务，实现战略、管控、人员稳定、赋能与发展、文化及组织结构等各层面目标。

德勤始终致力于在中国企业跨境投资并购和后续整合运营过程中提供支持；凭借以往的项目经验与独特视角，不畏挑战、砥砺前行。未来，德勤也将继续发挥自身的专业优势，立足本土，连接全球，不遗余力地助力中国企业实现全球化目标。

阿里云出海能力中心&德勤中国

ALIBABA CLOUD & DELOITTE CHINA

中国企业海外业务数据合规指导书

参考资料

07 参考资料

1.Data Protection in India: Overview by Supratim Chakraborty, Khaitan & Co LLP, with Practical Law Data Privacy & Cybersecurity

2.Personal Data Transfer Restrictions (Japan) by Oki Mori and Takeshi Hayakawa, Nagashima Ohno & Tsunematsu, with Practical Law Data Privacy Advisor

3.Data Protection in South Korea: Overview by Kyung Min Son, Lee & Ko, with Practical Law Data Privacy & Cybersecurity

4.https://www.pwccn.com/zh/services/consulting/publications/strategies-for-data-security-protection-of-chinese-internet-companies-apr2021.html

5.https://en.investgo.cn/article/hzxxc/anyong/202103/535035.html

6.http://www.landinglawyer.com/a/landigongyi/1200.html

7.https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P16-#P16

8.https://zhuanlan.zhihu.com/p/403190604

9.http://www.hackdig.com/08/hack-122402.htm

10.https://www.dongchedi.com/article/7084518494632722955

11.https://www.secrss.com/articles/43758

12.http://www.cicjc.com.cn/info/1040/14919.htm

13.https://www.shangyexinzhi.com/article/11127558.html

本书作者

毕龙飞，阿里云出海能力中心资深解决方案架构师，fengwu.blf@alibaba-inc.com

刘珺，阿里云法务专家，jingqi.lj@alibaba-inc.com

陈维皓，德勤中国管理咨询并购整合重组服务领导合伙人，vicchen@deloitte.com.cn

江玮，德勤中国风险咨询网络安全合伙人，davidjiang@deloitte.com.cn

钟建华，德勤中国管理咨询合伙人，jhzhong@deloitte.com.cn

林松祥，德勤中国风险咨询网络安全合伙人，chaphylin@deloitte.com.cn