腾讯云

IBM

合规翼展 御浪远航

企业出海数据合规指导书



【 版权声明 】

本报告相关部分版权属于腾讯云计算（北京）有限公司或IBM（中国）有限公司，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：腾讯云计算（北京）有限公司或IBM（中国）有限公司”。违反上述声明者，权利人将追究其相关法律责任。

【 主要作者 】

毕龙飞　腾讯云出海行业 专家架构师
郑　鑫　腾讯云政企行业 市场总经理
贺　明　腾讯云出海行业 技术总经理
魏子瑞　腾讯云出海行业 高级架构师
周洪飞　腾讯云制造行业 专家架构师
程立伟　腾讯云教育行业 高级架构师
杨子维　腾讯云金融行业 资深项目经理
丁　伟　IBM中国商业价值研究院 院长
石延霞　IBM中国商业价值研究院 高级咨询经理
王　莉　IBM中国商业价值研究院 高级咨询经理
孙爱军　IBM中国商业价值研究院 高级咨询顾问
包娜布棋　IBM中国商业价值研究院 咨询顾问
胡琼琼　IBM咨询大中华区战略咨询部 高级咨询经理
蔡广宁　IBM咨询大中华区战略咨询部 咨询经理
孔祥慧　IBM咨询大中华区混合云转型咨询部安全&隐私团队 咨询经理
黄子芸　IBM咨询大中华区混合云转型咨询部安全&隐私团队 咨询经理
曾工棉　IBM咨询大中华区混合云转型咨询部安全&隐私团队 咨询顾问
夏小婷　IBM咨询大中华区混合云转型咨询部安全&隐私团队 咨询顾问
卢依湄　IBM咨询大中华区混合云转型咨询部安全&隐私团队 咨询顾问
金希玥　IBM咨询大中华区混合云转型咨询部安全&隐私团队 咨询顾问

【 致谢 】

感谢以下部门领导及专家对本指导书的支持和指导

腾讯云与智慧产业事业群：汤道生、邱跃鹏、李强、钟翔平
腾讯云与智慧产业事业群CSIG市场部
腾讯云与智慧产业事业群泛互联网、制造与能源、金融、教育、出行行业
腾讯云与智慧产业事业群港澳台及国际业务部
腾讯云与智慧产业事业群安全产品部、云鼎实验室
腾讯云与智慧产业事业群产业生态合作部
腾讯数据合规与隐私保护部
腾讯海外法务中心
腾讯云与智慧产业事业群公共事务部
腾讯研究院
IBM咨询大中华区：Kher Tean Chen、李民、董海军、马勇、张玉明、石晓刚、殷俊

Contents
目录

01 企业出海形势分析与合规要求 001

企业全球化的新纪元 002
企业出海路径及趋势 003
企业出海过程中的合规要求概述 004
数据合规的重要性 006

02 企业出海面临的数据合规挑战 007

全球法律法规的多样性 008
数据跨境传输的复杂性 009
- 国家安全 009
- 数字主权 009
- 数据本地化 009

数据合规策略的一致性 010
不同行业数据跨境的特殊性 011

03 各国家地区数据合规法规概览 012

欧盟 013
北美 019
- 美国 019
- 加拿大 021

拉丁美洲 023
- 墨西哥 023
- 巴西 025
- 阿根廷 027



中东地区 029
- 以色列 029
- 沙特 031
- 阿联酋 033
- 土耳其 036

东南亚 037
- 印尼 037
- 新加坡 040
- 泰国 043
- 越南 045
- 马来西亚 047

印度 049

俄罗斯 051

日韩 053
- 日本 053
- 韩国 055

非洲 057
- 埃及 057
- 南非 059

大洋洲 061
- 澳大利亚 061
- 新西兰 063

中国 065

04 数据合规体系建设 071
站在全球看全球 072
全球化框架 072
定战略 073
布业务 073
搭运营 074
建系统 075
数据安全与合规体系 076
企业出海数据现状概览 076
全球化数据合规管理组织 083
数据合规管理制度与流程 087
数据合规技术体系 089
数据合规运营体系 107
数据安全与合规嵌入研发流程 114
Security and Privacy by Design 114
IT系统开发生命周期中的安全隐私管控 116
工业产品（汽车为例）V模型的安全与隐私设计 119

05 腾讯出海/数据合规服务产品及解决方案 120
腾讯云在数据合规中的责任与建议 121
腾讯云全球合规资质认证 121
腾讯云的合规资源与能力准备 125
角色：合规责任共担模型 125
腾讯云平台数据合规保障 127
国际站账号 127
云平台数据保护能力 127
云平台数据安全治理体系 129
云平台供应链合规 130
云平台数据留存与删除管理 131
云平台数据合规问题应对体系 132
云平台的透明性与可审计性 132
腾讯云数据合规工具箱 133
数据安全 133
数据权限管理 142
数据合规审计 149
可信计算 152
数据库 154
大数据与数据湖 157

腾讯云助力数据重要环节的安全合规 167
数据生命周期视角合规实施框架 167
数据采集收集 168
数据存储 168
数据共享 169
数据使用 169
数据传输 170
数据删除与销毁 170

06 不同行业出海数据合规建议 171
跨境电商 172
社交文娱 176
游戏 181
汽车/出行 185
教育 193
金融服务 195
传统制造业 203
智能终端制造业 207
行业案例梳理 211
某跨境电商企业数据合规审计体系化建设 211
某社交公司海外数据合规落地实践 211
三一集团有限公司海外数据出入境合规管控 212
某能源企业数据跨境合规项目 212
某制造业人力资源运营模式转型项目 213
某制造业海外一体化运营项目 213
某生物医药企业数据跨境合规项目 214
某国有大型银行数据跨境项目 214

07 中国企业出海数据合规关键行动建议 215
精准识别：数据合规要求 216
精细梳理：数据出境场景 216
规范评估：数据合规差距 216
高效修复：合规改进建议 217
标准编制：出境评估报告 217
体系搭建：长效管理机制 218

01

企业出海形势分析与合规要求

企业全球化的新纪元

企业出海路径及趋势

企业出海过程中的合规要求概述

数据合规的重要性

企业全球化的新纪元 1.1

全球化是一个动态演化的进程，随着人类文明的不断发展，全球化也经历了不同阶段的演变。从二十世纪九十年代的早期全球化到近年来的再全球化，全球化的格局也在急速变化。早期的全球化阶段，从近代工业革命开始至一战、二战期间，全球化主要表现为商品、资本、劳动力的跨境流动，以及国际社会在努力降低国家对于国际商品、服务、人员、知识产权跨境流动所设置的壁垒，使得国际经济贸易的法律环境变得更为顺畅。这几个阶段的全球化是自由贸易和资本流动的体现，促进了全球经济的快速增长和国际交流的增加。

2020年以来，随着疫情的全球蔓延，全球经济受到冲击，许多国家开始对原有的经济运行方式和法律制度进行重新审视。与早期的全球化相比，当前的全球化更加注重建设当地的供应链体系，强调与当地社会的融合与发展。这一变化反映了全球化进程中的动态调整和适应，以及不同国家在全球经济中的角色和地位的变化。在复杂多变的国际贸易环境之下，中国企业出海一方面是主动参与国际循环，应对国内部分行业市场饱和等现实问题的必然选择；另一方面也是中国企业核心竞争优势不断扩大、国际影响力逐渐增强的直接体现。总之，今天中国企业思考和推动适合自身发展的、新的全球化战略已经成为时代发展的必然。

全球化的四个阶段

全球化第一阶段

约1492年–1914年

航海技术的发展打开了国与国之间的交流渠道。此阶段全球化的特点聚焦在原材料，商品和人力的流动

全球化第二阶段

约1914年–1989年

两次世界大战的矛盾态势驱使各国在政治，经济等多领域展开更深入的互动与交流

全球化第三阶段

约1989年–2019年

上世纪90年代，互联网的普及使全球经济贸易，文化交流进入了一个新的高峰期

全球化第四阶段

2020年至今

再全球化趋势，更加注重建设当地的供应链体系，强调与当地社会的融合与发展

在变局之下，中国企业的全球化主要受到以下三个关键因素的推动：

- **企业自身发展壮大的原动力**：中国企业自身的发展壮大成为推动其全球拓展的内生动力。随着全球市场的紧密联系和贸易自由化的推进，中国企业意识到在全球舞台上拓展业务的机遇和必要性，以获取更广阔的市场、资源和合作伙伴。在可再生能源与储能、新能源汽车、电子商务、游戏开发等新兴行业中，许多中国企业已具备国际竞争力，海外市场成为其业务增长的重要驱动力。2024年初数据显示，国内头部新能源车企2023年第四季度销量首次超过海外新能源车企，标志着中国在全球电动汽车市场上的新兴实力[1]。
- **国内市场竞争激烈的强压力**：一方面，中国企业目前也面临着将近饱和、竞争激烈的国内市场，企业持续盈利的能力存在较大挑战。因此，开拓海外市场成为这些企业继续发展乃至生存的必然选择。另一方面，产业升级的历史逻辑需要中国企业在全球价值链中积累资本，加强创新，并向价值链中高附加值环节上升。这也进一步推动中国企业积极进军海外市场，寻求更广阔的发展机遇。以工程机械行业为例，2023年我国工程机械新机需求不旺，内销大幅下滑，但是工程机械出口依然保持增长态势。据海关数据整理，1–11月我国工程机械产品累计出口额446.22亿美元，同比增长10.6%[2]。
- **中国政府双循环战略的推动力**：中国政府的政策推动是中国企业走向海外市场的重要动力。中国实施的“双循环”战略需要加强对外循环，促进更多中国企业在海外市场扎根发展。政府推出了一系列支持企业海外投资的政策和措施， 为企业拓展全球业务提供了支持和便利。

中国企业在全球化的过程中，需要不断学习和适应，以应对各种复杂的国际环境和竞争挑战，同时抓住全球化机遇，思考和推动适合自身发展的、新的全球化战略，实现高质量、可持续发展。

[1] 陈宇轩、印朋、梁希之. “中国新能源车企销量再创新高 巩固全球领先地位”. 新华社. 20240105. https://h.xinhuaxmt.com/vh512/share/11844277?d=134d6e9&channel=qq

[2] 《去年中国挖掘机销量降25%：12月内销开始增长，海外仍是主要增长点》. 澎湃新闻. 20240110. https://m.toutiao.com/is/iLrL6e2J/

企业出海路径及趋势 1.2

中国企业“走出去”，面对着数字化转型、全球市场扩张和创新合作等新机遇。同时，它们也面临技术竞争和保护主义、跨文化管理和品牌建设、可持续发展和社会责任等挑战。

总体来说，中国企业走出去有三种路径：

- **供应商合作**是指与当地成熟的销售供应商合作，由供应商帮助拓展海外市场。这种路径的初始成本较低，可以借助供应商的分销网络、跨境物流、数据分析等能力，快速切入市场。然而，由于企业自身并不掌握核心分销资源，利润会受到影响。

- **投资自建**是指在直接海外投资设立分公司，从零开始拓展市场。这种路径需要企业根据自身的业务情况，选择目标国家和地区，制定建设的方向和策略。这种模式对企业出海人才的储备、经验及运营能力有较高要求。同时，由于一切从零开始，需要的周期较长，建设的速度和切入市场的速度也会有一定影响。

- **海外并购/合资**是指通过收购海外已有的公司或团队，获取其业务、渠道、品牌、技术等资源，或者与海外合作公司共同出资完成资源共享。这种路径便于快速切入海外市场，可以直接获取海外公司较为成熟的销售渠道、供应链体系等，也有利于企业遵从海外的法律法规。然而，在标的筛选、团队融合、谈判周期、投资金额等方面都需要付出更多的成本。

随着我国企业出海的数量不断增长，出海策略持续迭代，中国企业全球化的新阶段，呈现出以下特点和趋势：

- **注重技术创新驱动**：中国企业越来越注重技术创新，努力提升核心竞争力。通过自主研发和技术引进，中国企业在不少关键领域取得突破，国际市场竞争力进一步增强。2022年中国互联网公司网易宣布成立首家美国游戏工作室Jackalope Games推动技术创新。利用当地的技术人才和创新环境，进一步提升游戏开发和技术能力，推出更具创新性和竞争力的游戏产品[1]。

- **加大跨境投资和并购**：中国企业加大了对海外市场的投资力度，通过收购、并购等方式获取海外资源、市场和技术。这有助于提升企业的全球影响力和市场份额。阿里巴巴于2016年宣布收购新加坡电商平台Lazada的控股权，通过这一交易，阿里巴巴进一步扩大了其在东南亚地区的市场份额。Lazada是东南亚最大的电商平台之一，涵盖多个国家，包括印尼、马来西亚、菲律宾等。通过收购该企业，阿里巴巴能够利用其强大的物流和电商基础设施，进一步拓展在东南亚地区的业务[2]。

- **重视品牌建设与文化输出**：中国企业越来越重视品牌建设和文化输出。以往中国企业主要依赖商品出口贸易的模式拓展海外市场，现在更多的企业注重打造具有国际竞争力的品牌形象，通过文化产品和服务输出能力，提升了中国企业的全球影响力。TCL致力于品牌建设和市场拓展，通过参与国际知名赛事和赞助顶级体育俱乐部等方式提升品牌知名度。TCL还积极拓展海外市场，与全球的零售商、电信运营商和合作伙伴建立合作关系，加强产品的销售和分销网络[3]。

- **推动服务贸易和创新合作**：相较于之前中国企业在海外单打独斗，当今中国企业在全球服务贸易中的地位不断提升，积极参与国际产业链，开展跨国创新合作，推动了全球合作与资源共享。2023年，宁德时代匈牙利电池工厂规划产能100GWh，一期已开工建设，预计2年左右建设完成。同年，全球第四大汽车集团Stellantis集团与宁德时代宣布双方已签署备忘录。在该备忘录中，宁德时代将在欧洲当地向Stellantis集团供应磷酸铁锂（LFP）电池的电芯和模组，助力Stellantis在欧洲市场的电动汽车生产[4]。

[1]《网易游戏首家美国工作室！Jackalope Games正式成立》. 网易. 20220506. https://www.163.com/dy/article/H6N2HHQO05465WDP.html

[2]《Lazada再获阿里注资，东南亚电商市场跑马圈地已开始》. 21世纪经济报道. 20230721. https://rmh.pdnews.cn/Pc/ArtInfoApi/article?id=36832194

[3]《TCL全球化营销战略升级，签约内马尔为全球品牌大使》. 钛媒体. 20240115. http://www.hzhcontrols.com/new-8268.html

[4]《宁德时代与Stellantis签署战略谅解备忘录 探讨成立合资公司》. 腾讯网. 20231121. https://new.qq.com/rain/a/20231121A05VG300

- **践行可持续发展和社会责任**：中国企业越来越注重可持续发展和社会责任。他们关注环境保护、社会公益和企业道德，努力在全球范围内推动可持续发展目标的实现。某头部新能源汽车厂商致力于推动可持续供应链管理。他们与供应商合作，确保采购的材料和零部件符合环保标准，减少环境影响。同时还鼓励供应商采用可再生能源和节能措施，提高整个供应链的可持续性。

企业出海过程中的合规要求概述 1.3

在中国企业拓展国际市场的过程中，合规能力的建设必不可少。企业在海外运营中面临着不同国家和地区的法律法规和数据保护要求，数据合规不仅关系到企业的声誉和信任度，更直接影响到企业在全球市场的运营效率和竞争力。数据合规是本文的主要关注点，将展开详细阐述。

除了数据合规以外，中国企业出海过程中面临的其他合规要求还包括财税合规、人力资源合规、知识产权合规、贸易管制与制裁等。

- **财税合规**

  合规的财税管理可以帮助企业遵守当地法律和规定，高效管理财务风险，确保企业的可持续发展。每个国家或地区都有其特定的税收法规，企业需要确保其商业活动的合法性，并按照规定完成税务申报和缴纳。否则，企业将可能面临罚款、禁业等行政处罚。

  企业在跨境财税合规方面遇到的主要问题有：

  税收管辖权冲突：跨境企业可能面临多个国家和地区的税收管辖权冲突，导致双重征税或出现税收漏洞。当同一笔收入在两个不同的税收管辖区内都要缴税时，就会构成双重征税，这对于企业而言无疑是一种重复的负担。

  转移定价：在跨境企业关联交易中，转移定价可能受到税务部门关注，需要合理规范以避免税收风险。

  永久性机构：跨境企业需要明确哪些海外活动可能构成永久性机构。一旦构成永久性机构，企业则需要按照所在国的规定缴纳相应的企业所得税。

  财税信息对接：各国近年来加大了财税信息透明度的要求和跨境税收信息对接力度，跨境企业需要做好全球财务信息的申报。

  为实现跨境财税合规，中国企业在出海前，应进行详细的财税规划和准备工作，例如，了解目标国家的税法、会计准则和报告要求，了解税款缴纳和报表申报规则等。同时，企业还需建立健全的审计和内部控制系统，加强利润调整和会计核算，确保财务报表的准确性和合规性。此外，在进行国际贸易时，企业需要遵守相关的关税、进出口贸易规定和海关法规，如商业合同、国际支付等规定。

- **人力资源合规**

  人力资源合规也是中国企业在海外市场开拓中不可忽视的问题。中国企业如果对于出海国家当地的法律法规和劳动法了解不深入的话，容易在用工时产生劳务纠纷或面临高额罚款。此外，签证类型不适当也可能带来出入境管理风险。

  中国企业在海外雇佣员工之前，需要深入了解当地的劳动法律法规，包括最低工资标准、劳动时间、员工福利、假期制度等。建立完善的用工制度和流程，包括招聘流程、薪酬福利、员工培训等，以确保员工能够在合规的框架下开展工作，同时也提高员工的满意度和忠诚度。此外，还需针对管理者和员工开展法律法规培训和指导，并定期对合规情况进行检查，及时发现问题并予以解决。

- **知识产权合规**

  不同国家和地区在知识产权保护方面的法规差异比较大，中国企业需要保护自身的创新成果不被侵犯，必须具备跨国知识产权管理和风险防控的能力。此外，在参与国际竞争的时候，欧美地区的企业常常通过知识产权侵权诉讼等方式针对中国企业，一旦在海外遭遇知识产权诉讼，中国企业需要面临较长的诉讼周期和高昂的应诉成本，不仅影响海外业务发展，而且还可能对企业的长期竞争力产生负面影响。因此，建立系统的知识产权风险防控机制非常必要。

  中国企业在出海过程中常见的知识产权风险包括：海外知识产权诉讼风险（如专利侵权、商标侵权和商业秘密侵权诉讼）；海外参展知识产权风险（如商标风险、参展产品的专利风险、参展材料或展台设计的版权风险）；跨境电商知识产权风险（因商标、专利、版权侵权投诉等被电商平台封号、冻结资金甚至诉讼）；海关扣押风险（海关对侵权嫌疑货物实施扣留并进行调查、罚款、追究刑事责任等）；知识产权相关的贸易风险（如美国的“337调查”、“特别301调查”以及欧盟针对相关不公平贸易措施的调查等）；跨境技术交易的知识产权风险（专利侵权或自身知识产权流失）。

  中国企业需要建立一套全球性的知识产权管理体系，同时加强海外知识产权应诉能力，积极维权，最大化地实现知识产权价值。

- **贸易管制与制裁**

  受当前国际政治经济环境影响，中国企业在出海贸易和投资方面，受到海外其他国家基于安全利益实施的管制、制裁的风险日益增加。以美国为例，违反出口管制相关法律，可能遭到行政处罚（如民事罚金、进出口禁令、禁止从事BIS相关业务等）以及刑事处罚。若触发刑事处罚程序，依据《美国出口管制条例》规定，任何故意实施、试图实施或密谋违反相关规定的主体，可能会被处以100万美元的罚款，涉案高管个人则有可能面临最高20年的监禁，二者可并处。中国企业出海的过程中，应遵守国际贸易规则，如国际条约、多边/双边协定、商业惯例、海外国家或地区的法律法规、监管规定、行业准则、平台规则等要求。

通过建立健全的合规体系，企业能够更有效地应对复杂多变的国际市场环境，保持业务的持续健康发展。接下来，我们将重点阐述数据合规的重要性、主要挑战、全球各地区的数据合规要求、以及数据合规体系建设。

数据合规的重要性 1.4

数据是每个组织的命脉。在全球化的过程中，随着中国企业国际市场的不断拓展和业务的深入发展，数据合规作为海外运营的核心支撑板块，成为了不可忽视的关键因素。

中国企业在出海过程中，数据合规的重要性主要体现在以下三个方面：

- **遵守当地的数据保护法规是企业合法合规经营的基础**

  中国出海企业已经进入双向监管合规时代，一方面国内企业要遵守《网络安全法》、《数据安全法》、《个人信息保护法》等中国法律法规，另一方面还要遵从目标国家的法律法规、行业监管要求和安全标准。各国在数据保护方面的法律规定各不相同，对企业的数据收集、存储、处理和传输提出了严格的要求。

  中国企业在国际化过程中必须深入理解并遵守各国的法规，以确保合规运营，避免因数据违规而面临法律风险或经济处罚。仅就罚款而言，违规企业可能面临当年全球年营业额的4%的巨额罚款。例如，某汽车新势力企业因违反欧盟隐私保护法律，被罚2亿欧元，影响了该企业的海外业务发展进程。

- **企业数据合规对于保护企业的声誉至关重要**

  数据泄露和违规行为不仅会导致巨额罚款，还会严重损害企业的品牌形象和市场信任度。海量的数据催生了许多数据安全管理问题，消费者的数据安全和用户的隐私保护工作愈发重要。全球消费者越来越重视个人数据的隐私和安全，企业必须以高度的责任感和透明度来管理和保护客户数据，以赢得和保持客户的信任。

  随着组织的数据足迹扩展至各种云服务提供商、SaaS（软件即服务）应用程序和端点，组织面临的数据泄漏风险也不断增加。黑客和网络罪犯试图利用安全漏洞来访问分布在多个云数据中心和数据存储区的敏感数据。例如，某快消品企业因侵犯员工隐私被处罚3500万欧元，面临长时间的监管调查，声誉严重受损。《2024年数据泄露成本报告》显示，2024年，全球数据泄露的平均成本再创新高，比2023年增加了10%，达到 488万美元[1]。

- **企业数据合规有助于提升企业的竞争力和运营效率**

  合规的数据管理实践可以帮助企业优化数据流程，提升数据质量和安全性，从而支持更精准的市场分析和业务决策。如果企业忽视隐私数据安全合规风险与挑战，监管机构有权力临时或永久限制或禁止违规企业的数据处理活动。例如，某短视频平台因隐私保护不足被处罚3.45亿欧元，多国对其展开调查或暂停其业务[2]。

  在复杂多变的国际政治经济形势之下，中国企业应当变被动为主动，积极融入全球合规治理体系，提升企业的合规竞争软实力，为实现高质量、可持续的全球化发展奠定坚实的基础。

[1] “Cost of a Data Breach Report 2024.” IBM Security and the Ponemon Institute. 202407. https://www.ibm.com/reports/data-breach

[2] 杜知航. “未做好未成年人保护 TikTok被欧盟罚款3.45亿欧元”. 20230917. https://m.caixin.com/m/2023-09-17/102104596.html

02

企业出海面临的数据合规挑战

全球法律法规的多样性

数据跨境传输的复杂性

数据合规策略的一致性

不同行业数据跨境的特殊性

全球法律法规的多样性 2.1

根据联合国贸易和发展会议（United Nations Conference on Trade and Development，UNCTAD）统计，到2023年，在全球230多个国家(地区)中，已经有161个国家(地区)出台了数据隐私保护法，其中大多数制定了跨境数据流动法律或政策[1]。各国对数据保护的法规和要求不同，主要包括限制性规范和推动性规范两类。限制性规范以限制数据流动、数据安全偏好为主要策略，如印度、俄罗斯在促进数字经济发展的同时，制定数据本地化的规定；新加坡、欧盟在提倡数据跨境自由流动的同时，规定多样化的数据出境机制。推动性规范以推动数据自由流动、数据红利偏好为主要策略，如经济合作与发展组织（OECD）、亚洲太平洋经济合作组织（APEC）等国际组织确立了若干数据跨境流动的原则，建立了若干具有代表性的框架，推动数据在国家/地区间有序流动，以期减少数据跨境流动摩擦，但对于数据向组织外的跨境则较为谨慎。欧洲的《通用数据保护条例》（GDPR）提供了目前唯一的对外跨境合规框架，并采取了世界范围内的持续性实质推广，对全球多个国家/地区的相关规则产生了显著影响。

在这些全球法规中，欧盟的《通用数据保护条例》（GDPR）号称是“史上最严个人数据保护立法”。从2018年正式实施到2023年11月，欧盟成员国根据GDPR针对与处理个人数据相关的违规行为发起了1701起罚款，罚款总额达到40亿欧元。根据欧盟对GDPR执法的总结和期望，未来GDPR的执法会越来越严格和频繁。我国的《个人信息保护法》自2021年11月1日正式实施，在规则的严厉程度上基本对标欧盟GDPR，而美国加州隐私立法（CCPA&CPRA）相较更为宽松。在适用地域范围上，GDPR最广泛，中国《个人信息保护法》更为克制，CCPA&CPRA最有限。在个人信息处理的合法性基础、同意规则、行政监管等方面，《个人信息保护法》比GDPR更严格，CCPA&CPRA最宽松。在个人信息定义、敏感信息处理规则等方面，《个人信息保护法》和GDPR严格程度基本一致，CCPA&CPRA最宽松。在受规制的对象类型、数据安全事件通知义务等方面，GDPR最严格《个人信息保护法》次之，CCPA&CPRA最宽松[2]。

另外，各国数据保护政策和法规可能会不断变化，企业需要保持高度敏感，及时调整合规策略，以应对政策变化带来的挑战。例如，美国的数据保护法规在2023年之前一直保持相对宽松，但在2023年后，开始逐步收紧。2023年10月25日，在瑞士举行的世界贸易组织电子商务联合声明倡议会议期间，美国放弃了长期以来坚持的部分关于跨境数据自由流动的主张，并且美国正在审查其在数据和源代码等敏感领域的贸易规则现行举措。2023年11月15日，14名美国国会议员联合签署信函，向10家在美国进行自动驾驶汽车测试的中国公司发出质询，要求他们就“如何收集和处理美国的数据、以及与中国政府关系”做出回应[3]。虽然拥有自动驾驶汽车的中国公司在加州仍然相对不受限制，但未来可能会越来越困难。现在是质询，紧接着就会正式审查。美国的一位国会众议员已经起草了众议院《国防授权法案》的修正案，要求国防部报告可能涉及中国自动驾驶汽车的国家安全威胁，该法案已获得众议院批准。

企业需要密切关注并遵守不同国家的法律法规及执法动态，一方面最大限度规避限制性规范的违规风险，另一方面充分利用推动性规范的弹性空间，降低企业跨境管控压力和成本。

---

[1] https://www.privacylaws.com/reports-gateway/articles/int181/int181_2023/

[2] 王融、易泓清.“中美欧个人信息保护法比较”. 腾讯研究院. 20210822. https://mp.weixin.qq.com/s/UhFcT1W9O9LKU2JJofToZw

[3] https://www.secrss.com/articles/61718

数据跨境传输的复杂性 2.2

数据跨境传输除了需要满足各地法律法规要求外，往往还面临“国家安全”、“数字主权”相伴而生的复杂地缘环境，各国围绕数据本地化的不同要求也进一步增加了企业的合规难度。

2.2.1 国家安全

“国家安全”日益成为相关国家限制数据跨境流动的动力。一方面，特定重要数据的确需要加以保护和管理，例如基因、地理、气象等敏感数据以及大量个人数据等，都存在构成国家安全风险的可能。但另一方面，“国家安全”的概念同样也是模糊且覆盖广泛的，一旦跟国家安全风险挂钩，数据“真正的用途”便不再被关注，一方面政府无需提出合理有效的证明，另一方面企业亦难以“自证清白”。美国对中国某短视频平台海外版的打压，其中一个理由就是怀疑其搜集的大量数据会交给中国政府、影响其国家安全；美国也以国家安全为由，出台了阻止外国实体获得大量美国人个人数据的行政令，禁止数据流向中国在内的所谓“受关注国家”。

2.2.2 数字主权

数字主权是国家主权在数字领域的延展。美国GAFA（谷歌、苹果、Facebook 和亚马逊）的全球扩张，加剧了价值转移的严重失衡，产生了数字领域的经济依赖，各国围绕数字经济发展的自主权的讨论开始增加。2013年斯诺登等事件的接连发生，也使得各国政府越发担忧由于跨境数据流动而失去对他国数字平台的控制，进而损害本国主权。数字主权的概念因此应运而生。

尽管数字主权的概念仍然广泛而模糊，但已得到不少国家认可或接受，并在各自国家内以不同的方式得到解释和应用，也反映了有关国家各自的价值观和政治偏好。比如，欧盟的“数字主权”具有较强的代表性和影响力，最早于2008年进入欧盟公共领域，并逐渐确认为“欧洲数字政策的主旋律”；由于欧盟在数字领域的发展落后于美国和中国，且更加注重保护基本的个人权利，其实现数字主权的路径和愿景会更加侧重于强化数字平台责任。中国的数字主权意味着将数据保护作为政府的核心和战略资产，重点在于安全。美国由于缺少联邦层面的数据保护法规，美国企业对数据具有更多的自主权。而其他发展中国家提到的数字主权，往往是上述不同概念的混合，特别是曾经做过殖民地的国家，更多是从对“数字殖民主义的反抗”角度出发理解数字主权。但与此同时，过度强调数字主权及其有关概念，反过来可能也会削弱国家在数字领域的国际吸引力、加深国际数字鸿沟，因此并不是没有反对意见。

2.2.3 数据本地化

数据本地化是数据跨境管理的一种措施，通常理解为某一主权国家和地区，通过制定法律或规则来限制本国和地区数据向境外流动，是对数据出境进行限制的做法之一。数据本地化不仅增加了企业的合规成本，还可能影响数据的流动性和企业的全球运营效率。

目前，全球多个国家和地区提出了本地化要求，宽严程度有所不同，几种模式交织并行：

模式1：无本地化要求，但有出境限制。比如，日本和欧盟规定原则上允许数据合规流动。

模式2：境内存储副本，对转移或出境无限制。比如，印度仅要求将数据副本存储在国内计算机设备中，对外转移或处理数据副本无限制，其通常的目的是确保监管需求。

模式3：境内存储，可境外处理。比如，俄罗斯规定数据必须首次存储在国内，满足出境合规条件的情况下可以向境外传输，在境外处理数据。

模式4：境内存储、处理。比如，美国、土耳其、澳大利亚规定数据只能在境内存储、处理，仅在特定的条件下（如国家安全需求）的情况下，经审批出境。

数据合规策略的一致性 2.3

出海企业在全球化的商业环境中，面临着复杂的数据保护和隐私法规挑战。为了在各个国家和地区顺利开展业务，企业必须与当地的监管机构、合作伙伴以及供应商等多方进行深入的沟通和协调。这种协调不仅涉及到对各国数据保护法规的理解和遵守，及时了解和适应法规变化，降低因违反法规而面临的企业声誉风险、法律风险和罚款；还需要基于对各国法规的理解，制定一套统一的数据合规策略，明确数据收集、存储、处理和传输等方面的操作规范，确保在全球范围内的数据处理活动都能遵守相关法规。

通过协调一致的数据合规策略，企业可以确保与各方合作伙伴和供应商的合作更加顺畅，避免因数据问题影响合作关系。同时，数据合规策略的一致性有助于企业在全球市场中做出更明智的战略决策，确保企业的长期可持续发展。

不同行业数据跨境的特殊性 2.4

除了以上各行业均面临的共性挑战之外，不同的行业在数据跨境时都面临着不同的挑战。

这主要受到行业特性、法律法规、数据敏感度、业务模式和国际合作等多方面因素的影响。例如：

- **金融行业**：金融数据通常涉及个人隐私和财务信息，因此对数据保护要求极高。跨境数据传输需要符合严格的金融监管要求，如欧盟的GDPR、美国的ADPPA和CCPA。
- **医疗行业**：医疗数据包含敏感的个人健康信息，需要遵守HIPAA等健康信息保护法规。跨境数据传输需要确保数据的安全性和隐私性，避免泄露给未授权的第三方。
- **工业制造业**：工业制造业数据可能包含商业秘密和知识产权信息，对数据保护有特别要求。跨境数据传输需考虑供应链管理和国际合作的需要。
- **信息技术行业**：IT行业数据跨境涉及大量的用户数据和网络流量，需要高度的数据安全和隐私保护。跨境数据传输需遵守各国的数据保护法规，如欧盟的GDPR。
- **媒体和娱乐行业**：媒体数据跨境可能涉及版权问题，需要确保内容的合法传播。跨境数据传输需考虑不同国家对媒体内容的审查和监管政策。
- **电子商务**：电商数据跨境涉及消费者个人信息和交易数据，需要保护消费者隐私。跨境数据传输需考虑税务、关税和消费者权益保护等问题。
- **出行行业**：出行行业包括航空、铁路、公路、水路等交通方式，涉及大量的乘客信息、行程数据和支付信息等敏感信息，需要出行企业采取特殊的保护措施。跨境数据需要确保数据存储在安全的服务器上，并需要实施严格的访问控制措施。
- **汽车行业**：汽车行业涉及车辆数据、位置数据、个人信息、供应链数据，需要实施严格的访问控制，防止数据泄露、篡改和丢失。跨境数据传输需要使用安全的传输协议，以及确保数据存储的安全，定期进行审计，实时监控数据访问和传输活动。
- **消费电子行业**：消费电子行业主要涉及用户数据、设备数据、位置数据、供应链数据等，需要采取特殊的保护措施，以确保数据安全和合规。跨境数据传输时，需要采用安全的加密算法和传输协议，并需要定期备份跨境数据，确保数据安全。
- **能源行业**：能源数据跨境可能涉及关键基础设施和国家安全，对数据的控制非常严格。跨境数据传输需符合国际能源合作和安全协议。

每个行业在数据跨境时都需要考虑其特殊性，并制定相应的数据管理和保护策略，以确保合规性、安全性和业务的连续性。

总之，中国企业在出海过程中需要全面了解和遵守各国的数据保护法规，建立完善的数据合规体系，并通过技术和管理措施确保数据的安全和合规性。同时，企业还需要密切关注政策变化和执法动态，及时调整合规策略，以应对不断变化的国际数据保护环境。

03

各国家地区数据合规法规概览

欧盟

北美

拉丁美洲

中东地区

东南亚

印度

俄罗斯

日韩

非洲

大洋洲

中国

欧盟 3.1

3.1.1 欧盟GDPR法规要求概述

《通用数据保护条例》（General Data Protection Regulation， GDPR）于2018年5月25日正式生效，是20多年来数据保护/数据隐私领域的最大的变革。在GDPR出台之前，每个欧盟成员国都有着各自的数据保护法，这些法律都源于1995年的欧盟数据保护指令（95指令）。95指令只规定了数据保护的最低标准，由于每个欧盟成员国在实施时都采取了不同的方法，导致当时的欧盟实际上拥有20多部不同的数据保护法。GDPR的出台，统一了欧盟各成员国分散的立法现状。

在GDPR颁布之后，其它国家和地区也陆续颁布了数据隐私或数据安全方面的法律法规，可以说，GPDR的影响力是全球性的。

GDPR共有99条规定，它授予个人更多的权利，加大了个人数据的保护力度，也顺应了欧盟消费者对数据隐私安全的迫切需求。具体而言，GDPR的出台：

- 定义了法律允许的个人数据的传输和处理方式。
- 详细说明了组织保护静态和传输中个人数据的具体方式。
- 确立了欧盟居民对个人数据的收集、使用和拥有的权利。

GDPR定义的三种角色

为了清晰阐述权利、责任与义务，GDPR定义了三种角色：

- **数据主体**：个人数据的所有者。例如，如果一家公司收集电子邮件地址，那么这些电子邮件地址的所有者就是数据主体。
- **数据控制者**：收集个人数据并确定其使用方式的任何组织、公共机构或其他团体或个人。例如，保留用户数据库的社交媒体网站就是数据控制者。
- **数据处理者**：以某种方式对个人数据进行操作（例如分析、存储或更改数据）的任何组织。公司既可以是控制者，也可以是处理者。处理者也可以是代表控制者处理数据的第三方机构，如提供数据存储和分析的云服务提供商。

GDPR的适用范围

GDPR的适用范围极广，所有位于欧洲经济区（包括27个欧盟成员国以及冰岛、列支敦士登和挪威）的数据控制者和处理者都受到GDPR的约束（即使是在欧盟之外存储和处理数据）。

如果存在以下几种情况，欧洲经济区以外的企业也将受到GDPR的约束：

- 公司定期向欧洲经济区居民提供商品和服务，即使没有资金易手。
- 公司定期监控欧洲经济区居民的活动，例如使用跟踪cookie。
- 公司代表欧洲经济区的控制者处理数据。

唯一不受GDPR约束的数据处理活动是国家安全或执法活动以及纯粹的个人数据使用。

GDPR较广的适用范围也会对中国企业的移动应用安全、数据收集、处理和交易产生重大影响。例如，一家中国的互联网公司在中国境内为欧盟数据主体提供服务，其收集的有关个人数据，也应当遵循GDPR相关要求。

GDPR的七项基本原则

GDPR制定了七项核心原则作为法律基础。这些原则与合法性、数据处理原因以及同意条件相关，包括：

- **合法性、公平性与透明性**：企业须告知数据主体其个人数据的使用方式，必须有正当理由才能处理数据。
- **用途限制**：企业只能出于特定目的收集数据，这是有意纳入隐私原则中的一项重要概念，其重点在于确保数据“被收集用于指定的、明确的且合法的目的”。
- **数据最小化**：企业收集数据的范围不得超出其特定处理需求的范围。
- **准确性与及时更新**：收集并处理数据的企业应及时更新数据，确保数据准确，还必须应数据主体的要求更改或删除数据。
- **存储限制**：企业保留收集数据的期限不得超过所需时长。
- **完整性和保密性**：企业必须采取适当的安全保护措施，保护个人数据，以避免数据被盗/未经授权访问等。
- **合规性**：措施和文档必须证明受管辖实体已遵循GDPR规定。

GDPR赋予数据主体的八项主要权利

GDPR第3章定义了数据主体拥有的八项权利，包括：

- **知情权**：数据主体有权知道谁拥有其数据、他们获得这些数据的方式以及正在使用这些数据做什么。
- **访问权**：数据主体有权访问公司拥有的任何数据。
- **纠正权**：数据主体有权更正不准确或过时的个人数据。
- **删除权**：也即“被遗忘权”，指主体有权要求公司删除其数据。公司必须遵守，除非他们对数据的权益（例如，维护某些记录的法律义务）超越了这项权利。
- **限制处理权**：如果主体认为其数据不准确、遭到非法使用或不再需要用于公司目的，他们可以要求公司限制其数据的使用方式。公司必须遵守，除非能够证明其在处理数据方面拥有压倒性的权益。
- **数据携带权**：数据主体有权将其数据从一家公司转移到另一家公司。公司必须通过以可共享格式存储数据，或根据主体的请求将其发送给第三方来促进个人数据的传输。
- **拒绝权**：数据主体可以随时拒绝处理其数据。除非公司能够证明自己有压倒一切的合法理由，否则必须停止处理。
- **不受自动化决策限制的权利**：数据主体不受基于自动化处理行为得出的决定的制约，例如预测他们的工作表现或网页浏览行为。未经受影响人员同意，公司不能使用自动化处理制定重大决策。数据主体有权对仅基于自动化处理做出的决定提出异议。他们可以对决策提出意见，并要求公司任命一名员工来核查决策。

GDPR规定数据控制者/处理者的主要义务

GDPR规定了控制者和处理者在处理个人数据时必须遵守的责任和义务：

- **信息透明**：数据控制者/处理者在收集个人数据前务必征询数据主体，如应以简单透明、清晰且容易获取的方式，通过清楚明确的语言向数据主体提供相关信息。
- **设计和默认的数据保护**：设计隐私和默认隐私必须在项目、产品或服务的所有阶段实施。控制者应当实施适当的技术和组织措施保护数据主体的权利，如匿名化等。且对特定事项，该技术和组织措施应确保在默认情况下只有对每个特定处理目的有必要的个人数据才能被处理。
- **活动记录**：控制者及其代表应当依职责保存处理活动的记录，且记录应当包含特定信息，如处理者/控制者的联系方式、处理目的、数据主体类别等。
- **泄露通知**：在个人数据泄露的情况下，控制者在知悉后应及时且最迟在72小时内通知监管机构。
- **影响评估**：在进行数据处理之前，控制者应当就个人数据保护所设想的处理操作方式的影响进行评估。
- **提前咨询**：根据影响评估情况，如果控制者不采取措施，处理会带来高风险，那么控制者应当在处理之前咨询监管机构。
- **设立数据保护官**：控制者和处理者需要指派专门的数据保护官（Data Protection Officer，DPO）负责降低数据风险，确保数据合规，响应请求，报告违规，并创建良好的数据安全策略。

3.1.2 欧盟GDPR法规重点梳理

监管机构

根据欧盟GDPR的规定，欧盟成员国中每个国家都应当设置相应的数据监管机构（如数据保护委员会或数据保护局），以对本国内部的个人数据处理活动进行有效监管，并与其他成员国之间的数据处理活动进行协调。欧盟数据保护委员会（EDPB）会由各成员国的监管机构代表或者首长联合组成，以进一步促进协调。

数据跨境

GDPR规定了欧盟个人数据跨境的三种途径：

- **获得“充分性认定”**
  当欧盟委员会决定第三方已经确定达到充分的保护标准时，数据便可以向第三方转移，而无需经过任何特别授权程序（第三方白名单国家）。由于欧盟的充分性认定较为全面与严格，自瑞士成为首个获得充分性认定的第三方以来，20余年间仅有15个第三方通过欧盟的充分性认定，分别是：瑞士、英国、美国（仅限已加入欧美隐私框架的商业组织）、加拿大（仅限商业组织）、日本、韩国、安道尔、阿根廷、法罗群岛、根西岛、以色列、曼岛、泽西岛、新西兰、乌拉圭。
- **为欧盟境内数据主体提供“适当保障措施”**
  当数据出境的目的地没有获得欧盟的充分性认定时，数据控制者或处理者只有在提供了适当的保障措施并且满足数据主体能行使权利、能获得有效的法律救济的条件时，欧盟境内主体才能将相关个人数据向第三国或国际组织转移。这些保障措施包括：政府间签订有法律约束力和可执行性的文书、有约束力的公司规则、采纳欧盟提供的标准合同条款等。
- **特定情况下的豁免**
  在充分性认定和适当保障措施均不能满足的情况下，数据跨境需求方还可以退而求其次，判断其数据跨境传输是否属于特定情况下的豁免，GDPR规定了7种豁免情形，如数据主体在被告知该转移行为由于缺乏充分的保护标准和适当的保护措施可能会对其带来的风险后仍明确同意转移。

数据本地存储

GDPR没有规定数据必须存储在本地，但对数据跨境有严格要求。此外，对于金融、医疗、政府业务等行业，还需要遵从欧盟各所在国的规定。

个人数据保护

GDPR非常重视个人数据保护。GDPR将**个人数据**定义为与可识别人员相关的任何信息，包括直接和间接标识符。直接标识符是指一个人的唯一数据点，例如姓名或信用卡号。间接标识符包括可以识别一个人的非独特特征，例如Cookie标识符、IP地址、外形特征、出生日期等。

GDPR还对**敏感个人数据**给予更大保护力度，包括以下信息：族裔或种族、宗教信仰、生物识别数据、政治观点、遗传数据、健康信息、性取向或性生活、工会会员身份。敏感数据需要接受更为严格的保护，是因为对这些数据的处理会大大增加个人权利和自由方面所面临风险的可能性和严重性。

根据GDPR的规定，只有满足如下条件中的至少一项，对于个人敏感数据的处理才是合法的：

- 数据主体已经明确同意基于一项或多项目的而对其个人数据进行处理。
- 处理对于控制者履行责任以及行使其特定权利是必要的，或者对于在雇佣、社会安全与社会保障法领域采取符合欧盟或成员国法律或集体协议的措施以保护数据主体的根本权利或利益是必要的。
- 数据主体因身体原因或法律原因而无法表达同意，但处理对于保护数据主体或另一个自然人的核心利益所必要的。
- 基金、协会或者其它具有政治、哲学、宗教或工会目的的非营利机构的正当性活动中所进行的处理，并且已经采取了恰当的保护措施。
- 对数据主体明显已经公开的相关个人数据的处理。
- 当处理对于提起、行使或辩护法律性主张必要。
- 处理对实现实质性的公共利益是必要的。
- 处理对于预防性医学或者临床医学目的是必要的。
- 在公共健康领域，处理是为了实现公共利益所必要的。
- 对于实现公共利益、科学或历史研究目的或统计目的是必要的，处理采取了与其期望目的所相称的处理，并且对数据主体的基本权利与利益采取了合适与特定的措施。

3.1.3 欧盟GDPR数据违规案例

因违反GDPR而产生的罚款有以下两个级别：

- **1级：**轻微违规行为（例如未经父母同意，处理16岁以下儿童的数据），处以全球年收入的2%或1000万欧元的罚款，以较高者为准。
- **2级：**重大侵权行为（例如出于非法目的处理数据），处以全球年收入的4%或 2000万欧元的罚款，以较高者为准。

GDPR的实施将加重中国企业及跨国公司涉欧业务的合规义务。所有在欧盟有业务的中国公司，无论是在欧盟内部还是在欧盟之外处理个人数据，或者是在欧盟以外处理欧盟居民的个人数据，都面临风险。GDPR的监管要求覆盖了各个行业，根据GDPR Enforcement Tracker 统计的罚款情况，以下行业的公司面临的风险最大：

- 媒体、通信和广播行业
- 银行、保险公司、咨询
- 工业企业
- 零售电商平台
- 将个人数据用于营销目的的航空公司和酒店连锁
- 房地产开发商

根据GDPR Enforcement Tracker 的分析[1]，罚款原因中位列前三的原因如下：

- 违反通用数据处理原则。
- 数据处理的法律依据不足。
- 缺乏用于确保信息安全的技术和企业措施。

2023年5月，因违反GDPR，爱尔兰数据保护委员会向美国某社交平台开出了12亿欧元（即13亿美元）的罚单，高居近期大额制裁榜首。关于GDPR第46(1)条，爱尔兰隐私监管机构指责该公司在提供服务时，未能在将个人数据从欧盟或欧洲经济区（EEA）转移到美国的过程中提供足够的数据隐私保护[2]。

2021年7月，荷兰数据保护局（Autoriteit　Persoonsgegevens）以侵犯儿童隐私为由，决定对中国某出海社交平台处以75万欧元的罚款。这是GDPR实施三年以来，中国企业第一次因违反GDPR相关条款而遭受处罚[3]。 2023年9月15日，爱尔兰数据保护委员会称该社交平台违反GDPR多条规则，再次对其罚款3.45亿欧元[4]。 2024年3月14日，意大利竞争管理局认为，该社交平台的内容审核不到位，尤其是可能威胁到未成年人和弱势群体的内容，分别处罚该社交平台爱尔兰有限公司、英国有限公司、法国有限公司一千万欧元[5]。

---

[1]GDPR Enforcement Tracker fines statistics: https://www.enforcementtracker.com/?insights

[2]Shweta Sharma.“迄今为止最大的数据泄露罚款、处罚和和解”. 20240428. http://www.d1net.com/security/news/581076.html

[3]“欧盟数据保护(GDPR)动态：中国企业首次被罚”. 20210724. https://www.dehenglaw.com/CN/tansuocontent/0008/022088/7.aspx?MID=0902

[4]杜知航.“未做好未成年人保护 TikTok被欧盟罚款3.45亿欧元”. 财新. 20230917. https://m.caixin.com/m/2023-09-17/102104596.html

[5]肖潇.“再被意大利罚款一千万，TikTok为何总被欧洲监管针对？”.21财经.20240318.https://m.21jingji.com/article/20240318/herald/f875b7fafdb7c64dcce30c26839fc49a.html

3.1.4 欧盟网络安全法规要求

随着网络和信息系统以及电子通信网络和服务逐渐成为欧盟经济增长的支柱，欧盟陆续出台了多项政策，搭建了一套较为完善的关键基础网络安全防护法律体系，实行以风险管理为基础的网络安全治理策略。

欧盟《网络安全法案》（CSA）

欧盟《网络安全法案》（EU Cybersecurity Act，CSA）于2019年6月27日正式施行[1]。该法案设立的目的是确保欧盟机构在处理个人用户、组织和企业网络安全问题的过程中加强网络安全结构、增强对数字技术的掌控、确保网络安全应当遵守的法律规制，旨在促进卫生、能源、金融和运输等关键部门的经济，特别是促进内部市场的运作。

为了实现这一目标，该法案包括两个主要部分：

- 建立欧盟网络和信息安全局（European Network and Information Security Agency，ENISA）管理的监管框架，旨在为各种信息和通信技术 (ICT) 产品和服务制定认证计划。
- 授权欧盟委员会建立一个自愿的网络安全认证机制。随着时间的推移，可能会成为欧盟对关键产品或活动的强制性认证。

在网络风险不断增加的形势下，《欧盟网络安全法案》一方面将把欧盟网络和信息安全署（ENISA）定位成欧盟永久性机构，从而提升加强ENISA的地位；另一方面，还为信息和通讯技术（ICT）等产品创建了一个欧洲网络安全认证框架，旨在欧盟内部提供网络韧性和响应能力，因为协调各种标准以提升效率也是欧盟“数字单一市场”（Digital Single Market）战略的核心命题。

设计、制造或实施ICT产品、服务或流程的企业应监控相关认证计划，评估其合规程度，并在计划正式采用后考虑认证。虽然《网络安全法案》的真正影响和有效性还有待观察，但它对网络安全的日益关注可能会促进 ENISA 认证计划的成功和广泛采用。

欧盟NIS 2指令

2022年12月，欧洲议会和理事会共同通过了《关于在整个欧盟全境实现高度统一网络安全措施的指令》（NIS 2指令），其目标是在欧盟各成员国之间建立统一的网络安全水平[2]。

NIS 2指令作为欧盟关键基础网络安全防护的核心法规，构建了一套基于分级分类原则的网络安全防护体系。NIS 2适用于欧盟范围内的任何公司，包括“在内部市场中，作为一个整体在经济和社会方面履行重要职责的公有和私有实体”，并且这些公司“应按要求采取充分的网络安全措施”。

该指令将“受监管实体”分为两类：必要实体 (Essential Entities，EE) 和重要实体(Important Entities，IE)。这两类实体在合规方面的区别在于：必要实体在合规监控、事件报告义务和信息系统保护措施执行方面须遵循更为严格的监管要求。

- NIS 2规定的**必要实体**包括：能源、健康、交通、饮用水、废水、空间、公共政府、信息通信技术服务管理（B2B商家对商家）、金融市场基础设施、银行业、数字基础设施（包括互联网服务提供商ISP和云）等。
- NIS 2规定的**重要实体**包括：数字供应商、研究、邮政和快递服务、食品生产与分销、制造业、化学品制造生产和分销、废弃物管理等。

未遵循NIS 2的要求会被处以巨额罚款：

- **必要实体**：最高1000万欧元或全球年营业额的2%，以金额较高者为准。
- **重要实体**：最高700万欧元或全球年营业额的1.4%，以金额较高者为准。

[1]https://eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html
[2]https://eur-lex.europa.eu/eli/dir/2022/2555

▶ 欧盟CER指令

欧盟《关于关键设施弹性的指令》（the Critical Entities Resilience Directive， CER）于2022 年12月27日生效[1]，该指令明确了欧盟地区的关键基础设施涉及的11个领域(能源、交通、银行、金融市场基础设施、卫生、饮用水、废水、数字基础设施、公共行政、空间、食品)，并明确识别关键基础实体的考虑因素和安全义务，如：

- 风险评估。
- 弹性措施。
- 强制性背景调查。
- 事件通知要求。
- 现场检查/审核。

CER和NIS 2指令下的国家主管部门必须定期合作和交换相关信息，如网络和非网络风险、威胁和事件等。

▶ 欧盟《网络弹性法案》（CRA）

《网络弹性法案》（Cyber Resilience Act，CRA）是即将出台的欧盟法规，旨在确保在欧盟销售的所有数字产品和服务都采用强大的网络安全措施[2]。2022年9月，欧盟委员会发布了《网络弹性法案》（CRA）草案。欧洲议会于2024年3月12日通过了CRA最终文本的临时版本。该法案要求数字产品制造商在整个产品生命周期内确保其安全，并提供自动安全更新服务。未来的产品必须符合最低安全要求，以获得CE标志。CRA涉及整个开发过程中的访问保护、保密性、完整性和可用性等基本层面。

▶ 欧盟针对金融行业的合规要求

《数字运营弹性法案》（Digital Operational Resilience Act，DORA）旨在为欧盟金融行业（Financial Entities）创建具有约束力的全面信息和通信技术（ICT）风险管理框架[3]。该法案于2022年12月通过，并将于2025年1月17日生效。

DORA有两个主要目标：

- 全面解决金融服务行业的ICT风险管理问题。
- 协调各个欧盟成员国已有的ICT风险管理法规。

DORA适用于欧盟的所有金融机构。其中包括银行、投资企业和信贷机构等传统金融实体，以及加密资产服务提供商和众筹平台等非传统实体。此外，DORA还适用于一些通常被排除在金融监管之外的实体。例如，为金融公司提供ICT系统和服务的第三方服务提供商（例如云服务提供商和数据中心）必须遵守DORA的要求。DORA还涵盖提供关键第三方信息服务的公司，例如信用评级服务和数据分析提供商。

DORA在四个领域为金融实体和ICT提供商制定了技术要求：

- ICT风险管理和治理。
- 事件响应和报告。
- 数字化运营弹性测试。
- 第三方风险管理。

DORA鼓励但不要求信息共享。金融实体必须建立从内部和外部ICT相关事件中吸取教训的流程。为此，DORA鼓励实体参与自愿的威胁情报共享安排。以这种方式共享的任何信息仍必须受到相关准则的保护，例如，个人身份信息仍受《通用数据保护条例》（GDPR）的注意事项的约束。

---

[1]https://eur-lex.europa.eu/eli/dir/2022/2557/oj

[2]https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html

[3]https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

北美 3.2

3.2.1 美国

美国法规要求概述

美国联邦级的数据合规法规主要有以下2个：

- **《通用数据保护条例》（GDPR）**：虽然GDPR的原则和要求主要针对欧盟设计，但通常也适用于美国的数据处理。在美国，没有等同于GDPR的联邦法律。许多美国公司，尤其是那些在全球运营的公司，可能会选择采用类似GDPR的做法，以确保遵守欧盟数据保护法规。
- **《联邦贸易委员会》（FTC）法案**：FTC法案是一项联邦法律，授予联邦政府的独立机构联邦贸易委员会在该国监管和执行消费者保护和反垄断法的权力。其中规范了个人数据的收集、使用和披露，并要求公司采取合理措施保护消费者数据。并对未能采取合理措施保护消费者数据，导致数据安全漏洞的公司采取行动[1]。

另外，美国各州有权独立制定隐私法规，而以《加州隐私权法案》（CPRA）为代表。CPRA于2023年1月1日生效，自2023年7月1日起执行，是对2018年6月28日颁布的《加州消费者隐私法案》（CCPA）的修订和扩展，旨在保护加州消费者的隐私。

美国法规重点梳理

监管机构

《联邦贸易委员会》（FTC）法案的监管机构是美国联邦贸易委员会（Federal Trade Commission，FTC）。FTC是美国政府的一个独立机构，成立于1914年，最初的目的是防止垄断和促进竞争。随着时间的推移，FTC的职责和权力不断扩大，今天已成为美国政府的重要机构之一。FTC的主要职责包括：保护消费者免受欺诈和不公平的商业行为，促进竞争和防止垄断，监管商业广告和营销活动，监管数据保护和隐私，监管金融服务和信用报告。

加州隐私权法案（CPRA）的监管机构是加州隐私保护局（California Privacy Protection Agency，CPPA）。该机构成立于2021年，负责执行CPRA的规定。CPPA由五名成员组成，成员由加州州长任命，并经加州参议院确认。CPPA的主要职责包括：执行CPRA的规定，调查消费者投诉，对违反CPRA的企业进行处罚，向消费者提供教育和资源，与其他政府机构合作。CPPA的权利包括：调查企业的数据处理活动，发布命令和规定，对违反CPRA的企业进行处罚，向法院提起诉讼，与其他政府机构合作。

数据跨境

美国联邦贸易委员会（FTC）法案和加州隐私权法案（CPRA）对数据出境提出了相同的要求，旨在保护消费者的个人数据隐私。这些要求包括：

- 数据在传输过程中必须加密。
- 数据在存储过程中必须加密。
- 必须采取访问控制措施，限制对数据的访问。
- 必须采取监控措施，检测和响应安全事件。
- 消费者必须被告知他们的数据将被传输到国外。
- 消费者必须被告知数据传输的目的和范围。
- 消费者必须给予明确的同意，才能传输他们的数据。
- 数据控制者必须与数据处理者签订合同，规定数据处理者的义务和责任。
- 合同必须包括数据保护的条款，包括安全措施、知情同意和监控措施。
- FTC有权监控和执行数据出境的要求。
- FTC有权调查和处罚违反数据出境要求的行为。

同时，FTC法案和CPRA法案也都规定了一些例外，在某些情况下，数据出境的要求可能被豁免，例如在紧急情况下或根据法律要求。

[1]https://www.ftc.gov/enforcement

另外，美国与其他国家签订了多项国际协定，规定数据出境的要求和标准，包括欧盟-美国隐私盾框架和亚太经济合作组织（APEC）跨境隐私规则（CBPR）。多个行业组织也制定了数据出境的标准和指南，包括支付卡行业数据安全标准（PCI DSS）和国际标准化组织（ISO）27001。企业也应采取多种措施来确保数据出境的安全和合规，包括实施安全措施、知情同意和监控措施，签订合同，并遵守相关法案、国际协定和行业标准。

数据本地存储

美国联邦贸易委员会（FTC）法案和加州隐私权法案（CPRA）都对数据本地存储有特定的要求，旨在保护消费者的个人数据隐私。

- 首先，前者要求数据控制者必须将个人数据存储在美国境内或符合FTC标准的国家，后者要求数据控制者必须将个人数据存储在加州境内或美国境内。
- 另外，这两项法案都要求：
  - 数据控制者必须确保数据存储的安全和保密。
  - 数据控制者必须对数据存储进行监控和审计。
  - 数据控制者必须采取适当的安全措施来保护数据存储的安全。
  - 数据控制者必须对数据存储进行加密。
  - 数据控制者必须对数据存储进行访问控制。
  - 数据控制者必须与数据存储服务提供商签订合同，规定数据存储的义务和责任，合同必须包括数据保护的条款，包括安全措施、保密性和监控措施。
  - FTC和CPPA均有权监控和执行数据本地存储的要求，以及有权调查和处罚违反数据本地存储要求的行为。

另外，这两项法案都规定了在某些情况下，例如在紧急情况下或根据法律要求，数据本地存储的要求可能被豁免。

个人数据保护

美国联邦贸易委员会（FTC）法案和加州隐私权法案（CPRA）对个人数据保护均有特定的要求，旨在保护消费者的个人数据隐私。这些要求包括：

- 企业必须向消费者披露他们所收集的个人数据的类型和用途。
- 消费者有权选择是否允许企业收集和使用他们的个人数据。
- 消费者有权访问和更正他们的个人数据。
- 企业必须采取适当的安全措施来保护个人数据。
- 企业必须对个人数据的保护负责。
- 企业只能收集必要的个人数据。
- 企业必须确定个人数据的保留期限。
- 企业必须确保个人数据的传输安全。
- 企业必须确保个人数据的存储安全。
- 企业必须控制个人数据的访问。
- 企业必须在合同中包括个人数据保护条款。
- 企业必须确定数据保护义务。
- 企业必须确定违约责任。

▶ 美国数据违规案例

2017年，美国某信用报告机构的安全团队发现了一个安全漏洞，黑客利用该漏洞进入了该机构的系统。黑客在系统中逗留了数月，窃取了大量客户数据，包括姓名、地址、出生日期、社会保障号码和驾驶执照号码等。经调查发现，该机构的安全措施存在严重缺陷，导致黑客能够轻易进入系统。

此次事件的具体原因包括：该机构未能及时更新其系统的安全补丁，导致安全漏洞未被修复；未能采取适当的密码管理措施，导致黑客能够轻易猜测密码；未能采取适当的监控措施，导致黑客能够长时间地访问系统而不被发现。

该数据泄露事件导致了1.47亿客户数据被泄露，包括姓名、地址、出生日期、社会保障号码和驾驶执照号码等。该机构声誉受到了严重损害，导致客户对公司的信任度下降。该机构面临了大量的法律诉讼和监管调查，导致公司的财务状况受到了严重影响。该机构在发现数据泄露事件后，立即采取了以下措施：通知受影响的客户，并提供相应的支持和帮助。与监管机构合作，进行调查和处理。采取措施来修复安全漏洞，并加强安全措施。提供免费的信用监控服务，以帮助客户保护其信用信息。此次数据泄露事件表明，数据保护是企业运营中的重要环节，企业必须采取适当措施来保护客户数据，否则可能面临法律和声誉风险。同时，企业必须及时更新其系统的安全补丁，采取适当的密码管理措施和监控措施，以防止黑客攻击。

3.2.2 加拿大

加拿大法规要求概述

加拿大联邦级的数据合规法规主要有个人信息保护和电子文档法（Personal Information Protection and Electronic Documents Act，PIPEDA），于2001年生效，这是加拿大联邦政府的一项法规，规范了商业组织如何收集、使用和披露个人信息。PIPEDA适用于所有在加拿大运营的商业组织，包括联邦政府机构、银行和金融机构、保险公司、电信公司、航空公司、医院和医疗机构、教育机构[1]。

PIPEDA的主要原则有10条：

- 商业组织负责保护个人信息，并确保其员工和代理人遵守该法规。
- 商业组织必须明确说明收集个人信息的目的，并确保该目的是合法和合理的。
- 商业组织必须获得个人信息主体的知情同意，才能收集、使用和披露其个人信息。
- 商业组织只能收集必要的个人信息，并确保该信息是最新的和准确的。
- 商业组织只能使用和披露个人信息用于指定的目的，并确保该信息是保密和安全的。
- 商业组织必须确保个人信息是准确和最新的。
- 商业组织必须采取合理措施保护个人信息免受未经授权的访问、使用和披露。
- 商业组织必须明确说明其个人信息保护政策和做法。
- 个人信息主体有权访问其个人信息，并要求更正或删除不准确或不完整的信息。
- 商业组织必须建立纠纷解决机制，以解决个人信息主体的投诉和问题。

除此之外，加拿大的各个省份也都有自己的个人信息保护法，例如：安大略省的《个人信息保护法》（Freedom of Information and Protection of Privacy Act，FIPPA），不列颠哥伦比亚省的《个人信息保护法》（Personal Information Protection Act，PIPA），魁北克省的《个人信息保护法》（Act Respecting the Protection of Personal Information in the Private Sector，P-39.1）。

另外，加拿大针对一些行业也制定了个人信息和数据安全法规，例如：加拿大支付卡行业数据安全标准（Payment Card Industry Data Security Standard， PCI DSS）规范了支付卡行业的数据安全要求。加拿大健康信息法（Personal Health Information Protection Act，PHIPA）规范了健康信息的收集、使用和披露。加拿大银行法（Bank Act）规范了金融机构如何处理个人信息。

加拿大法规重点梳理

监管机构

PIPEDA的监管机构是加拿大隐私委员会（Office of the Privacy Commissioner of Canada，OPC），成立于1983年，独立于政府，直接向议会报告。2001年，OPC的职责扩展到监管和执行PIPEDA，保护加拿大公民的个人信息和隐私权，促进隐私保护和个人信息保护。主要职责包括：

- 监管和执行PIPEDA，确保组织遵守PIPEDA的规定，保护个人信息和隐私权。
- 调查个人信息和隐私权相关的投诉，并采取适当的措施。
- 为组织和个人提供关于PIPEDA和隐私保护的指导和教育。
- 审查组织的隐私政策和做法，确保它们符合PIPEDA的要求。
- 发布关于隐私保护和PIPEDA执行的报告和建议。
- 与其他机构合作，促进隐私保护和个人信息保护。
- 为政府和其他机构提供关于隐私保护的建议和指导。
- 监测和分析隐私趋势和风险，确保OPC的工作始终与隐私保护的最新发展保持一致。

[1]https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

数据跨境

PIPEDA关于数据出境的要求主要有7项，旨在确保个人信息的安全和隐私。组织在数据出境时必须采取适当的措施和遵守相关的规定：

- 组织必须确保在数据出境时采取适当的安全措施，以保护个人信息的安全和隐私。
- 组织必须获得个人同意，才能将个人信息传输到加拿大境外。
- 组织必须向个人披露个人信息将被传输到加拿大境外，以及传输的目的和范围。
- 组织必须确保数据出境的目的合法，并且符合PIPEDA的要求。
- 组织必须与数据接收方签订合同，确保数据接收方遵守PIPEDA的要求，并且保护个人信息的安全和隐私。
- 组织必须监测和控制数据出境，确保数据出境的安全和合法性。
- 组织必须遵守跨境数据传输协议，例如欧盟的《通用数据保护条例》（GDPR）等。

数据本地存储

PIPEDA没有明确要求组织必须在加拿大境内存储所有个人信息。根据PIPEDA的规定，组织可以将个人信息传输到加拿大境外，但必须确保个人信息的安全和隐私，并且遵守相关的规定和标准。PIPEDA的重点是确保个人信息的安全和隐私，而不是要求组织必须在加拿大境内存储所有个人信息。组织可以根据自己的业务需要和风险评估来决定是否将个人信息传输到境外，但必须确保遵守相关的规定和标准，包括：

- 组织必须确保数据中心的安全，包括物理安全和网络安全。
- 组织必须遵守数据存储的标准，包括数据加密、访问控制和数据备份等。
- 组织必须确保数据的可用性，包括数据的完整性和可恢复性。
- 组织必须遵守数据保留的要求，包括数据的保留期限和删除要求等。
- 组织必须确保数据的机密性，包括数据的加密和访问控制等。
- 组织必须遵守数据审计的要求，包括数据的审计日志和审计报告等。

个人数据保护

PIPEDA对个人数据保护的要求是为了确保个人信息的安全和隐私，并且促进组织负责任地处理个人信息。主要有以下10项原则：

- 组织只能收集必要的个人信息，并且必须明确说明收集的目的。
- 组织必须获得个人同意，才能收集、使用和披露其个人信息。
- 组织只能使用个人信息用于指定的目的，并且必须确保使用的方式是合理和合法的。
- 组织只能披露个人信息给授权的第三方，并且必须确保披露的方式是安全和合法的。
- 组织必须确保个人信息的保留期限是合理的，并且必须删除不必要的个人信息。
- 组织必须确保个人信息的准确性，并且必须纠正不准确的信息。
- 组织必须确保个人信息的安全性，并且必须采取合理的措施来防止数据泄露和滥用。
- 组织必须确保个人信息的开放性，并且必须提供个人信息的访问和更正的机会。
- 组织必须确保个人可以参与个人信息的管理，并且必须提供个人信息的访问和更正的机会。
- 组织必须确保对个人信息的处理是负责任的，并且必须承担个人信息泄露和滥用的责任。

▶ 加拿大数据违规案例

违反PIPEDA的商业组织可能面临以下三种处罚：最高50,000加元的罚款；法院可以命令商业组织采取特定措施以纠正违反行为；商业组织的名誉可能受到损害。

2020年3月，加拿大一家提供无线通信的移动网络运营商发生了数据泄露事件。据报道，黑客入侵了该公司的数据库，盗取了大约15,000名客户的个人信息。泄露的信息包括客户姓名、地址、电话号码、电子邮件地址、账户信息（包括账户余额和支付信息）。黑客使用了一种称为"SQL注入"的攻击方法，利用该公司网站上的漏洞，入侵了该公司的数据库。该数据泄露事件对公司客户造成了影响，包括潜在的身份盗窃风险，财务信息泄露，对该公司的声誉造成了损害。

该公司在发现数据泄露事件后，立即采取了措施，包括通知受影响的客户、提供免费的信用监测服务，更新了该公司的安全措施，以防止类似的事件再次发生。该公司的数据泄露事件提醒我们，网络安全是非常重要的。公司必须采取合理的措施，以保护客户的个人信息，包括定期更新安全措施，提供员工培训，使用安全的编码实践。

拉丁美洲 3.3

3.3.1 墨西哥

墨西哥法规要求概述

在欧盟的GDPR推出之前，墨西哥就已经拥有数据隐私的法规。在数据隐私保护方面，墨西哥主要有两部法律：

- 墨西哥《保护私人持有的个人数据的联邦法》（The Federal Law on the Protection of Personal Data Held by Private Entities）于2010年7月6日发布，该法确定了个人数据保护原则，以及对个人数据处理相关各方的义务[1]。规范了个人信息的合法、受控和知情处理，保障个人隐私和自主决定权。
- 墨西哥《保护义务主体持有的个人数据联邦法》（《义务主体数据保护法》，The General Law of Protection of Personal Data in the Possession of Obliged Subjects）于2017年1月27日发布，该法为在联邦、州和市一级行政、立法和司法部门、自治机构、政党、信托机构和公共基金的任何当局、实体、机关和机构保护个人数据制定了法律框架[2]。

墨西哥的《保护私人持有的个人数据的联邦法》具有域外效力，在以下情形之下，位于墨西哥境外的实体也应当遵守该法律的合规要求：

- 数据在位于墨西哥的数据控制者的营业地点进行处理。
- 数据由数据处理者（无论其位于何处）处理，且该数据处理者代表位于墨西哥的数据控制者行事。
- 数据控制者不在墨西哥，但使用位于墨西哥的方法（means）处理个人数据，除非此类方法仅用于传输目的。

墨西哥法规重点梳理

监管机构

墨西哥个人数据保护最主要的监管部门是联邦信息获取和数据保护局（The National Institute for Access to Information and Data Protection），负责发布指导性意见、监督法律和法规的落实情况、监督相应主体履行法务义务的情况、根据法律规定开展行政执法、以及与其他国内国际监管机构合作等。

数据跨境

当数据控制者拟向除数据处理者之外的境外第三方传输个人数据时，必须通过隐私声明向数据所有者告知传输目的，并包含数据所有者是否同意跨境传输的条款。数据控制者和境外数据接收方就数据跨境传输承担相同的责任。

然而，对于以下例外情况，数据控制者无需获取数据主体的同意也可进行数据跨境传输：

- 国家法律或墨西哥参与的国际条约明确规定。
- 为医疗诊断或预防、医疗保健、医疗卫生服务管理所必需。
- 集团内部公司在相同的内部流程和政策下进行数据传输。
- 为履行数据控制者与第三方之间为数据主体之利益所签订的合同所必需。
- 为保护公共利益或司法行政所必需。
- 为在司法程序中确认、行使或维护法律权利所必需。
- 为维护或实现数据主体与数据所有者之间的法律关系所必需。

2018年，美国、墨西哥和加拿大签订了《美国-墨西哥-加拿大协定》（USMCA），该自由贸易协定旨在促进整个北美的商业流动。APEC跨境隐私规则（APEC CBPR，Cross-Border Privacy Rules）由APEC制定统一标准，获得相关认定后，APEC各成员之间即可开展便捷的数据跨境传输，以促进商贸往来。美国、加拿大、墨西哥已正式加入APEC CBPR体系。

数据本地存储

墨西哥没有规定数据必须存储在本地，但对数据跨境传输有明确规定（如上）。

[1]https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/in-mexico

[2]https://news.bloomberglaw.com/privacy-and-data-security/mexicos-general-law-on-the-protection-of-personal-data-held-by-obliged-subjects

个人数据保护

《保护私人持有的个人数据的联邦法》的第8条规定，“除本法规定的例外情况外，所有个人数据的处理均应征得其所有者的同意”，征得同意是在墨西哥开展数据处理活动的唯一合法性基础。根据个人数据性质的不同，同意可以是明示的、也可以是默示的。

根据该法律规定，数据主体享有以下权利：撤回同意的权利、查阅权、更正权、删除权、异议权。而数据控制者需要履行以下法定义务：最小必要、存储受限、安全保护、告知义务、报告数据安全事件、任命数据保护官。

在法律规定的以下例外情况下，数据控制者无需获取数据主体的同意即可处理个人数据：

- 法律规定的无需获取同意的情形。
- 数据包含在可公开访问的来源中。
- 个人数据经过事先去关联化处理，个人数据无法与数据所有者建立联系。
- 履行与数据主体签订合同所必需的。
- 存在可能会损害个人的人身或财产的紧急情况。
- 它们对于医疗保健、预防、诊断、提供医疗保健、医疗或管理健康服务至关重要，而数据所有者无法根据《通用健康法》和其他适用法律规定的规定给予同意，并且此类数据处理是由受专业保密或同等义务约束的人进行的。
- 满足主管当局的要求。

对于个人敏感数据，《保护私人持有的个人数据的联邦法》明确规定，数据控制者获得数据主体的明确书面同意之后才能处理其个人数据。

▶ 墨西哥数据违规案例

违反墨西哥个人数据保护法律法规的，将面临罚款等行政处罚和监禁等处罚。INAI主要针对数据主体的投诉进行调查，已经多次对数据控制者处以大额处罚，主要原因包括：未向数据处理者提供隐私声明、提供不完整声明、未经同意传输个人数据以及泄露数据等。

罚款金额按照违法程度不同，存在以下罚款区间（自2024年起，墨西哥的最低工资水平提高到每天约248比索，约合14.25美元左右）：

- 墨西哥城最低工资100至160,000天的罚款。
- 墨西哥城最低工资200至320,000天的罚款。
- 如果重复出现违法行为，额外再加当前墨西哥城最低工资100至320,000天的罚款。

《保护私人持有的个人数据的联邦法》还规定了违法处理个人数据的刑事责任：

- 任何授权主体为牟利处理个人数据而造成安全漏洞，影响其所保管的数据库的，将被判处三个月至三年监禁。
- 任何主体以获取非法利益为目的，利用数据所有者或经授权传输数据的主体的错误，以欺骗方式处理个人数据，将被判处六个月至五年监禁。

如果数据控制者使用欺骗手段、处理的数据涉及敏感个人数据或者存在累犯的情形，处罚将根据实际情况加重或翻倍。

2015年，墨西哥一家金融机构被INAI处以3,200万比索（约合170万美元）的罚款，原因是其未经数据主体明确书面同意就处理了个人敏感数据（包括个人健康数据）。根据INAI的报告，2023年罚款总额超过4,600万墨西哥比索（约合270万美元）[1]。

[1]https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-007-24.pdf

3.3.2 巴西

巴西法规要求概述

巴西《通用数据保护法 》（Lei Geral de Proteção de Dados，LGPD）于2020年9月18日生效。LGPD以欧盟的《通用数据保护条例》（GDPR）为蓝本，与GDPR一样，规定了个人和公司如何收集、使用和以其他方式处理个人数据[1]。

另外，巴西电信法（Lei Brasileira de Telecomunicações）是巴西联邦法律，规范巴西电信行业。法律适用于巴西所有电信服务和提供商，包括固定电话、移动电话、互联网服务和卫星通信等，也适用于国际电信服务和提供商在巴西的业务。国家电信局（ANATEL）负责执行法律和确保遵守巴西电信法。ANATEL有权对违反法律的电信提供商实施罚款、暂停或撤销许可证等执行措施。国家电信局（ANATEL）负责执行法律和确保遵守巴西电信法。ANATEL有权对违反法律的电信提供商实施罚款、暂停或撤销许可证等执行措施。

巴西法规重点梳理

监管机构

国家数据保护机构（ANPD）是执行LGPD的政府机构，负责保护个人数据，监督和执行该法律，并对违反该法律的处罚。此外，该机构还负责与其他政府部门协调其活动，以确保遵守该法律，并保护商业秘密和信息的保密。

数据跨境

LGPD对跨境数据传输有严格规定，旨在确保即使数据被传输到其他国家，数据主体的隐私和数据保护权利仍然得到充分的保障。

根据LGPD的规定，跨境数据传输可以在以下条件之一满足时进行：

- **充分保护水平**：如果数据接收国根据巴西国家数据保护局（ANPD）的评估，被认定为具备充分的隐私保护水平，那么可以进行数据传输。
- **法律工具**：如果跨境数据传输的国家或地区没有被认定为具备充分保护水平，数据控制者可以通过标准合同条款、全球公司间的企业规则（BCRs）或其他法律工具，确保接收方遵守与LGPD类似的保护义务。
- **数据主体的同意**：在跨境数据传输之前，数据主体必须被明确告知数据转移的国际性质，并且他们必须明确同意这种传输。
- **法律或监管规定**：如果传输是为了履行国际法律或监管义务，或者是在公共利益、医疗、研究等特定情况下，这种传输可能被允许。
- **合同义务**：当数据传输是履行合同的一部分时（例如，为了履行客户请求或为其提供服务），这种传输可能被允许。

巴西的LGPD对跨境数据传输有严格的规定，要求企业确保接收方的保护水平足够，或采取法律工具、获得数据主体同意，或者在特定情况下遵守例外条款。所有这些规定的核心目标是确保巴西公民的个人数据在跨境传输时，仍然受到与LGPD相当的保护。企业必须遵守这些要求，以避免法律责任和潜在的制裁。

数据本地存储

巴西的《通用数据保护法》（LGPD， Lei Geral de Proteção de Dados， Law No. 13，709/2018）并没有明确要求数据必须在巴西境内存储。

虽然LGPD没有要求数据必须在巴西本地存储，但对于某些公司和行业来说，出于合规性、数据主权、法律便捷性或商业策略等考虑，可能会选择在巴西境内存储数据。

个人数据保护

LGPD共十章，包含基本条款、个人数据的处理、个人数据所有者权利、公共机构对个人数据的处理、国际数据传输、个人数据处理代理人、数据安全及良好实践、国家数据保护局及国家保护个人数据和隐私委员会等内容。

- **个人数据保护**：LGPD旨在确保个人数据在透明、公平和安全的处理中，并且个人有控制自己数据的权力。
- **透明度和责任**：该法要求数据控制者（收集和处理个人数据的组织）对如何收集、使用和共享个人数据的透明度，并且对数据保护的违反负责。
- **数据主体权利**：LGPD授予个人某些权利，例如访问、更正和删除个人数据的权利，以及反对数据处理的权利。
- **数据安全**：该法要求数据控制者实施适当的技术和组织措施来确保个人数据的安全和完整性。
- **数据转移**：LGPD 规范个人数据的转移，确保数据被转移到提供个人数据保护的国家。
- **罚款和处罚**：该法规定了数据控制者违反LGPD的罚款和处罚，包括罚款和严重案件中的监禁。

[1]https://www.gov.br/anpd/pt-br

巴西数据违规案例

根据LGPD，数据处理代理人（即控制者或操作者）如果违反法律规定，可能面临如下行政处罚：警告；罚款；公开违法行为；删除或封存与违法行为相关的个人数据；暂停运行违法行为所涉数据库；暂停违法行为所涉个人数据处理活动；部分或全部禁止开展与数据处理相关的活动。其中，罚款的最高额为该私法人实体、集团或联合企业在巴西上一财政年度营业额的2%（不含税），每次违规罚款总额不超过5,000万雷亚尔（约合人民币7,000万元）。

在2020年，巴西某银行因未能正确通知个人数据泄露和未能实施适当的数据保护措施而被罚款R$1.5万（约USD375,000）。巴西某银行的违法行为涉及两个主要问题：

- **未能通知个人数据泄露**：巴西某银行未能正确通知个人数据泄露，这是LGPD的关键部分，因为个人有权知道可能影响他们的数据泄露。
- **缺乏适当的数据保护措施**：巴西某银行未能实施适当的数据保护措施，以防止数据泄露的发生，这包括缺乏加密、不充分的访问控制和不充分的监控和事件响应程序。

ANPD的调查发现，巴西某银行未能采取合理措施保护其客户的个人数据，这包括敏感信息，如姓名、地址和金融数据。对巴西某银行的罚款是非常具有代表性，作为对其他组织的一个警告，表明未遵守LGPD就要承担相关法律后果。

3.3.3 阿根廷

阿根廷法规要求概述

2000年10月30日，阿根廷发布个人数据保护法（Personal Data Protection Law，PDPL），以帮助保护阿根廷境内的个人数据隐私，以及个人数据在国际间的跨境传输。PDPL与欧盟的数据保护立法模式一致，而且阿根廷是拉丁美洲中第一个获得从欧盟进行数据传输的“充分性认定”的国家[1]。

阿根廷PDPL适用于位于阿根廷境内就个人或法律实体（后者需位于阿根廷或在阿根廷设有办事处、分支机构）个人数据的处理行为。

2018年7月23日由阿根廷公共信息获取机构（简称“AAPI”）颁布的第47/2018号决议（Resolution 47/2018，简称 “第47号决议”）。第47号决议旨在保护从数据收集到数据删除的个人数据处理过程中的机密性和完整性。该决议规定数据使用者应采取必要技术和组织措施，保障个人数据的安全性和机密性，从数据收集、访问控制、变更管理、备份和恢复、漏洞管理、销毁信息、安全事件及开发环境八个控制领域出发，依据国际标准提出了共30个具体安全保护目标以及相对应的建议安全控制措施。此外，第47号决议还包括适用于“敏感数据”的安全措施清单。

阿根廷《个人数据保护法》修订草案于2022年9月公布并于同年11月通过。修订草案在许多方面遵循了欧盟GDPR的规定。该法案的关键条款包括但不限于：

- 新设的域外效力原则。
- 个人数据处理的合法性、公平性与透明度原则。
- 个人数据处理的目的明确、数据最小化、准确性和问责制原则。
- 数据主体的同意以及同意的特征、要求。
- 公共部门的数据处理。
- 新设的允许个人信息自由跨境传输的机制。
- 对儿童和青少年个人数据的特别保护。
- 数据主体所享有的查阅、纠正、限制和删除的权利等。
- 数据控制者应当履行的义务，包括与隐私影响评估相关的义务。

阿根廷法规重点梳理

监管机构

阿根廷的公共信息获取机构（AAPI）负责执行个人数据保护法。

数据跨境

2016年，AAPI发布了一条新法规（条款60-E/2016），用来管理个人数据的跨境传输。在该规则下，批准了传输到数据控制器和数据处理器的模式（部分基于欧盟中的数据传输模式）。根据阿根廷的法律规定，除例外情况外，应在确认传输的国家或国际组织有足够的水平保护个人数据时才能进行个人数据的跨境传输。

阿根廷已正式承认一系列具有足够数据保护水平的国家或地区，其中包括欧盟和欧洲经济区成员国、瑞士、根西岛和泽西岛、马恩岛、法罗群岛、加拿大（仅限商业组织）、新西兰、安道尔、乌拉圭，以及大不列颠及北爱尔兰联合王国。

阿根廷禁止将任何类型的个人信息转移到未提供足够保护水平的国家或国际或超国家实体。但是，该禁令不适用于以下披露：

- 用于国际司法合作。
- 用于流行病学调查目的的医疗保健或匿名个人数据。
- 用于股票交易所或银行转账。
- 受阿根廷共和国签署的国际条约约束。
- 用于情报机构在打击有组织犯罪、恐怖主义和贩毒方面的国际合作。
- 数据主体明确同意转移的情况。

[1]https://d1.awsstatic.com/whitepapers/compliance/Argentina_Privacy_Workbook.pdf#:~:text=In%20July%202018%2C%20the%20Argentine%20Data%20Protection%20Authority,processing%20%E2%80%93%20from%20data%20collection%20to%20data%20deletion.

数据本地存储 阿根廷没有规定数据必须存储在本地，但对数据跨境传输有明确规定（如上）。

个人数据保护 PDPL规定了数据拥有者和数据使用者两种角色：

- 数据拥有者是个人数据的所有者，享有PDPL赋予的知情权、访问权、撤回权、更正、更新和限制处理权等。
- 数据使用者需对收集的个人数据负责，基于PDPL的核心要求收集、处理、保护、传输数据拥有者的个人数据，并应遵从如第 47号决议等监管机构发布的条例、良好实践指南等官方文件。

阿根廷PDPL规定了如下有关个人数据处理的核心监管要求：

- 保障个人数据的质量
- 通知和获取同意
- 有条件地收集和处理敏感数据与医疗数据
- 保障数据安全
- 保密义务
- 数据传输相关的同意
- 有条件的跨境传输
- 信息登记要求
- 数据留存时间限制
- 直接促销的数据处理限制

针对个人敏感数据，阿根廷法律规定，不得强迫任何人提供敏感个人数据。获得处理敏感个人数据的同意必须是明确的和知情的。根据具体情况，同意应为书面形式或类似形式。敏感个人数据只能在以下情况下处理：

- 存在法律授权的普遍利益情况。
- 出于统计或科学目的，前提是无法从该信息中识别数据主体。

禁止创建直接或间接泄露敏感个人数据的个人数据库。但是，天主教会、宗教协会、政党和工会有权保存其成员的登记册。

▶ 阿根廷数据违规案例

对于违反阿根廷个人数据保护法律法规的行为，AAPI可实施行政处罚或刑事处罚。

- 行政处罚包括警告、暂停营业、关闭数据库或最高15,000,000阿根廷比索的罚款。处罚与侵权严重性和程度成正比。
- 刑事处罚包括：
  - 故意在个人数据库中插入虚假信息，可处以最高两年监禁。
  - 故意向第三方提供个人数据库中的虚假信息，可处以最高三年监禁。
  - 入侵个人数据库，可处以最高三年监禁。
  - 泄露数据库中的机密信息可处以最高三年监禁。
  - 如果对数据主体造成伤害或公职人员在履行职责时犯下罪行，处罚将加重。

2021年9月9日，AAPI对一家大型的超市连锁店进行了制裁，原因是该连锁店未通知其客户他们因恶意软件导致了个人数据泄露，随后发送了网络钓鱼邮件。该机构得出结论，该超市连锁店未遵守法律规定的安全和保密原则，并处以290,000阿根廷比索的罚款[1]。

[1]https://www.linklaters.com/insights/data-protected/data-protected---argentina

中东地区 3.4

3.4.1 以色列

以色列法规要求概述

以色列《隐私保护法》（Protection of Privacy Law，PPA），它由以色列法律框架下的数据保护监管机构负责执行。该法律旨在保护个人数据的隐私，并规定了数据处理的条件、数据主体的权利、数据控制者的义务以及跨境数据传输的要求[1]。

以色列法规重点梳理

监管机构

以色列《隐私保护法》的监管由以色列隐私保护局（Privacy Protection Authority， PPA）负责。隐私保护局负责监督所有涉及个人数据处理的活动，确保各方遵守《隐私保护法》的规定。它有权对违反法律的机构进行调查，并实施相应的处罚，如行政罚款或其他法律制裁。

数据跨境

对于需要传输到国外的数据，必须确保接收方所在国家或地区具备与以色列相当的数据保护水平，或事先获得数据主体的明确同意，并且采取必要的安全措施。在某些情况下，数据应保留在以色列境内，以避免可能的隐私风险。个人或实体不得将来自以色列的数据库数据转移到国外，除非境外国家的法律保护水平与以色列法律相当或更高，并满足以下原则：

- 数据应合法且公正收集和处理。
- 数据应仅用于收集它们的目的。
- 数据应准确且最新。
- 数据主体保留查阅权。
- 数据库所有者应采取适当的安全措施来保护数据库中的数据[2]。

然而，数据库所有者可以在满足以下条件之一时将数据从以色列传输到国外：

- 数据主体同意转移。
- 无法获得数据主体的同意，但转移对其生命或身体健康至关重要。
- 数据转移到数据库所有者控制的公司。
- 数据转移给按照数据库所有者的要求遵守保护条件的人。
- 数据已公开或已由法定机构公开检查。
- 数据转移对公共安全或安全至关重要。
- 数据转移是根据以色列法律的要求。
- 数据转移到与欧洲自动处理敏感数据保护公约的国家/地区、接受欧盟成员国同样条件的国家/地区或具有适当保护机构并与其达成合作安排的国家/地区。

在转移数据时，数据库所有者应在书面保证中确保收件人采取适当的措施来保护数据主体的隐私，并确保数据不会转移给其他人。

数据本地存储

以色列收集的个人数据，尤其是涉及敏感信息的，应优先存储在本地服务器上。此要求旨在确保数据的处理和保护符合以色列的隐私和安全标准。以色列的《隐私保护法》并未规定强制的数据本地存储要求。因此，个人数据可以在国外存储和处理，只要符合相关的数据保护标准。

[1]https://www.gov.il/en/departments/the_privacy_protection_authority/govil-landing-page

[2]https://www.gov.il/BlobFolder/legalinfo/legislation/en/PrivacyProtectionTransferofDataabroadRegulationsun.pdf

个人数据保护 以色列的“隐私保护法”是一项涵盖性法律，规定以色列境内的个人数据收集、处理和保护。该法律旨在平衡个人对隐私数据的保护权利和组织对这些数据的合法使用需求。

- **个人数据定义**：法律定义个人数据为任何能够识别或允许识别个人的信息，包括姓名、身份证号、地址、电话号码、电子邮件地址等其他信息。
- **同意**：法律要求个人在其个人数据被收集、处理或披露前提供明确的同意。同意必须是明确的、特定的和自愿的。
- **目的限制**：法律要求个人数据只用于指定的、明确的和合法的目的。数据不得用于与原有目的不符的目的。
- **数据最小化**：法律要求个人数据只收集和处理到达指定目的为止。
- **准确性**：法律要求个人数据是准确的、最新的和完整的。组织必须采取合理措施确保数据的准确性。
- **存储和保留**：法律要求个人数据只存储和保留到达指定目的为止。
- **安全性**：法律要求组织采取合理措施保护个人数据免受未经授权的访问、使用、披露、修改或销毁。
- **数据主体权利**：法律授予个人以下权利：
  - 访问个人数据
  - 更正不准确的数据
  - 删除数据
  - 对数据的处理提出异议
  - 限制数据的处理
  - 接收数据泄露通知
- **数据泄露通知**：法律要求组织在数据泄露可能对个人权利和自由造成风险时通知个人和以色列数据保护局（DPA）。
- **执行力**：法律由以色列DPA执行，该局负责调查投诉、罚款和其他执行措施。

▶ 以色列数据违规案例

以色列在实施《隐私保护法》时，对违反隐私保护规定的行为采取了严格的处罚措施。

- **罚款**：罚款金额取决于违反行为的性质和严重性，最高可达500,000 谢克尔（约合15,000美元）。
- **行政处罚**：以色列隐私保护局（PPA）可以对违反隐私保护规定的组织或个人实施行政处罚，包括警告、罚款、暂停或终止业务等。
- **刑事处罚**：在某些情况下，违反隐私保护规定的行为可能构成刑事犯罪，结果可能是罚款、监禁或其他刑罚。

2022年，一家以色列医疗机构发生了数据泄露事件，患者的个人健康信息被未经授权的第三方获取。调查发现，该机构未能实施足够的安全措施来保护敏感的健康数据，如数据加密和访问控制。数据泄露未得到及时报告。

调查结果表明，该事件发生的原因有以下几点：

- **弱密码**：医院的数据库使用了弱密码，使得黑客可以轻松地访问网络。
- **缺乏加密**：医院的数据库没有加密，使得黑客可以轻松地访问敏感信息。
- **安全措施不足**：医院的安全措施不足，使得黑客可以轻松地访问数据库。

以色列隐私保护局（PPA）对该医疗机构罚款了150,000 谢克尔 (约40,000美元)，以彰显其未能遵守数据保护法的责任。

3.4.2 沙特

沙特法规要求概述

沙特阿拉伯在2021年9月发布了其第一部数据保护法(The Personal Data Protection Law ，PDPL)，这项法规受欧洲通用数据保护法（GDPR）的启发。随后，沙特阿拉伯于2023年3月对PDPL进行了修正，并最终于2023年9月14日生效[1]。

PDPL兼具域内效力和域外效力。PDPL适用于在沙特境内以任何方式处理的与个人有关的任何个人数据，包括沙特境外任何一方以任何方式处理与居住在沙特境内的个人有关的个人数据。个人和家庭用途的数据处理不在该法案适用范围内，依据PDPL执行条例的定义，只要不向第三方发布或披露，“个人在其家庭或有限社交圈内作为任何社交或家庭活动的一部分而处理的个人数据”不在法案适用范围内。

沙特法规重点梳理

监管机构

沙特阿拉伯王国数据和人工智能管理局 (SDAIA) 是负责数据保护的主要监管机构，其下设三个部门，分别负责不同领域：国家信息中心、国家人工智能中心和国家数据管理办公室(NDMO)。

其中，国家数据管理办公室是该局的立法机构，负责制定和实施计划、政策、数据法规及相关项目，并监督其合规情况。它还承担着与其他司法管辖区的数据保护办公室类似的职能。国家数据管理办公室与商界保持密切合作，定期发布简讯，阐明其在技术、人工智能和数据领域的立场，并促进与在沙特运营的国内外企业的直接沟通。SDAIA将发布有关保护数据传输机制、监督个人权利处理的进一步指导方针和政策，并对违规行为进行处罚。

数据跨境

沙特主要在《传输条例》中规定数据跨境事项，立法上，为数据跨境传输设置了三条路径：充分性保护水平、适当保障措施、特定豁免条件。同时PDPL还概括性地规定，在将数据传输至境外的过程中，必须满足以下条件：

- 转让或披露不得对王国的国家安全或重大利益造成不利影响。
- 基于“适当措施”或“特定豁免条件”开展数据跨境转移，或持续大规模向境外传输敏感数据，须开展风险评估。
- 个人数据的转移或披露应仅限于所需的最低限度。

数据本地存储

沙特阿拉伯PDPL并没有明确规定所有数据必须本地化存储。敏感数据，例如卫生数据、金融数据，必须在沙特阿拉伯境内存储。非敏感数据可以存储在境外，但必须遵守PDPL中的数据保护原则。

沙特PDPL允许组织在以下情形下在境外存储个人数据：

- 沙特阿拉伯监管机构批准境外数据存储计划。
- 组织能够确保个人数据在境外存储的安全性和保密性。
- 组织能够向个人数据所有者提供相关信息和保护措施。

个人数据保护

数据主体享有以下权利：

- 知道数据处理的目的和手段
- 访问个人数据
- 修正或删除个人数据
- 对数据处理提出异议
- 请求删除个人数据

数据控制方必须确保个人数据的保密性、完整性和可用性，并采取适当措施防止未经授权的访问、公开、修改或删除个人数据。

[1]https://dgp.sdaia.gov.sa/wps/wcm/connect/f579bc32-fda8-47bd-bc6f-66b8cb77985c/ENG-Guide+to+the+saudi+PDP+law+for+controllersprocessors.pdf?MOD=AJPERES

沙特数据违规案例

对于为了谋取私益而违反PDPL泄露或公布敏感数据的行为，最高可处以300万沙特里亚尔（约合5,784,900人民币）的罚款和最高两年的监禁。

对于违反数据传输规则的行为，最高可处以100万沙特里亚尔（约合1,928,300人民币）的罚款和最高一年的监禁。

对其他违反PDPL的行为处以最高500万沙特里亚尔（约合9,641,500人民币）的一般罚款，屡犯者罚款额有可能翻倍。

2023年，某国际公司在沙特阿拉伯运营的分支机构发生了大规模的数据泄露事件，泄漏了客户、员工和业务伙伴的敏感信息。调查结果表明，该事件发生的原因有以下几点：

- **缺乏安全措施**：公司的网络没有实施足够的安全措施，包括防火墙、入侵检测系统和加密。
- **弱密码**：员工使用了弱密码，使得黑客可以轻松地访问网络。
- **培训不足**：员工没有接受充分的网络安全培训，导致他们在使用密码和网络时不当行为。
- **软件过时**：公司的软件和操作系统过时，留下了已知漏洞的窗口。

公司因事件而遭受重大财务损失，损害了公司的声誉，包括通知受影响个人的成本、提供信用监控服务的成本。沙特数据保护局(SDAIA)对该公司处以2,000,000沙特里亚尔 (约533,000美元)的罚款，并要求公司采取整改措施以加强数据保护。

3.4.3 阿联酋

阿联酋法规要求概述

阿联酋联邦政府于2021年9月20日颁布了《个人数据保护法》(Protection of Personal Data Protection， PDPL)（2021年第45号联邦法令），为该地区提供了统一的个人数据保护框架，这是阿联酋数据保护法律的核心。该法律于2022年1月2日正式生效，适用于在阿联酋境内的任何数据控制者（data controller）或处理者（data processor）所进行的所有个人数据处理活动，不论数据主体身处何地[1]。此外，位于阿联酋境外但处理阿联酋境内数据主体个人数据的任何控制者或处理者的活动也在该法的适用范围内。

《个人数据保护法》在结构上与欧盟《通用数据保护条例》（GDPR）相似，涵盖了多个重要内容，包括合法性基础（第4条）、数据主体的权利（第13至18条）、数据控制者和数据处理者的义务（第7和8条）、数据保护官的任命（第10和11条）、以及数据跨境传输（第22和23条）等方面。总体而言，《个人数据保护法》与欧盟的GDPR和中国的《个人信息保护法》在原则和要求上有许多相似之处。

自由经济区数据相关法规

阿联酋自由贸易区有权发布其区域内适用的数据保护法律法规。目前，迪拜国际金融中心（Dubai International Financial Centre，DIFC）、阿布扎比全球市场（Abu Dhabi Global Market，ADGM ）都分别颁布了各自区域内的数据保护条例。

迪拜国际金融中心

迪拜国际金融中心的主要法律依据是《迪拜国际金融中心数据保护法》（The DIFC Data Protection Law），并辅以《迪拜国际金融中心数据保护条例》（DIFC Data Protection Regulation）。《DIFC数据保护法》的内容与GDPR相似，涵盖了数据处理的基本原则、数据主体的权利、数据控制者和数据处理者的义务、数据泄露通知、法律责任等方面。具体内容包括合法性基础、数据主体的权利、数据控制者/处理者的义务，透明度要求、数据保护机构、以及违法后果等。《DIFC数据保护条例》进一步细化了《DIFC数据保护法》中若干条款的实施规则，如数据泄露通知的程序与规则和数据保护专员的职权行使程序与限制。

根据《DIFC数据保护法》，处理个人数据的合法性基础是获得当事人的同意，除非符合其他例外情况。数据主体享有知情权、更正权、删除权和拒绝处理权等多项权利。数据控制者和处理者则负有保障数据安全、记录和通知等义务。在透明度方面，数据控制者和处理者应避免引发数据主体误解，并不得通过暗示可能受到歧视的方式来诱导数据主体同意数据处理。

与GDPR或中国的《个人信息保护法》不同，《DIFC数据保护法》对每个具体条款的违反后果都明确了相应的罚款金额，罚款范围从25,000美元到100,000美元不等。此外，同一行为可能同时违反多条规定，因此除了罚款外，还可能需要承担赔偿责任。

阿布扎比全球市场

阿布扎比全球市场所实施的为2021年2月11日所发布的《2021数据保护条例》（Data Protection Regulation 2021）。《ADGM数据保护条例》为数据控制者和数据处理者设置了较高的保护义务，处理个人数据的合法性基础原则上需要取得个人同意，除非具备其他合法性基础；数据主体享有知情权、更正权、删除权、可携带权、拒绝权等权益；明确了合法、目的正当、最小必要、充分保障安全的处理原则。

与阿联酋《个人数据保护法》不同的是，《ADGM数据保护条例》对企业必须设置数据保护官的情形更多参考了GDPR的规定。根据《ADGM数据保护条例》，若企业的核心业务活动包括个人数据处理活动，需要定期和系统地大规模监测数据主体，或包括大规模处理特殊类别的个人数据，则企业应当设置一名数据保护官。《数据保护条例》也规定了独立的数据保护办公室（ODP），由新成立的数据保护专员领导。

阿联酋自由贸易区迪拜国际金融中心（Dubai International Financial Centre，DIFC）和阿布扎比全球市场（Abu Dhabi Global Market，ADGM）已经通过了适用于其自贸区的隐私保护法。在DIFC和ADGM设立的实体以及在DIFC范围内通过稳定安排处理个人信息的公司需要评估是否落入DIFC和ADGM自贸区数据保护法。

与阿联酋的《个人数据保护法》（PDPL）相比，迪拜国际金融中心（DIFC）和阿布扎比全球市场（ADGM）的数据保护立法更加细致和全面。此外，DIFC和ADGM的各自数据保护主管机构还发布了一系列指南和模板供数据处理者参考使用，例如数据保护影响评估模板、数据泄露通知模板、跨境传输白名单和标准合同条款等。目前，中国并未被列入DIFC和ADGM认可的跨境传输白名单国家。

[1]https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws　　https://uaelegislation.gov.ae/en/legislations/1972/download

阿联酋其它酋长国

除了《阿联酋数据保护法》（Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data），沙迦、阿治曼、富查伊拉、乌姆盖万、哈伊马角这些酋长国还可能遵循其他相关的法规和政策，特别是在特定行业或领域。以下是一些适用的数据保护法规或要求：

- **电信行业法规**：阿联酋电信监管局（TRA）对电信行业有一系列的规定，其中包括对用户数据保护的要求。这些规定适用于在各个酋长国运营的电信服务提供商。
- **健康数据保护法规**：卫生领域的数据保护有特定的要求，特别是对于涉及病人信息的处理。阿联酋卫生部和各个酋长国的地方卫生部门可能有相关规定，确保健康数据的隐私和安全。
- **金融行业法规**：阿联酋中央银行和各酋长国的金融服务监管机构对金融数据的处理有严格的规定。这些规定可能包括客户数据保护的要求。
- **网络安全法规**：阿联酋的网络安全法律和政策也包含了对数据保护的要求，如《阿联酋网络安全法》（Federal Law No. 5 of 2012 on Combating Cybercrimes）。这些规定旨在防止网络犯罪，并保障个人和企业的数据安全。
- **自由区的特定规定**：在一些酋长国，如沙迦和富查伊拉，存在自由区（Free Zones），这些自由区可能有其自身的数据保护条例。

除了上述内容，各个酋长国通常会遵循国家级别的指引，并根据国家法律在地方层面实施补充性措施。因此，除非特定行业或领域有特殊规定，沙迦、阿治曼、富查伊拉、乌姆盖万、哈伊马角主要还是依照阿联酋《个人数据保护法》和相关的联邦法律框架来管理数据保护事务。

阿联酋法规重点梳理

监管机构

根据阿联酋《个人数据保护法》（PDPL），PDPL的执行机构是阿联酋数据保护局（United Arab Emirates Data Protection Authority，UAE DPA）。

DPA负责执行PDPL，包括：

- 监管和监督数据处理活动，以确保数据处理的合法性和透明度。
- 处理数据泄露事件和数据保护违规行为的调查和处理。
- 提供数据保护指导和培训，帮助企业和个人遵守PDPL。
- 承担其他相关的数据保护职责。

数据跨境

阿联酋PDPL构建了基本的跨境传输框架。个人数据可以被转移到阿联酋境外，只要接收数据的国家的现行法律能够提供“足够水平的保护”，类似于GDPR下欧盟委员会做出充分性认定的白名单国家。但截止目前，阿联酋主管机关尚未发布白名单国家清单。

在当前没有保护充分性决定的情况下，阿联酋PDPL也提供了一些例外情况，满足下列情形之一的也可将个人数据转移到没有充分保护水平的国家：

- **合同保障**：传输数据的两个组织之间可以签订合同或协议，适用阿联酋PDPL的规定、措施、控制和要求。
- **明确同意**：数据主体明确同意其数据被转移至境外。
- **合同义务**：为签订或履行数据主体与控制者之间的合同，或是为实现数据主体利益而促进控制者与第三方之间的合同而进行的必要传输。
- **法律义务**：为履行义务以及向司法机关证明、行使或捍卫权利而进行的必要传输，以及为执行国际司法合作相关程序所必需的传输。
- 数据跨境传输是保护公共利益所必需的。

数据本地存储

PDPL要求组织在阿联酋境内存储个人数据，除非有合法的理由存储在外国。组织必须在阿联酋境内使用安全和受保护的数据中心或云服务提供商存储个人数据，该数据中心或云服务提供商必须由阿联酋通信管理局（TRA）认证。

个人数据保护 根据《个人数据保护法》的第四条规定，未经数据所有者的同意，处理其个人数据是被禁止的，除非存在《个人数据保护法》规定的例外情况，例如基于公共利益、处理已公开的个人数据、或为了保护数据主体的利益等。

PDPL 关于个人隐私保护的关键条款：

- **数据收集**：该法规要求数据控制器在收集个人数据前获得明确的同意。
- **数据处理**：数据控制器必须公平、合法和透明地处理个人数据，并确保数据的准确性、完整性和最新性。
- **数据安全**：数据控制器必须采取适当的技术和组织措施来确保个人数据的安全和完整性。
- **数据主体权利**：数据主体有权访问、修改、删除和异议对其个人数据的处理。
- **数据转移**：数据控制器必须在将个人数据转移到第三方前获得数据主体的明确同意。
- **数据泄露通知**：数据控制器在发生数据泄露时必须通知国家数据保护委员会（NDPC）和数据主体。
- **数据保护官员**：数据控制器必须任命数据保护官员（DPO）以确保遵守法规和处理数据保护相关事宜。

阿联酋数据违规案例

根据PDPL，阿联酋数据保护局（DPA）负责执行该法和对违反该法的个人和组织实施罚款。该法规定了违反法的罚款，包括：

- **警告**：DPA可能对违反者发布警告，并将其发布在DPA的网站上。
- **行政罚款**：DPA可能对违反者罚款，罚款范围为阿埃迪50,000至500,000迪拉姆（约合1,3600至136,000美元）的小规模违反。
- **刑事处罚**：对严重违反的违反者可能面临刑事处罚，包括最长两年的监禁和/或罚款500,000迪拉姆（约合136,000美元）。

2020年，阿联酋一家通信公司因未通知用户的一起数据泄露事件，被阿联酋数据保护局（DPA）罚款一百万阿联酋迪拉姆（约272,000美元）。该公司未能实施足够的安全措施来保护其用户的数据。因此，该公司的数据库被渗透，敏感信息，如姓名、地址、电话号码和使用模式被泄露。

经过调查发现，该公司违反了以下阿联酋PDPL的规定：

- 未能实施足够的安全措施来保护用户数据
- 未能在合适的时间通知用户数据泄露
- 未能向用户充分提供关于数据泄露的信息
- 未能采取合理的步骤来预防数据泄露

阿联酋数据保护局（DPA）的罚款旨在警告其他阿联酋公司不要类似地违反数据保护法。这个案例表明了阿联酋数据保护法的重要性，以及违反这些法规的后果，同时也强调了公司需要采取合理措施保护用户数据。

3.4.4 土耳其

土耳其法规要求概述

土耳其《个人数据法》（Personal Data Protection Law，PDPL）于2016年3月7日颁布。该法旨在规范个人数据的处理和保护个人权利和自由。该法律为个人数据的处理、存储、传输和销毁等各个环节提供了详细的规范和指导。

PDPL适用于在土耳其处理个人数据的所有数据控制者和处理者[1]。

土耳其法规重点梳理

监管机构

根据PDPL，监督和执行法规的监管机构是土耳其个人数据保护局（KİŞİSEL VERİLERİN KORUNMASI KANUNU，KVKK）。土耳其个人数据保护局是独立的公共机构，于2016年建立，以确保PDPL的实施和保护个人在个人数据处理中的基本权利和自由。

数据跨境

2024年3月12日，KVKK宣布，对土耳其多项法律进行修改的第7499号法案对PDPL进行了多项修订。对第9条进行了修订，修改了可将数据跨境传输的情形，并增加了有关个人数据保护委员会作出充分性决定的某些要求。通过签署委员会公布的标准合同，无需单独授权即可进行数据跨境传输。在没有根据合同协议（即标准合同条款或具有约束力的公司规则）做出适当性决定的情况下传输数据，罚款的金额为5万至100万土耳其里拉（1557美元至31,140美元）。

数据本地存储

PDPL并不要求数据控制方在土耳其境内存储个人数据，但数据控制方必须确保个人数据在安全和保护的环境中，且采取适当的措施保护个人数据，无论存储在哪里。如果数据处理活动在土耳其境内进行，数据控制方必须确保个人数据在土耳其境内存储，除非有合法的理由要在外国存储。

个人数据保护

- **数据控制器**：PDPL定义数据控制器为自然或法人实体，决定个人数据的处理方式和目的。
- **数据处理**：该法要求数据控制器公平、合法和透明地处理个人数据。数据控制器还必须确保数据的收集和处理是明确的、明确的和合法的。
- **数据主体**：PDPL 授予数据主体某些权利，包括访问、修改、删除和异议个人数据的处理。
- **安全措施**：数据控制器必须采取必要的技术和组织措施，以确保个人数据的安全、保密和完整性。
- **数据转移**：该法规定了将个人数据转移到第三个国家的规则，要求数据控制器确保接收国提供个人数据的适当保护。
- **数据泄露通知**：数据控制器在发生数据泄露时必须通知土耳其数据保护局（DPA）和数据主体。
- **数据保护官员（DPO）**：数据控制器拥有50名以上员工或处理敏感个人数据必须任命DPO。
- **记录**：数据控制器必须保留个人数据处理活动的记录，包括目的、数据类别和数据主体类别。
- **同意**：PDPL 需要数据主体对个人数据的处理提供明确的同意，除非存在特定的情况，如公共利益或合法利益。

土耳其数据违规案例

2023年，土耳其个人数据保护局（KVKK）通报了一起涉及某鞋履和配饰品牌的数据泄露事件。KVKK指出，该品牌违反了第6698号《个人数据保护法》第12（5）条的规定。该条款规定了数据处理者在数据保护中的义务，特别是关于数据泄露的处理和报告要求。

调查发现，有未经授权的人员试图登录品牌的管理平台。该平台由数据控制者创建，用于发送短信和电子邮件。未经授权的访问者通过获取客户的手机信息，向相关个人发送了包含网络钓鱼内容的短信，试图进行欺诈。此次数据泄露事件影响了1,926,889条记录，受影响的个人数据主要包括客户的手机号码等。

KVKK强调了数据控制者的法律责任，特别是在数据保护和隐私方面的责任。品牌被要求采取必要的措施以防止类似事件再次发生。KVKK会对涉事品牌处以100万土耳其里拉（约140,000美元）罚款，并要求其进行整改，以加强数据保护措施。品牌必须改进其数据安全和管理流程，确保符合《个人数据保护法》的要求。

[1] https://www.kvkk.gov.tr/

东南亚 3.5

3.5.1 印尼

印尼法规要求概述

印尼针对所有行业有两项比较重要的法规和指南：

- 第一是《电子信息和交易法》(Electronic Information and Transaction Law， EIT Law)，该法于2008年通过，主要目的是规范电子信息和交易的使用和保护，涵盖了数据隐私、电子签名、电子交易、电子信息等方面[1]。 该法之后经历了多次修订，2016年11月的修订增加了有关电子签名、电子合同和电子交易的规定，提高了电子交易的安全性和效率[2]。 2020年9月的修订增加了有关个人数据保护和电子信息安全的规定，加强了个人数据保护和电子信息安全。
- 第二是《个人数据保护法》(Personal Data Protection Law， PDP Law)，该法于2022年颁布，编号为第 27 号法令，颁布机关为印尼总统。该法专门针对个人数据的保护，对数据控制者和处理者提出了明确的义务，包括获得个人同意、确保数据准确性、实施安全措施等[3]。

另外，印尼针对一些行业也制定了个人信息和数据安全法规，例如：《金融服务管理局条例第1/POJK.07/2013号》由印尼金融服务管理局(OJK)颁布，主要针对金融机构的消费者保护和金融服务中个人数据的处理。《卫生部条例第269/Menkes/Per/III/2008号》由印尼卫生部颁布，涉及医疗记录和个人健康信息的保密性和安全性。《通信和信息技术部条例第20/PER/M.KOMINFO/09/2016号》由印尼通信和信息技术部颁布，涉及电子系统运营商保护个人数据的指南。

印尼法规重点梳理

监管机构

《电子信息和交易法》(EIT Law)的监管机构是印尼通信和信息技术部 (Ministry of Communication and Information Technology，MCIT)。该部负责监督和检查电子信息和交易的合法性和安全性，主要职责包括：监督和检查电子信息和交易的合法性和安全性；制定和实施电子信息和交易的技术标准和规范；处理电子信息和交易相关的投诉和纠纷。其他相关的监管机构还包括：印尼金融服务管理局(OJK)负责监督和检查金融机构的电子信息和交易活动。印尼国家警察局(Polri) 负责调查和处理电子信息和交易相关的犯罪活动。 印尼消费者保护机构 (BPKN) 负责保护消费者在电子信息和交易中的权益。

《个人数据保护法》(PDP Law)的监管机构是印尼个人数据保护局 (Personal Data Protection Authority， PDPA)。该局负责监督和检查个人数据处理的合法性和安全性，主要职责包括：监督和检查个人数据处理的合法性和安全性；制定和实施个人数据保护的技术标准和规范；处理个人数据保护相关的投诉和纠纷；对违反个人数据保护法的行为进行调查和处罚。

数据跨境

《电子信息和交易法》(EIT Law)对数据出境有明确的要求，以确保电子信息和交易在跨境传输时的安全和合法性。主要包括：

- 数据出境必须遵循该法的规定和原则。
- 数据控制者和处理者必须确保数据出境的合法性和安全性。
- 数据控制者和处理者必须获得数据主体的同意。数据出境必须有正当理由，例如商业合作、技术支持等。
- 数据控制者和处理者必须确保数据出境的目的地国家或地区有相应的电子信息和交易保护法律和监管机制。
- 数据控制者和处理者必须向印尼通信和信息技术部提交数据出境申请，数据出境申请必须包括数据出境的目的、范围、方式等信息。印尼通信和信息技术部会审查数据出境申请，并在必要时进行调查。
- 数据控制者和处理者必须采取必要的安全措施，以保护数据出境的安全性。数据控制者和处理者必须确保数据出境的加密和访问控制。

[1]http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html
[2]https://conventuslaw.com/report/indonesia-electronic-information-and-transactions/
[3]https://fpf.org/blog/indonesias-personal-data-protection-bill-overview-key-takeaways-and-context/

《个人数据保护法》(PDP Law)对数据出境有明确的要求，以确保个人数据在跨境传输时的安全和合法性。 主要包括：

- 数据出境必须遵循该法的规定和原则。
- 数据控制者和处理者必须确保数据出境的合法性和安全性。
- 数据控制者和处理者必须获得数据主体的同意。
- 数据出境必须有正当理由，例如商业合作、技术支持等。
- 数据控制者和处理者必须确保数据出境的目的地国家或地区有相应的个人数据保护法律和监管机制。
- 数据控制者和处理者必须向印尼个人数据保护局提交数据出境申请，数据出境申请必须包括数据出境的目的、范围、方式等信息印尼个人数据保护局会审查数据出境申请，并在必要时进行调查。
- 数据控制者和处理者必须采取必要的安全措施，以保护数据出境的安全性。
- 数据控制者和处理者必须确保数据出境的加密和访问控制。

数据本地存储

《电子信息和交易法》(EIT Law)对数据本地存储有明确的要求，以确保电子信息和交易数据在印尼境内的安全和合法性。主要包括：

- 数据本地存储必须遵循该法的规定和原则。
- 数据控制者和处理者必须确保数据本地存储的合法性和安全性。
- 数据控制者和处理者必须将电子信息和交易数据存储在印尼境内。
- 数据控制者和处理者必须确保数据本地存储的安全性和完整性。
- 数据控制者和处理者必须遵循印尼的数据保护和隐私法律和监管机制。

同时，在某些情况下，数据控制者和处理者可以将电子信息和交易数据存储在印尼境外，但必须获得印尼通信和信息技术部的批准。数据控制者和处理者必须确保数据本地存储的例外符合该法的规定和原则。数据控制者和处理者必须确保数据本地存储的加密和访问控制。

《个人数据保护法》(PDP Law)对数据本地存储有明确的要求，以确保个人数据在印尼境内的安全和合法性。 主要包括：

- 数据本地存储必须遵循该法的规定和原则。
- 数据控制者和处理者必须确保数据本地存储的合法性和安全性。
- 数据控制者和处理者必须将个人数据存储在印尼境内。
- 数据控制者和处理者必须确保数据本地存储的安全性和完整性。
- 数据控制者和处理者必须遵循印尼的数据保护和隐私法律和监管机制。

同时，在某些情况下，数据控制者和处理者可以将个人数据存储在印尼境外，但必须获得印尼个人数据保护局的批准。数据控制者和处理者必须确保数据本地存储的例外符合该法的规定和原则。数据控制者和处理者必须确保数据本地存储的加密和访问控制。

个人数据保护

《电子信息和交易法》(EIT Law)对个人数据保护有明确的要求，以确保电子信息和交易中的个人数据安全和合法性。 主要包括：

- 个人数据保护必须遵循该法的规定和原则。
- 数据控制者和处理者必须确保个人数据保护的合法性和安全性。
- 数据控制者和处理者必须获得个人数据主体的同意。
- 数据控制者和处理者必须确保个人数据的准确性、完整性和安全性。
- 数据控制者和处理者必须遵循印尼的数据保护和隐私法律和监管机制。
- 数据控制者和处理者必须采取必要的安全措施，以保护个人数据的安全性。
- 数据控制者和处理者必须确保个人数据的加密和访问控制。

同时，在某些情况下，数据控制者和处理者可以不遵循个人数据保护的要求，但必须获得印尼通信和信息技术部的批准。数据控制者和处理者必须确保个人数据保护的例外符合该法的规定和原则。

《个人数据保护法》(PDP Law)规定了对个人数据保护的要求，旨在保护个人信息免受未经授权的收集、使用、披露和其他处理。PDP规定了七项个人数据保护原则：

- 个人数据的收集和处理必须有合法的依据。
- 个人数据的收集和处理必须有明确的目的。
- 个人数据的收集和处理必须是必要的。
- 个人数据的收集和处理必须与目的相符。
- 个人数据必须准确、完整和最新。
- 个人数据必须保密。
- 个人数据必须受到合适的安全措施保护。

PDP还规定了五项个人数据保护措施：

- 组织必须制定和实施数据保护政策。
- 组织必须指定数据保护官负责个人数据保护。
- 组织必须保留个人数据收集和处理记录。
- 组织必须进行数据保护影响评估。
- 组织必须在数据泄露事件发生后通知相关个人和监管机构。

PDP还规定了五项个人数据权利：

- 个人有权访问其个人数据。
- 个人有权更正其个人数据。
- 个人有权删除其个人数据。
- 个人有权反对其个人数据的处理。
- 个人有权携带其个人数据。

最后，PDP还规定了执法措施，包括调查、罚款和其他行政处罚。

▶ 印尼数据违规案例

印尼最大的电子商务平台之一在2020年3月遭遇了一起严重的数据泄露事件，导致超过900万用户的个人数据被泄露。泄露的数据类型包括用户姓名、邮箱地址、电话号码、密码哈希值等，泄露数据数量超过900万条。泄露的原因是该平台的数据库配置错误，导致数据未加密且可公开访问。

该平台确认了数据泄露事件，并通知了受影响的用户，建议他们更改密码。同时，该平台向印尼信息和通信部报告了事件，并被印尼信息和通信部罚款10亿印尼卢比（约67万美元）。此次数据泄漏事件导致该平台的声誉受损，用户信任度下降。之后，该平台升级了安全措施，以防止类似事件发生。此次数据泄露事件表明，即使是大型企业也可能出现数据泄露问题。组织和个人必须重视数据安全，采取必要措施保护用户数据。

3.5.2 新加坡

新加坡法规要求概述

2012年10月15日，新加坡颁布了《个人数据保护法》（Personal Data Protection Act，PDPA），该法是一部规范个人数据的收集、使用和披露的综合性立法。2020年11月2日，新加坡议会通过了《个人数据保护法（修正案）》，该修正案自2021年2月1日分阶段生效[1]。为了更好地执行《个人数据保护法》，新加坡还配套出台了针对特定领域（如电信业、房地产行业、教育行业、医疗行业、社会公益服务行业）的各项个人数据保护指南，以指导企业更好地对个人数据进行保护，且不断根据现实情况对指南进行修订。

另外，新加坡的《网络安全法》（Cybersecurity Act，CSA) 于2018年6月1日生效，是新加坡政府颁布的一系列法规和政策，旨在保护新加坡的网络和数字基础设施免受各种威胁和攻击，保护国家和个人免受网络攻击和数据泄露的影响。该法是落实新加坡网络安全战略的重要举措，为涉及关键信息基础设施（CII）的公司提供明确的指导方针，说明其保护CII免受网络攻击的义务[2]。

CSA 的主要内容包括：

- 加强对CII的保护，防范网络攻击，涉及CII的行业包括能源、水利、银行和金融、医疗保健、运输（包括陆地、海事和航空）、信息通信、媒体、安全和应急服务以及政府。
- 授权新加坡网络安全局预防和应对网络安全威胁和事件，并且可以根据网络安全威胁或事件的严重程度以及响应所需的措施来调整可行使的权力。
- 建立共享网络安全信息的框架。
- 为网络安全服务提供商设立许可证制度，目前仅要求提供渗透测试服务、管理网络安全营运中心服务的企业必须申请许可证。因为这两类服务提供商可以访问客户的敏感信息，对整体安全格局有重大影响。

新加坡法规重点梳理

监管机构

新加坡通讯和新闻部于2013年1月2日建立了个人数据保护委员会（Personal Data Protection Commission， PDPC）是管理和负责实施PDPL的监管机构。

新加坡网络安全局在《网络安全战略》颁布后，成为一个独立的国家机构，负责监督所有网络安全事务，包括网络安全战略、运营、教育、外展和生态系统发展。新加坡网络安全局的设立不仅能够维持对国家网络安全的集中监督和维护，保持对不同部门需求的灵活应对。

数据跨境

PDPA在2020年修订了数据跨境传输的相关规定：除非根据PDPA相关要求确保接收方对传输的个人数据提供至少与PDPA同等的保护，不得将任何个人数据传输到新加坡以外的国家或地区。该规定在《条例》中进一步细化："组织只有在采取适当措施，确保数据接收方受法律强制义务的约束，对传输的个人数据提供与PDPA同等的保护标准时，才能将个人数据向第三国转移。"实际操作中，通常建议与数据接收方签订跨境传输合同或BCRs（ Binding Corporate Rules）等文件，以确保数据的安全和隐私。 除此之外，如果个人数据传输方获得了个人数据主体关于跨境事项的有效同意、个人数据为过境中转数据或已公开数据、接收方企业具备新加坡政府要求的认证等情况，可以直接进行跨境传输个人数据。

合法性基础（满足下列其一要求）：

- 告知个人并取得有效同意。
- 个人被视为同意。
- 豁免同意中保护数据主体利益及国家利益的必要情形，并且已经采取合理措施确保数据接收方不会基于其他目的使用或披露所传输的数据。
- 个人数据过境中转，指个人数据通过新加坡传输至新加坡以外的国家或地区，且在新加坡期间未被传输服务组织及其员工以外的主体接触、使用或披露。
- 个人数据是在新加坡已公开的数据。
- 境外接收方拥有特定的数据保护认证，即 APEC PRP 或 APEC CBPR。

[1]https://www.pdpc.gov.sg/overview- of- pdpa/the- legislation/personal- data- protection- act
[2]https://www.csa.gov.sg/legislation/Cybersecurity-Act

数据本地存储

新加坡的PDPA没有强制要求数据必须本地存储（即在新加坡境内存储）。然而，PDPA对跨境数据传输有明确规定，确保个人数据在转移到其他国家或地区时仍然受到充分的保护。虽然新加坡没有强制的数据本地存储要求，但某些行业或公司可能会出于商业、法律或合规性考虑，选择在新加坡本地存储数据。这通常与对数据安全、访问速度、法律监管的方便性有关。此外，在跨境传输数据时，公司通常需要评估风险，并可能采取额外的保护措施，以确保遵守PDPA的规定。根据PDPA第26条，数据控制者在将个人数据传输到境外时，必须确保接收国的法律或安排能够提供与PDPA同等或更高的保护水平，除非获得个人明确同意或满足其他特定条件。数据控制者可以通过合同条款确保境外接收方履行与PDPA类似的保护义务。

个人数据保护

PDPA涵盖以电子和非电子格式存储的个人数据。 PDPA规定了机构在收集、使用和披露个人数据时所使用的方式需要合理且恰当，同时也承认了个人有权保护其个人数据，且拥有对个人数据的各项权利[1]。

PDPA 个人数据保护义务：

- **同意义务**：组织在采集、使用或披露某人的个人数据之前必须事先获得其同意。
- **目的限制义务**：组织采集、使用或披露个人数据时的目的必须合理。
- **告知义务**：组织在收集、使用或披露个人数据时或之前必须将目的告知相关个人。
- **许可访问和更正义务**：组织有义务应个人要求告知自己所掌握的其个人数据和在过去一年中可能使用或披露其个人数据的记录；并应个人要求更正或补正其个人数据。
- **准确性义务**：组织如果可能需要在其决策中参考相关个人数据或者可能需要向其他组织披露的，必须通过合理方式保证其收集或受托收集的个人数据准确、完整。
- **保护义务**：组织必须通过合理的安全措施防止其掌握的个人数据被非法获取、收集、使用、披露、复制、修改等风险，并防止储存个人数据的媒介或设备丢失。
- **保留限制义务**：组织可以合理假设所保留的个人数据已不能实现相关目的，或者继续保留相关个人数据已无法律或商业意义时，必须立即删除相关个人数据。
- **传输限制义务**：组织在将个人数据传输至新加坡境外地点时，必须遵守 PDPA 相关规定。
- **数据泄露通知义务**：组织认为发生个人数据泄露，且经过评估认为符合 PDPA 规定的条件时，必须向受影响的委员会和有关个人通知。
- **谢绝来电义务**：组织不得向“谢绝来电”登记簿上的号码拨打营销电话、发送营销信息或传真。
- **责任制义务**：组织对自己拥有或控制的个人数据承担责任，需就此满足PDPA 规定的合规义务，包括任命数据保护官（DPO）、制定和实施数据保护政策和操作流程、在规定场合进行个人数据影响评估（DPIA）等。

▶ 新加坡数据违规案例

违反PDPL的法律后果

PDPA对违反数据保护义务规定了比较严格的处罚，包括刑事犯罪、行政处罚、民事责任三个方面。

- **刑事责任**：未经授权披露、使用个人数据，或未经授权重新识别匿名数据，可能面临最高5000新加坡元罚款和2年监禁。在已经构成犯罪但未明确规定处罚的场合，可能按照第56条，在定罪后处以不超过10,000新加坡元的罚款或不超过3年的监禁，或两者兼施。
- **民事责任**：个人可以依据 PDPA中 PART 9C 第480 条保护自己的个人数据，向法院提起诉讼，请求赔偿损失或获得其他民事救济。
- **行政责任**：委员会有权对违反PDPA的组织进行惩罚，包括要求违法的组织：（1）停止违法收集、使用或披露个人数据，销毁违法收集的个人数据；（2）警告；（3）指令；（4）经济处罚。对于违反信息保护义务的自然人处以20万新加坡元以下处罚；对其他组织最高处以1百万新加坡元以下或年营业额10%以下的经济处罚（二者取高者）。

[1]https://sso.agc.gov.sg/Act/PDPA2012?WholeDoc=1

新加坡某私人有限公司的病例数据库系统遭到网络攻击，黑客从公司数据库中非法访问和复制近150万病人的个人数据和近160万门诊病人的处方记录，导致大规模的病人数据泄露。PDPC遂依受害人的投诉启动了调查程序，并在综合考虑证据、当事人陈述，以及公司方面事后所采取的有效补救措施等减轻情节后，对该公司和综合健康信息系统公司分别作出了25万新加坡元（约125万元人民币）和75万新加坡元（约375万元人民币）罚款指令。

PDPC认为，该公司作为医疗机构可以将部分业务外包给服务供应商，但不能将其PDPA规定的法定义务亦转移给他人。上述两公司最终自愿承认病例数据遭到泄露的事实，接受个保委的调查结果，同意按照个保委的指令承担责任，并认为上述指令的处罚力度合理适当。迄今为止，PDPC 对组织施加的最大罚款(75 万新元)是由于该组织未能采取足够的安全措施或作出必要安排，以保护个人数据免遭未经授权的访问。

违反CSA的法律后果

新加坡CSA法规规定，违反CSA法规的组织可能承担法律责任，包括因违反法规而导致的损失或损害。

- 个人和组织违反法规可能遭受罚款，最高罚款为新加坡元100,000元，还可能面临监禁，最高监禁期为6个月。
- CSA法规提供了对违反法规组织的监管行动，包括暂停或吊销许可证和许可证。在某些情况下，个人违反CSA法规可能面临刑事诉讼。

2018年，新加坡的某银行受到黑客攻击，导致超过130,000名客户的个人数据泄露，受影响的数据包括客户的姓名、身份证号、联系方式、地址、银行卡号和密码等信息。这些数据可能会被黑客攻击者用于非法活动，例如身份盗用、银行卡盗用等。事件的原因是该银行的一些系统中发现了漏洞，黑客攻击者能够访问和盗取客户的个人数据。

该银行未能采取合理的步骤来保护客户的个人数据，未能及时通知受影响的客户，未能采取合理的步骤来防止数据泄露。因此，该银行的数据泄露事件违反了新加坡《网络安全法》的多项规定，导致了该银行受到新加坡数据保护局的罚款新加坡元13,000元。事件也导致了该银行的名誉损害和客户信任度的下降。

3.5.3 泰国

泰国法规要求概述

泰国针对所有行业比较重要的法规是个人数据保护法（Personal Data Protection Act，PDPA），于2022年6月正式生效，适用于在泰国境内收集、使用或披露个人数据的组织和个人。主要内容是规定了个人数据的保护原则、数据主体权利、数据控制者和数据处理者的义务等。PDPA借鉴了GDPR的立法模式，共分为七章，涉及数据主体权利、数据处理者义务、跨境数据传输、滥用个人数据处罚等方面。从立法目的来看，PDPA体现出泰国作为东盟经济体在自由贸易方面的考量[1]。

另外，泰国针对一些行业也制定了个人信息和数据安全法规，例如：电信法（Telecom Act），于2001年生效，适用于在泰国境内提供电信服务的组织和个人，规定了电信服务的法律框架，包括电信许可、电信服务质量等。计算机犯罪法（CCA），于2007年生效，适用于在泰国境内发生的计算机犯罪行为，规定了计算机犯罪的类型和处罚，包括数据泄露、网络攻击等。数字经济和社会发展法（DESDA），于2017年生效， 适用于在泰国境内发展数字经济和社会的组织和个人，规定了数字经济和社会发展的法律框架，包括数字基础设施、数字服务等。

泰国法规重点梳理

监管机构

泰国PDPA的监管机构是泰国个人数据保护委员会（PDPC）。PDPC的职责主要包括：负责监管个人数据保护，包括调查、罚款和其他行政处罚。负责制定个人数据保护政策和指南。负责提供个人数据保护咨询和培训。PDPC的权力主要包括：有权调查个人数据泄露事件和其他违反PDPA的行为。有权对违反PDPA的行为处以罚款。有权对违反PDPA的行为采取其他行政处罚。

数据跨境

泰国PDPA关于数据出境的定义是指将个人数据从泰国境内传输到泰国境外。数据出境必须符合四项条件：

- 数据控制者必须获得数据主体的同意方可进行数据出境。
- 与境外数据接收者签订合同。
- 数据控制者必须与境外数据接收者签订合同，规定数据接收者必须遵守泰国个人数据保护法的规定。
- 数据控制者必须确保数据接收国有适当的个人数据保护水平。

同时，PDPA也规定了数据出境的三种例外情况，不需要遵守数据出境的规定：

- 数据主体同意数据出境的。
- 数据出境是为了执行合同。
- 数据出境是为了保护公共利益。

数据出境必须执行的安全措施包括：数据控制者必须对数据进行加密，以防止数据泄露；数据控制者必须与数据接收者签订安全协议，以确保数据的安全。泰国的数据保护委员会负责监督数据出境的活动，数据控制者必须向数据保护委员会报告数据出境的活动。

数据本地存储

泰国PDPA对数据本地存储的要求主要有三条：

- 关键信息基础设施的运营者必须将个人数据存储在泰国境内。
- 公共部门必须将个人数据存储在泰国境内。
- 私营部门可以选择将个人数据存储在泰国境内或境外，但必须遵守PDPA的规定。

同时，PDPA也规定了数据本地存储的三种例外情况，不需要遵守数据本地存储的条件：

- 数据主体同意数据存储在境外的。
- 数据存储是为了执行合同的。
- 数据存储是为了保护公共利益的。

数据本地存储必须执行的安全措施包括：数据控制者必须对数据进行加密，以防止数据泄露；数据控制者必须与数据存储服务商签订安全协议，以确保数据的安全。泰国的数据保护委员会负责监督数据本地存储的活动，数据控制者必须向数据保护委员会报告数据本地存储的活动。

个人数据保护　泰国PDPA旨在保护个人数据免受未经授权的收集、使用、披露和其他处理。内容主要包括：

- **定义**
  - 个人数据：指与个人有关的任何信息，包括姓名、地址、电话号码、电子邮件地址等。
  - 数据主体：指个人数据的所有者，即个人。
  - 数据控制者：指决定个人数据处理目的和方式的组织或个人。
  - 数据处理者：指代表数据控制者处理个人数据的组织或个人。
- **个人数据保护原则**
  - 合法性原则：个人数据的收集和处理必须有合法的依据。
  - 目的明确原则：个人数据的收集和处理必须有明确的目的。
  - 必要性原则：个人数据的收集和处理必须是必要的。
  - 比例原则：个人数据的收集和处理必须与目的相符。
  - 准确性原则：个人数据必须准确、完整和最新。
  - 保密性原则：个人数据必须保密。
  - 安全性原则：个人数据必须受到合适的安全措施保护。
- **数据主体权利**
  - 访问权：数据主体有权访问其个人数据。
  - 更正权：数据主体有权更正其个人数据。
  - 删除权：数据主体有权删除其个人数据。
  - 反对权：数据主体有权反对其个人数据的处理。
  - 携带权：数据主体有权携带其个人数据。
- **数据控制者和数据处理者义务**
  - 数据保护政策：数据控制者必须制定和实施数据保护政策。
  - 数据保护官：数据控制者必须指定数据保护官负责个人数据保护。
  - 数据收集和处理记录：数据控制者必须保留个人数据收集和处理记录。
  - 数据保护影响评估：数据控制者必须进行数据保护影响评估。
  - 数据泄露通知：数据控制者必须在数据泄露事件发生后通知相关个人和监管机构。

▶ 泰国数据违规案例

泰国的一家电信运营商于2020年遭遇了一起严重的数据泄露事件，包括超过460万条用户姓名、手机号码、电子邮箱地址等数据。泄露原因是该运营商的数据库配置错误，导致数据未加密且可公开访问。该运营商通知了受影响的用户，并建议他们更改密码，并向泰国国家广播和电信委员会报告了事件。该运营商被泰国国家广播和电信委员会罚款100万泰铢（约3.3万美元），也导致了声誉受损，用户信任度下降。

另外，泰国的一家电子商务平台也于2019年遭遇了一起严重的数据泄露事件，包括超过10万条的用户姓名、邮箱地址、电话号码等。此次事件的原因同样也是该平台数据库配置错误，导致数据未加密且可公开访问。该平台被泰国电子商务委员会罚款50万泰铢（约1.65万美元），声誉受损，用户信任度下降。这些案例表明，数据合规违规可能导致严重的后果，组织和个人必须遵守泰国数据合规法规的规定，以确保个人数据的安全和保护。

3.5.4 越南

越南法规要求概述

2023年4月17日，越南政府正式发布No：13/2023/ND-CP法令，即《个人数据保护法令》[1]（Personal Data Protection Decree，PDPD），于2023年7月1日起正式生效。

越南个人数据保护法具有域外效力，在越南境外直接参与或涉及越南个人数据处理活动的外国机构、组织和个人同样受该法规管辖。根据规定，越南个人数据保护法适用于：

- 越南的机构、组织和个人。
- 在国外经营的越南机构、组织和个人
- 在越南的外国机构、组织和个人。
- 直接参与或涉及越南的个人数据处理活动的外国机构、组织和个人。

在法规的适用方面，法规第43条特别指出，微型企业、小型企业、中型企业、初创公司在其成立之日起的两年内有权选择豁免任命数据保护负责人和负责部门的义务，但上述企业中直接从事个人数据处理活动的除外。

越南法规重点梳理

监管机构　越南与个人数据保护相关的主要监管机构包括公安部、信息和通信部、国防部和科技部等，其中最主要的监管机构是公安部。

数据跨境　越南个人数据保护法针对个人数据跨境传输所制定的合规要求和合规机制具有一定独特性，与欧盟以及周边的泰国、马来西亚等国家所采取的合规机制也有较大差别。

根据越南个人数据保护法的规定，越南实体从越南向境外传输数据，必须同时满足下述条件：

- 数据传输方就个人数据跨境传输开展影响评估，评估需包括以下内容：
  - 个人数据传输方和接收方的详细信息和联系方式。
  - 个人数据传输方旗下参与传输和接收越南公民个人数据的组织或个人的全名和联系方式。
  - 描述和解释个人数据跨境传输后对越南公民个人数据处理活动的目的。
  - 描述并阐明跨境传输的个人数据的类型。
  - 描述并说明跨境传输活动遵守越南个人数据保护法中关于个人数据保护规定的情况，以及所采取的具体个人数据保护措施。
  - 评估个人数据处理的影响，跨境传输可能造成的负面后果和损害，以及减少或消除此类后果和损害的措施。
  - 越南个人数据保护法第11条规定的个人数据主体（越南公民）在已得知出现问题/需求时的反馈/投诉机制的基础上，给予同意。
  - 数据传输方和接收方之间的关于处理越南公民个人数据的保护义务和责任的相关文件。
- 个人数据跨境传输影响评估档案应当随时备存，以供越南公安部检查和评估。此外，数据输出方应在处理个人数据之日起60天内，根据越南个人数据保护法附件第06号表格，向越南公安部（网络安全和高科技犯罪预防司）发送一份真实的评估副本。
- 数据输出方应在个人数据传输完成后，将数据传输的相关信息及负责传输的组织或个人的联系方式以书面形式通知越南公安部（网络安全和高科技犯罪预防司）。
- 越南公安部（网络安全和高科技犯罪预防司）应当进行评估，并在数据跨境传输影响评估根据相关法规不完整、不准确的情况下，要求数据输出方完善个人数据跨境传输影响评估档案。此外，数据输出方应在提交公安部（网络安全和高科技犯罪预防司）的个人数据跨境传输影响评估档案内容发生变化时，对其进行更新和修改。数据输出方应在内容发生变化之日起10天完成对评估档案的更新。
- 除特殊情况外，越南公安部可根据具体情形，决定每年对个人数据跨境传输活动进行一次检查。此外，有下列情形之一的，越南公安部可以决定要求数据输出方停止向境外传输个人数据：
  - 被传输的个人数据用于危害越南国家利益和国家安全的活动。
  - 数据输出方未遵守前述在数据跨境传输影响评估档案不完整、不准确的情况下完善评估档案和内容发生变化时更新和修改评估档案的规定。
  - 越南公民的个人数据被泄露或丢失。

数据本地存储

2022年8月15日，越南就2018年6月颁布的《网络安全法》发布数据处理法令。这项法令(第53/2022/ND　CP号法令)于2022年10月1日生效，规定在该国经营的公司必须于当地储存数据。

向越南客户提供跨境服务的公司必须在越南设立实体，并在该国储存数据。法令涵盖的活动包括：在网络储存和共享数据；电讯服务；电子商贸；提供域名；网上支付；社交网络和媒体；支付中介；网上游戏；提供、管理或操作电邮、短讯、电话、视频通话或网上聊天；以及网络传输连接。服务用户的个人数据和用户产生的数据同样受规管。

违反规定的外国企业会接到书面通知，该等企业须于12个月内在越南设立办事处并于当地储存数据。数据必须保存至少24个月，系统日志则至少保存12个月。越南当局或许会出于多种原因要求企业删除某些内容。

个人数据保护

越南个人数据保护法对各方主体的角色划分采用了与欧盟GDPR类似的概念和结构，将数据相关主体角色划分为“数据主体”、“个人数据控制者”、“个人数据处理者”、“个人数据控制者兼处理者”。

越南个人数据保护法将个人数据划分为一般个人数据与敏感个人数据。一般个人数据包括：姓名、性别、出生日期、出生地、个人照片、身份证号码、护照号码、驾驶执照、个人税号、婚姻状况以及有关家庭关系的信息等。敏感个人数据包括：政治观点、宗教观点、病历中所记载的健康状况及性取向等。

数据主体享有11项权利，包括知情权，同意权，访问权，撤回同意权，删除权，限制数据处理的权利，获得数据的权利，反对数据处理的权利，投诉、检举和提起诉讼的权利，索赔权，自我保护权。

在告知同意机制的设计方面，越南对告知同意的内容、方式等具体要求给出了较为细致的规定。越南个人数据保护法明确规定：

- 数据主体的沉默或不回应不被视为同意。
- 数据主体可以给予部分或有条件的同意。
- 在发生争议的情况下，个人数据的控制者、个人数据控制者兼处理者应该证明已获得数据主体的同意。

越南数据违规处罚案例

数据处理者违法违规处理个人数据，需要承担法律责任。根据违法行为的类型，基本罚款金额从4,000万越南盾到2亿越南盾不等。根据违法行为的严重程度，公司可被处以基本罚款金额的2-5倍，金额最高可达到企业上一财年收入或在越南境内所取得的利润的5%。

对于需要收集个人数据的行业，可能会受到吊销营业执照三个月的处罚。该处罚还适用于以下情况：在数据主体撤回同意后，未停止处理其个人数据。未编制数据处理影响的评估。违反个人数据安全性/保密性规定，可能会面临警告、罚款甚至最高3年监禁等刑事处罚。

2022年12月，越南的两家金融公司的3,848份客户数据遭到泄露，罪犯通过出售客户个人信息获得总金额为458,952,000越南盾（约合18,825 美元）的非法所得。该罪犯被处以1 亿越南盾（4,100 美元）的罚款，没收非法所得，并被判决缓刑二十四个月[2]。

[1]https://baovedlcn.gov.vn/

[2]https://www.tilleke.com/insights/with-illicit-personal-data-trading-on-the-rise-vietnam-seeks-solutions/

3.5.5 马来西亚

马来西亚法规要求概述

马来西亚的数据保护法律法规体系主要包括2010年《个人数据保护法》（Personal Data Protection Act 2010，PDPA）及其相关配套规定，该法案于2013年11月15日生效[1]。

2010年《个人数据保护法》规定了商业交易中个人数据的处理，并适用于：

- 处理数据的任何人。
- 控制或授权处理与商业交易有关的任何个人资料的人。

《个人数据保护法》包含七个数据保护原则：通用原则、通知和选择原则、披露原则、安全原则、保留原则、数据完整性原则和访问原则。这些原则将为个人数据提供保护，也为消费者、电子商务、网络及非网络设施从业人员的利益提供保障。

马来西亚法规重点梳理

监管机构

马来西亚的通讯及多媒体部成立了个人数据保护部，并任命一位个人数据保护专员来负责监督用户的数据，以监督《个人数据保护法》的实施。该专员由部长任免，任期为三年，可以连任。

数据跨境

《个人数据保护法》第129条禁止向马来西亚境外转移个人数据，除非经相关官员允许传输至指定的地方，或者符合以下条件（必须符合至少一项）：

- 数据主体书面同意。
- 为了履行数据主体与数据用户之间的合同所必需。
- 为了履行数据主体与第三方之间的合同所必需。
- 为执行法律程序或为了确立、行使或捍卫合法权利。
- 避免针对数据主体的不利行为或减轻类似行为造成的影响。
- 数据使用者已采取合理的预防措施和尽职调查。
- 为保护数据主体的利益或符合公共利益所必需。

2023年1月30日，马来西亚与新加坡就数字经济和绿色经济达成两项合作框架协议。在其中的数字经济合作框架协议中，双方就实施可互操作的个人数据保护框架、企业数字身份双边试点等举措开展合作。

2023年8月，马来西亚个人数据保护专员同新加坡和菲律宾一道被接纳为亚太经合组织(APEC)跨境隐私执法安排(CPEA)的成员。目前，马来西亚个人数据保护专员正在积极准备参与亚太经合组织跨境隐私规则(CBPR)。

数据本地存储

马来西亚没有规定数据必须存储在本地，但对数据跨境传输有明确规定（如上）。

[1]https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en

个人数据保护

马来西亚《个人数据保护法》范围内的“个人数据”必须直接或间接地涉及到个人，披露用户的身份或其它信息，而且该数据必须由自动化工具处理或意图被记录而形成相关文件系统的一部分。这些数据需透过商业交易而被收集，如销售商品或服务的供应。

《个人数据保护法》禁止在未经个人同意的情况下私自处理数据，严格地保护了个人数据。对于18岁以下的数据所有人，数据使用者应就处理其个人数据取得其父母、监护人或对数据所有人负有监护责任的人的同意。同时也对特定情况下，数据处理规定了相应的免责条款。免责条款适用于以下情形：

- 签订的合同中允许处理个人数据。
- 符合其他法规义务。
- 保护数据所有者最大利益。
- 执法或履行法律职能。

马来西亚《个人数据保护法》第9节和《个人数据条例》第6条规定了安全原则。安全原则要求数据用户在处理个人数据时，应采取相关切实措施保护个人数据不受任何丢失、误用、修改、未经授权或意外访问或泄露的影响。如：确保个人资料存放的地点安全；确保有权接触该等个人资料的人员的可靠性、完整性及能力而采取的措施；确保该等个人资料的能够安全转移等。

马来西亚数据违规案例

2024年7月4日，马来西亚内阁批准PDPA 2010的拟议修正案。该修正案提高了违规的处罚力度。违反《个人数据保护法》的七项数据保护原则，可能受到罚款和/或监禁的处罚。罚款范围最高可达100万令吉（约168万元人民币），而监禁最多可达3年。

近年来，马来西亚发起了多起数据泄露事件。2022年12月30日，马来西亚某银行遭遇数据泄露，影响了1300万账户持有人。这些信息发布在一个在线数据库市场上还发布了一个单独的列表，卖家声称拥有互联网提供商Unifi移动客户的个人数据库。2022年9月，马来西亚某航空公司遭遇数据泄露，4500万客户的电子邮件地址、出生日期、地址、护照号码和电话号码在网上被泄露[1]。然而，自2017年以来，只有20家公司因数据泄露被罚款，平均每家公司被罚款24,000林吉特（约合5,480美元）[2]。

[1]https://cybersecurityasean.com/daily-news/recurring-data-breaches-malaysia-plain-ignorance-or-just-weak-enforcement
[2]https://www.freemalaysiatoday.com/category/nation/2023/01/03/only-20-companies-fined-for-data-breaches-since-2017/

印度 3.6

3.6.1 印度法规要求概述

2023 年 8 月 11 日，印度议会颁布了《数字个人数据保护法案》（the Digital Personal Data Protection Act， DPDP Act），这是印度第一部全面的数据保护法案，取代之前2000、2008、2011年的相关规定[1]。

《DPDP 法案》适用于所有数字个人数据的处理，无论是以数字形式收集，还是以非数字形式收集后再数字化。该法案不仅适用于印度境内的数字个人数据处理，也适用于印度境外的数字个人数据处理，特别是对居住在印度的数据主体提供商品或服务有关的数字个人数据处理。

DPDP与 GDPR 有两个明显的不同之处：

- 第一，DPDP法案不承认将合法利益或合同必要性作为收集或处理个人信息（PI）的有效法律依据，而是需要征得数据主体的同意。但出于就业目的或在某些紧急情况下处理PI的情况除外。
- 第二，DPDP法案设想了一个“同意管理人consent manager”，该管理人应在印度数据保护委员会注册，并作为一个联络点，使数据主体能够给予、管理、审查和撤回其同意。

另外，DPDP法案要求企业为数据主体提供以英语或印度宪法承认的22种语言中的任何一种查看同意通知的选项。DPDP还要求企业向之前已同意个人数据处理的数据主体提供通知。通知说明将收集哪些个人数据、处理这些数据的目的、数据主体如何就这些数据行使其权利，以及相关数据保护官或数据控制者负责回应数据主体行使其权利的请求的其他负责人的详细联系信息。

3.6.2 印度法规重点梳理

监管机构

DPDP法案的监管机构是印度数据保护局（Data Protection Authority of India，DPAI）。DPAI是一个法定机构，负责监督和执行DPDP法案的规定。DPAI有权调查投诉，进行审计，并对不遵守法案的行为进行处罚。

数据跨境

DPDP法案允许将个人数据传输到印度境外，但必须得到数据主体（与数据相关的个人）的明确同意。此外，数据受托人必须确保数据传输到的国家/地区具有与印度相似的数据保护水平。

另外，DPDP法案授权中央政府通知某些国家为跨境数据传输的“批准司法管辖区”。数据可以传输到这些国家/地区，而无需获得数据主体的明确同意。该法案还允许使用示范合同条款，这些条款是标准化的合同条款，可确保在向数据保护水平不如印度的国家/地区传输数据时提供充分的数据保护保障。

在某些情况下，印度数据保护局(DPAI) 可能需要批准跨境数据传输，特别是如果传输到的国家/地区的数据保护水平不如印度。这些规定旨在促进数据跨境自由流动和确保保护印度公民的个人数据之间取得平衡。

[1]https://www.meity.gov.in/content/digital-personal-data-protection-act-2023

数据本地存储

DPDP法案要求所有敏感个人数据（Sensitive Personal Data）和关键个人数据（Critical Personal Data）都存储在印度，不能传输到印度境外。其中，敏感个人数据定义为包括与健康、财务信息、密码和其他敏感信息相关的个人数据。关键个人数据的定义包括对印度的主权和完整、国防和国家安全至关重要的个人数据。

同时，DPDP法案允许对敏感个人数据和关键个人数据的数据本地化要求有某些例外，例如在数据主体明确同意的情况下，或者出于法案中规定的出于国际合作、研究或法案等其他目的需要传输。这些规定旨在确保印度公民的敏感和关键个人数据存储在该国境内，同时允许在个人同意的情况下传输其他个人数据。

DPDP法案并未对其他个人数据（即非敏感或关键的个人数据）施加任何存储限制。经数据主体明确同意，组织可以将其他个人数据转移到印度境外。

个人数据保护

首先，DPDP法案赋予了数据主体五项权利：

- **知情权：**数据主体有权被告知其个人数据的收集、处理和使用。
- **访问权：**数据主体有权访问其个人数据并获取其副本。
- **更正权：**如果个人数据不准确或不完整，数据主体有权更正其个人数据。
- **删除权：**在某些情况下，数据负责人有权删除其个人数据，例如当数据不再需要用于收集数据的目的时。
- **数据可移植性的权利：**数据委托人有权将其个人数据从一个数据受托人移植到另一个数据受托人。

同时，DPDP为数据受托人也规定了五项义务：

- **透明度：**数据受托人必须对其数据收集和处理实践保持透明。
- **目的限制：**数据受托人只能出于特定、明确和合法的目的收集和处理个人数据。
- **数据最小化：**数据受托人只能收集和处理为收集目的所必需的个人数据准确性。
- 数据受托人必须确保他们收集和处理的个人数据是准确和最新的数据安全。
- 数据受托人必须实施适当的技术和组织措施，以确保个人数据的安全。

DPDP法案对不遵守其规定的数据受托人处以处罚，包括罚款和监禁。数据主体有权要求赔偿因数据泄露或不遵守本条例而遭受的任何损害或损失。这些规定旨在通过建立强大的数据保护框架来保护印度公民的个人数据，并确保数据受托人对其数据收集和处理实践负责。

另外，DPDP为重要数据受托人（SDF，Significant Data Fiduciary）规定了更高的义务。SDF指中央政府根据对以下因素评估而被通知为的数据受托人：所处理的个人数据的数量和敏感性、对数据委托人权利的风险、对印度主权和完整的潜在影响、对选举民主构成风险、国家安全、公共秩序。SDF在DPDP法案下承担了更高的义务，包括：完成数据保护影响评估，任命一名数据保护官，任命独立（第三方）审计师进行数据审计，并评估SDF是否遵守法律。

3.6.3 印度数据违规案例

2021年4月，印度一家全球知名的披萨连锁店因安全漏洞导致数据泄露，涉及数十万用户的个人数据，包括姓名、电子邮件地址、手机号码、地址等。数据泄露原因是该连锁店的第三方服务提供商使用了不安全的协议和密码，导致黑客能够轻松访问用户数据。此数据泄露事件对该连锁店的用户造成了严重影响，许多用户收到了诈骗邮件和短信。同时，数据泄露事件也对该连锁店的品牌声誉造成了严重损害，许多用户表示不会再使用连锁店服务。

数据泄露事件后，该连锁店采取了安全措施，防止进一步的数据泄露。包括更改密码、更新安全协议等，并通知了受影响的用户，提醒他们注意个人数据安全。印度政府和监管机构对该连锁店施加了严厉的处罚，包括罚款和安全整改要求。该数据泄露案例告诉我们：企业必须高度重视数据安全，采取有效措施保护用户数据；企业必须严格评估第三方服务提供商的安全风险，确保他们能够保护用户数据；企业必须使用安全的协议和密码，防止黑客攻击；企业必须能够快速有效地进行内部调查，确定数据泄露的原因和范围；企业必须与政府和监管机构合作调查数据泄露事件，确保用户数据安全。

俄罗斯 3.7

3.7.1 俄罗斯法规要求概述

俄罗斯个人数据保护类法律法规主要是2006年通过的第152-FZ号联邦法律（Federal Law No.152-FZ，PD Law），它是俄罗斯个人数据保护的关键法律[1]。PD Law在某些方面的制定参考了隐私和数据保护的国际法律文件如欧盟《一般数据保护条例》（GDPR）中的概念。PD Law适用于任何处理俄罗斯公民个人数据的数据运营商，无论其是否位于俄罗斯。

另外，还有一些具体的数据保护条款可以在俄罗斯其他法律中找到，包括Russian Labour Code《俄罗斯劳动法》第14章（2001年）、Russian Air Code《俄罗斯航空法》第85.1条（1997年）、Federal Law No.395-1 On Banks and Banking《关于银行和银行业的第395-1号联邦法》（1990年）、Federal Law No.323-FZ on the Fundamentals of Protection of the Health of Citizens in the Russian Federation《关于保护俄罗斯联邦公民健康基本原则的第323-FZ号联邦法》（2011年）、Federal Law No.38-FZ on Advertising《关于广告的第38-FZ号联邦法》（2006年）、Russian Administrative Offences Code《俄罗斯行政犯罪法》（2001年）等。

3.7.2 俄罗斯法规重点梳理

监管机构

俄罗斯主要的数据保护监管机构是联邦通信、信息技术和大众传播监督局（Roskomnadzor），数据保护领域的专门政府机构还包括联邦技术和出口管制局（FSTEK）和联邦安全局（FSS）。数据运营商在开始处理任何个人数据之前，应通知Roskomnadzor，并且数据运营商的细节应记入个人数据运营商的公共登记册。

数据跨境

在个人数据跨境转移的情况下，数据运营商在跨境传输前必须确保相关数据主体的权利和利益在相应的外国以适当的方式adequate manner得到充分保护adequate protection。（Article 12 of the PD Law）。

所有签署《斯特拉斯堡公约》的缔约国家都被认为是为数据主体的权利和利益提供“充分保护adequate protection”的管辖区。此外，Roskomnadzor还通过了一份官方清单，列出了非《斯特拉斯堡公约》缔约国但在个人数据跨境转移方面确保“充分保护（adequate protection）”的国家。向任何具有 "充分保护 "水平的司法管辖区进行的国际数据转移不受任何限制，前提是数据运营商已收到各自数据主体的事先同意。 此外，PD Law规定了向不提供“充分保护”水平的国家跨境转移个人数据的特殊要求。

在实践中，在将个人数据转移到国外之前，数据运营商应首先检查各外国管辖区的数据保护水平。此外，为了将个人数据转移到其他司法管辖区，需要事先获得相关数据主体的书面同意。 数据运营商也可以与个人数据主体签署国际数据传输协议。

数据本地存储

PD Law规定了本地数据存储要求，适用于任何处理俄罗斯公民个人数据的数据运营商，包括其在线商业活动例如通过互联。在收集个人数据时，经营者须满足通过使用一个实际位于俄罗斯联邦的任何数据库来记录、安排、积累、储存、指定（更新、更改）或检索俄罗斯联邦公民的个人数据，但以下情况除外(Article 18(5) of the PD Law)：

- 为实现国际条约的目标或执行经营者的法定权力和义务而进行的数据处理。
- 用于国家目的。
- 为记者的专业活动或大众媒体的合法活动提供服务。
- 可直接在外国数据库中进行的科学、文学或其他创造性活动。

[1]https://secureprivacy.ai/blog/comprehensive-guide-russian-data-protection-law-152-fz#:~:text=The%20Federal%20Law%20on%20Personal%20Data%20%28No.%20152-FZ%29%2C,then%2C%20the%20most%20recent%20being%20in%20February%202023.

个人数据保护

数据运营商或其他获得个人数据的实体有义务在未经个人数据主体事先书面同意的情况下不向第三方披露这些数据或传播这些个人数据，但联邦法律规定的情况除外。

一般来说，没有向数据保护机构报告数据泄露的法律要求。俄罗斯Roskomnadzor应审查个人数据主体自愿提出的有关个人数据内容的兼容性compatibility、存在或缺乏个人数据主体的同意、个人数据处理方法及其是否符合所宣称的处理目的。 Roskomnadzor应对此作出适当的决定，如果发现违规，数据运营商必须在三个工作日内终止这种未经授权的处理。如果不可能将未经授权的个人数据处理变成合法的处理方式，数据运营商必须在10个工作日内销毁这些个人数据（Article 21(3) of the PD Law）。数据运营商必须在终止处理或销毁个人数据时通知数据主体或其代表，如果终止或销毁的要求是由Roskomnadzor提出的，则必须将这种通知发送给Roskomnadzor。

没有特别的法律规定要向受影响的数据主体报告数据泄露事件。但是，权利受到侵犯的个人数据主体有权向Roskomnadzor提交索赔调查申请，Roskomnadzor可以行使相关的调查，并对被指控的侵权者及其对个人数据的未经授权的行为作出索赔决定。

数据运营商可能会对几种违反个人数据处理的行为负责——包括在需要时未经数据主体书面同意的数据处理，未在网站上公布数据处理政策，或未向数据主体提供与处理其个人数据有关的信息——犯罪的罚款最高可达75000卢布（The Russian Code for Administrative Offences《俄罗斯行政犯罪法》第13.11（2）条）。

违反本地存储要求的数据运营商会被处以罚款，初犯者最高罚款600万卢布，再犯者最高罚款1,800万卢布（The Russian Code for Administrative Offences《俄罗斯行政违法法典》第13.11条8 & 9款）。

The Russian Criminal Code《俄罗斯刑法典》规定了以下行为的刑事责任：未经个人同意，非法收集或传播，包括公开传播与个人或家庭秘密有关的个人资料，最高可处以20万卢布的罚款；非法访问计算机信息，造成个人数据的破坏、封锁、修改或复制，最高可处以50万卢布的罚款。特别要指出的是，根据俄罗斯法律，刑事处罚只能针对个人，而不能针对法律实体。

3.7.3 俄罗斯数据违规案例

2024年7月31日，俄罗斯对中国某领先社交平台开出了一张400万卢布（约合33.6万元人民币）的行政罚款，原因是该平台未能遵守俄联邦通信、信息技术和大众传媒监督局的指示。2024年5月，俄联邦通信、信息技术和大众传媒监督局要求该平台提供涉及俄联邦“个人数据”和“信息、信息技术和信息保护”信息，证明其遵守俄罗斯通信与传媒的相关法律。

2022年，数家外企因违反俄罗斯数据管理规定而被处以100万–200万卢布（约合3.77万美元）不等的罚款，其中包括美国某游戏直播平台、某社交媒体网站、某旅游住宿网站、某包裹运送服务公司。

日韩 3.8

3.8.1 日本

日本法规要求概述

日本的《个人信息保护法案》（Act on the Protection of Personal Information，APPI）于2003年颁布，并于2022年4月1日修订生效，是日本一部全面的数据保护法。APPI适用于位于日本的处理个人信息（PI）的控制者和处理者，以及位于日本境外，处理与向位于日本的数据主体提供商品或服务相关的个人信息的控制者和处理者[1]。

APPI与GDPR相似之处在于它授予个人有关其PI的权利，规定了数据治理义务（例如数据最小化和数据安全性）、加强对敏感PI的保护以及对国际数据传输的要求。 但是，APPI在两个关键方面与 GDPR不同：它在控制者和处理者之间没有明确的区别，并且PI的处理不需要法律依据（SPI 除外）；它还将假名和匿名处理的信息分类为具有自身特定要求的PI子集。

另外，2016年1月生效的《日本个人编号法》（My Number Act，MNA）补充了《个人信息保护法案》。在日本，所有注册居民都会获得一个称为“个人编号”的号码，用于社会福利和税收目的。MNA规定了包含“个人编号”或用作个人编号替代品的任何数字、标记或代码的信息的处理，包含此类数据的个人信息在 MNA中被定义为“特定个人信息（SPI）”。MNA 适用于位于日本境内和境外处理SPI的控制者和处理者[2]。

MNA要求MNA SPI仅用于社会保障、地方税收和灾害预防目的进行处理，控制者对处理者进行适当的监督，并且处理协议中包含特定条款，包括处理者和子处理者只有在控制者事先明确同意的情况下才能任命。《多边核协议》对应通报数据事件的定义也设定了较低的门槛。请注意，处理MNA SPI的控制者和处理者也必须遵守APPI。

日本法规重点梳理

监管机构

日本APPI法案的监管机构是个人信息保护委员会（Personal Information Protection Commission，PPC）。PPC是一个独立的行政委员会，成立于2016年，负责监督和执行APPI。PPC总部设在东京，并在日本各地设有区域办事处。它负责确保个人信息得到日本企业和组织的适当保护和处理。

日本MNA法案的监管机构是总务省（Ministry of Internal Affairs and Communications，MIC）。MIC负责监督《个人编号法》的实施，包括：个人编号卡的发行，My Number系统的管理，监督个人编号数据使用，个人信息保护。MIC与内阁秘书处和法务省等其他政府机构密切合作，以确保《个人编号法》的顺利实施。

数据跨境

日本APPI法案第24条对跨境数据传输主要有4项具体要求：

- 要求数据主体（个人数据被传输的个人）对跨境数据传输提供事先同意。
- 要求个人数据被传输到的国家/地区具有足够的个人数据保护水平，这意味着该国必须制定法律和法规，提供与APPI 同等的保护。
- 要求数据控制者（传输数据的组织）和数据处理者（接收数据的组织）之间签订数据保护协议，以确保数据按照APPI受到保护。
- 要求数据控制者将跨境数据传输通知个人信息保护委员会（PPC）。

日本MNA第17条对跨境数据传输主要有5项具体要求：

- 限制个人编号数据跨境传输到具有足够个人数据保护水平的国家。
- 个人编号数据被传输到的国家/地区拥有提供与MNA同等保护的法律法规。
- 要求事先获得总务和通信部长的批准，才能对个人编号数据进行跨境数据传输。
- 要求数据控制者（传输数据的组织）和数据处理者（接收数据的组织）之间签订数据保护协议，以确保数据根据MNA得到保护。
- 要求数据控制者将跨境数据传输通知总务省（MIC）。

此外，APPI 和MNA都规定了跨境数据传输要求的某些例外情况，例如：出于国际合作目的（如执法或国家安全）的跨境数据传输无需事先同意和充分保护要求。如果数据主体已明确同意跨境数据传输，则免除APPI或MNA要求。出于公共利益而必需的跨境数据传输，例如用于统计或研究目的，可以免于 APPI 或MNA要求。

值得注意的是，APPI和MNA都是相对较新的法律，日本政府仍在制定这两项法规实施的指导方针和法规。因此，APPI和MNA对跨境数据传输的要求将来都可能会发生变化或澄清。

数据本地存储

与其他一些国家不同，日本的APPI对数据本地化没有具体要求，不要求将个人数据存储在日本境内。但是，数据控制者仍必须确保个人数据根据 APPI 受到保护（个人数据保护），无论数据存储在何处。

而日本的MNA对个人编号数据的本地存储有一些具体要求：

- MNA要求将My Number数据存储在日本境内。这意味着数据控制者（收集和处理个人号码数据的组织）必须确保个人号码数据存储在位于日本境内的服务器或其他存储设备上。
- MNA还要求以安全的方式存储个人编号数据，以防止未经授权的访问、泄漏、丢失或损坏。这包括实施适当的技术和组织措施，例如加密、访问控制和备份系统。
- MNA要求对My Number数据的访问仅限于授权人员，并且仅在需要知道的基础上授予访问权限。
- MNA要求数据控制者实施备份和恢复程序，以确保在数据丢失或系统故障的情况下，可以恢复My Number数据。
- MNA要求将My Number数据保留一段规定的时间，通常为自收集之日起5年。
- MNA要求在不再需要或保留期限届满时，安全销毁My Number数据。这些要求旨在保护个人号码数据的隐私和安全，并确保以负责任和安全的方式处理这些数据。

个人数据保护

日本的APPI法案对个人数据保护主要有10项要求，这些要求旨在保护日本个人的隐私和权利，并确保以负责任和安全的方式处理个人数据。主要包括：

- 数据控制者必须对其个人数据处理活动保持透明，包括收集的目的、收集的数据类型以及数据的接收者。
- 个人数据必须为特定、明确和合法的目的收集，未经个人同意，不得用于任何其他目的。
- 数据控制者只能收集和处理为收集目的所必需的个人数据。
- 个人数据必须准确且最新。
- 数据控制者必须实施适当的技术和组织措施，以保护个人数据免遭未经授权的访问、泄露、丢失或损坏。
- 个人有权访问、更正和删除其个人数据，并有权反对处理其个人数据。
- 数据控制者在收集和处理其个人数据之前必须事先获得个人的同意。
- 数据控制者必须将任何数据泄露或未经授权访问个人数据的情况通知PPC和受影响的个人。
- 数据控制者在实施新的个人数据处理活动之前必须进行数据保护影响评估。
- 数据控制者有责任确保个人数据根据 APPI 受到保护，并且必须能够证明遵守法律。

日本的MNA对个人数据的保护同样有10项要求，这些要求旨在保护个人号码数据的隐私和安全，并确保以负责任和安全的方式处理这些数据。主要包括：

- 个人编号数据的收集和使用只能用于管理个人编号系统，未经个人同意，不得用于任何其他目的。
- 个人编号数据必须限制在收集目的所需的最低限度，并且不得包含任何不必要或过多的信息。
- 个人编号数据必须准确且最新。
- 必须保护个人编号数据免受未经授权的访问、泄露、丢失或损坏，并且必须以安全的方式存储。
- 个人编号数据必须保密，未经个人同意，不得向任何第三方披露。
- 个人有权访问、更正和删除其个人编号数据，并有权反对处理其个人编号数据。
- 只有在个人同意的情况下才能收集和使用个人编号数据，并且必须告知个人数据收集的目的和范围。
- MNA要求在实施任何新的个人数据处理活动之前进行数据保护影响评估。
- MNA要求数据控制者（收集和处理My Number数据的组织）负责确保My Number数据受到法律保护。
- MNA要求数据控制者遵守与保护My Number数据相关的法律法规。

[1]https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en

[2]https://www.kojinbango-card.go.jp/zh-cn/

日本数据违规案例

某国际社交平台公司提供的一款APP是日本国民级社交软件，也是绝大多数国民日常使用的服务。2023年11月27日该公司公布信息泄露，2024年2月14日该公司官网再次更新了信息泄露情况，总数增至约51万9,000条。经审查，总务省发现该公司在安全管理措施、网络安全措施以及业务委托方管理等方面存在缺陷，认定其违反了《电气通信事业法》第4条第1款规定的有关通信秘密保护的条款。总务省严厉指出，该公司的本次事件不仅严重损害了公司形象，也损害了用户对日本整个电信行业的信任。

一般而言，出海日本企业数据合规的相关法律规定主要集中在日本《个人信息保护法》和个人信息保护委员会发布的相关指南、条例中。但是，此次事件中，除了个人信息保护委员会就个人信息保护的相关问题下达行政指导外，总务省也多次就通信秘密泄露问题发布指导命令。这警示出海日本提供电信相关服务的厂商，在关注《个人信息保护法》相关法律框架之外，也需要重视《电气通信事业法》的合规要求，提前采取措施加强对数据的安全管理、做好数据泄露的应急备案。

3.8.2 韩国

韩国法规要求概述

韩国《个人信息保护法案》（Personal Information Protection Act，PIPA）在2020年8月生效， 并于2021年、2023年分别进行了修订，管理所有领域的个人信息采集、使用和处理[1]。

尽管PIPA中没有明确规定地域范围，但韩国数据保护法对控制者/处理者的执行标准与GDPR相似。在韩国成立的公司受该法律的约束，外国实体也可能受该法律的约束，具体取决于该组织是否针对韩国用户或是否通过在韩国开展业务而产生收入等因素。

2021年1月6日对PIPA的修正案中，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，韩国个人信息保护委员会（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》，规定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PIPC发布了《人工智能时代个人信息安全使用指南》。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。

韩国法规重点梳理

监管机构

韩国PIPA的监督机构是个人信息保护委员会（Personal Information Protection Commission，PIPC）。PIPC是一个独立机构，成立于2011年，负责监督和执行PIPA。其主要职责包括：监督和指导，合规监控，争议解决，政策制定。PIPC总部设在首尔，并在韩国各地设有区域办事处。

数据跨境

韩国的PIPA第17条对跨境数据传输有4项具体要求：

- 要求数据主体（个人数据被传输的个人）对跨境数据传输提供事先同意。
- 要求个人数据被传输到的国家/地区具有足够的个人数据保护水平，这意味着该国必须制定法律和法规，提供与PIPA同等的保护。
- 要求数据控制者（传输数据的组织）和数据处理者（接收数据的组织）之间签订数据保护协议，以确保数据按照PIPA得到保护。
- 要求数据控制者将跨境数据传输通知PIPC。

同时，PIPA规定了跨境数据传输要求的某些例外情况，例如：为执法或国家安全目的的国际合作，为向数据主体提供服务或产品而传输个人数据，为进行统计或科学研究而传输个人数据。

数据本地存储

与其他一些国家/地区不同，韩国的PIPA不要求个人数据存储在韩国境内。但是，数据控制者（收集和处理个人数据的组织）必须确保个人数据根据 PIPA 受到保护，无论数据存储在何处。

[1]https://pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2331

个人数据保护 韩国的PIPA对个人数据保护主要有10项要求，包括：

- 数据控制者必须对其个人数据处理活动保持透明，包括收集的目的、收集的数据类型以及数据的接收者。
- 个人数据的收集和使用只能用于收集目的，未经个人同意，不得用于任何其他目的。
- 个人数据必须限制在收集目的所需的最低限度，并且不得包含任何不必要或过多的信息。
- 个人数据必须准确且最新。
- 必须保护个人数据免受未经授权的访问、泄漏、丢失或损坏，并且必须以安全的方式存储。
- 个人数据必须保密，未经个人同意，不得向任何第三方披露。
- 个人有权访问、更正和删除其个人数据，并有权反对处理其个人数据。
- 只有在个人同意的情况下才能收集和使用个人数据，并且必须告知个人数据收集的目的和范围。
- PIPA要求在实施任何新的个人数据处理活动之前进行数据保护影响评估。
- 数据控制者有责任确保个人数据按照 PIPA 受到保护，并且必须能够证明遵守法律。

这些要求旨在保护个人数据的隐私和安全，并确保以负责任和安全的方式处理个人数据。

韩国数据违规案

根据韩国《个人信息保护法》第28条第8款，个人信息处理者不得将个人信息提供至境外，除非从信息主体获得关于境外转移的单独同意。此外，第29条第10款要求在跨境传输个人信息时必须采取保护措施，包括个人信息保护安全保障措施、对个人信息侵犯的投诉处理及纠纷解决措施等。

韩国个人信息监管机构7月26日对某跨境电商平台处以近19.8亿韩元罚款，原因是该平台在未通知韩国用户的情况下向约18万海外卖家泄露了他们的个人信息。

该跨境电商平台允许入驻卖家向用户销售商品，并从中收取一定比例的销售金额作为中介费。在此过程中，卖家将消费者的个人信息跨境传输给发货工厂，导致超过18万韩国用户的个人信息被提供给了中国卖家。该平台并未向用户告知“个人信息转移的国家”、“接收个人信息的个人或法人的姓名（公司名称）及联系方式”等根据个人信息保护法规定的应告知事项，也未在卖家须知中反映保护个人信息所需的措施。此外，该平台还通过使会员退出菜单难以查找、将账户删除页面以英文显示等方式，增加了用户行使个人信息权利权利的难度，违反了韩国《个人信息保护法》中关于个人信息跨境传输的规定。

非洲 3.9

3.9.1 埃及

埃及法规要求概述

埃及《数据保护法》（Data Protection Law，DPL）于2020年7月15日公布，并于3个月后正式生效[1]。埃及DPL共14章49条，系埃及国内首部关于个人数据保护的专门立法。埃及DPL在法律责任、跨境数据保护、数据主体的权利以及数据控制者和处理者的义务设定等方面体现出其鲜明的本土特色。埃及DPL的出台对于提升埃及整体的个人数据保护水平意义重大，完善了埃及国内的个人数据保护制度，并通过制定达到国际最佳实践标准的数据保护法来改善本国的营商环境，以吸引更多的外国投资者，助力埃及的技术创新和数字转型。

埃及DPL主要以GDPR为蓝本。它适用于处理属于埃及居民的个人数据的数据控制者和处理者，无论他们是否在埃及。根据DPL，所有数据泄露或网络攻击必须在72小时内向个人数据保护中心以及受影响的数据主体报告。只有在存在法律依据的情况下，才允许处理个人数据。埃及的DPL仅能适用于以电子方式处理的个人数据，相较之下，欧盟GDPR则适用于任何媒介手段下的所有数据处理活动。

埃及DPL第2条专门规定了数据主体所享有的权利，以强化对个人数据的保护，主要包括：数据访问权，撤回权，数据修改、编辑、删除及更新权，数据限制权，个人数据泄露的知情权，数据处理反对权。埃及的DPL第3条作了相当广泛的适用豁免规定，其中包括：自然人基于个人使用而进行的数据处理；基于官方统计目的进行的数据处理；与司法记录、调查和司法程序有关的个人数据处理等。其中，埃及中央银行以及所有受中央银行监管的金融机构并不适用该法；埃及国家安全机构在其职责范围内进行的个人数据处理也不受该法规限制。

与欧盟GDPR及非洲绝大多数国家的数据保护立法主要规范数据控制者不同，埃及《数据保护法》对数据处理者施加了与数据控制者同等的监管措施。在数据泄露的通知及告知义务方面，相比欧盟GDPR的模糊规定，埃及《数据保护法》则更为具体、清晰，还特别规定了涉及国家安全事项的通知要求。在数据保护官的设置方面，埃及《数据保护法》对数据控制者及处理者提出了更高要求。《数据保护法》第8条规定，所有数据控制者或处理者都应当任命一名数据保护官，专门负责个人数据安全工作。

在《数据保护法》之外，埃及个人数据处理及其治理散见于宪法和各个部门法中。如埃及已将个人隐私权保护作为一项基本原则写入《宪法》；《民法典》规定了侵犯隐私数据的一般侵权责任；《劳动法》规定了雇员个人数据的保护；《网络安全法》规定了网络经营者的个人数据保护义务等。在埃及《数据保护法》生效后，上述法律对于数据的相关规定仍将适用。

埃及法规重点梳理

监管机构

埃及DPL设立了专门的数据保护监管机构——埃及数据保护局（Data Protection Authority of Egypt， EDPA）。EDPA的主要职责包括：

- 制定有关个人数据保护的政策及计划。
- 明确涉及个人数据保护的标准、规则、程序及决定。
- 与其他政府部门及非政府部门合作。
- 支持政府和非政府部门有关个人数据保护工作人员的培养计划。
- 向数据控制者或处理者签发有关个人数据保护的许可证、认证证书等。
- 开展关于个人数据保护的教育、培训、宣传等。

数据保护中心最高权力机构是理事会，理事成员分别来自国防部、内务部、情报总局、行政管理局、信息技术产业发展局、电信管理局等部门。

EDPA采用许可及认证管理制度，即无论是个人数据的收集、存储、跨境传输，还是个人敏感数据的处理以及电子直销等，都需要取得数据保护中心的许可或认证。

[1]https://www.dataguidance.com/notes/egypt-data-protection-overview

数据跨境

埃及DPL在数据跨境传输方面遵循“不低于本国数据保护要求”原则。数据传输至埃及以外的任何第三国，必须同时满足两个条件，一是该数据输入目的国必须提供不低于埃及个人数据保护同等水平的保护，二是该跨境输出已经获得数据保护中心的许可。

埃及DPL第15条规定了数据跨境传输的例外条款。如果数据输入国的数据保护水平低于埃及，但满足下列条件仍可以进行跨境数据传输：（1）获得数据主体的明示同意；（2）数据处理是必要性，且符合以下任一目的：出于保护数据主体生命健康之所必需；在司法程序中行使诉权或抗辩权；为数据主体利益签订或履行合同；保护公共利益之所必需；履行国际司法协助之所必需；依法进行货币转移；履行双方或多边国际条约之所必需。

数据本地存储

根据埃及DPL第3条，个人数据的处理和存储必须按照以下原则进行：

- **数据最小化：**必须出于数据主体已知的合法、特定和透明目的收集个人数据。
- **准确性和安全性：**个人数据必须正确、有效和安全。
- **合法性：**个人数据必须以合法的方式处理，并适合其收集目的。
- **存储限制：**个人数据的保留时间不得超过实现目的所需的时间。

个人数据保护

埃及DPL对“个人数据”“个人敏感数据”的定义，与欧盟GDPR基本一致。“个人数据”即指任何一个可识别或已识别的自然人（数据主体）能够被直接或间接识别，如姓名、声音、图片、身份证号、在线标识符，或者与该自然人心理、健康、经济、文化或社会身份有关的任何数据。“个人敏感数据”则涵盖涉及自然人心理、精神、身体或遗传健康状况、生物特征、财务、宗教信仰、政治观点等以及与儿童有关的个人数据。

该法第12条专门规定了个人敏感数据的处理规则。数据控制者或处理者如需进行个人敏感数据的收集、访问、转移、存储、保留或处理，必须获得埃及数据保护中心的许可，除非该处理行为已经取得数据主体“明确的书面同意”。该法对于违反个人敏感数据的处理义务施以较重的刑事制裁，违法行为人将会被处以不少于3个月监禁及（或）不少于50万至500万埃及镑的罚款。

埃及数据违规案例

1.埃及银行被罚款一百万埃及镑（约63,000美元）：2020年，埃及一家银行因未通知客户的一起数据泄露事件，披露了客户的个人和财务信息，被埃及数据保护局（EDPA）罚款一百万埃及镑。

2.e-commerce公司被罚款五十万埃及镑（约31,500美元）：2019年，埃及一家e-commerce公司因未提供足够的安全措施保护客户数据，违反了通用数据保护法规（GDPR），被EDPA罚款五十万埃及镑。

3. 医疗机构被罚款二十五万埃及镑（约15,750美元）：2018年，埃及一家医疗机构因未通知病人的一起数据泄露事件，披露了客户的个人和医疗信息，被EDPA罚款二十五万埃及镑。

4.通信公司被罚款一百万埃及镑（约63,000美元）：2020年，埃及一家通信公司因未通知用户的一起数据泄露事件， 披露了客户的个人和使用信息，被EDPA罚款一百万埃及镑。

3.9.2 南非

南非法规要求概述

南非的《个人信息保护法案》(Protection of Personal Information Act 4，POPIA）于2018年年底施行，紧随着2018年5月28日施行的欧盟《数据通用保护条例》(GDPR)[1]。POPIA对于企业的合规要求于2019年完成。POPIA旨在保护个人的个人信息，并确保组织以负责任和透明的方式处理个人数据。

《个人信息保护法案（POPIA）》建立是为了让数据主体能够更好地控制其个人信息的自由流动。它适用于在南非注册的公共和私人机构，规范了商业主体收集、储存及使用个人信息的条件和行为。

《欧盟通用数据保护条例》（GDPR）启发了南非的《个人信息保护法》（POPIA），但这两项法律之间存在一些关键差异。以下是POPIA比GDPR较严格的三个方面：

- POPIA涵盖有关公司的数据——而不仅仅指个人。GDPR将“个人数据”定义为“与已识别或可识别的自然人相关的信息...”（“数据主体”）。POPIA同样将“个人信息”定义为“.....与可识别的在世自然人有关的信息...”。但南非法律随后进一步扩大了这一定义，并补充说，个人信息也可能与“可识别的现有法人.....”有关。这意味着在南非运营的企业可能需要保护有关业务合作伙伴、供应商等的数据，就像保护有关其客户/用户的数据一样。这不仅包含着有关这些商业实体的员工（他们是“自然人”）的数据，还意味着有关企业本身（“法人”）的数据。
- POPIA对儿童数据的规定更加严格。GDPR对儿童的规定已经相当严格，侧重于直接向儿童提供“信息社会服务”（在线服务）的控制者。此类控制者在处理儿童的个人数据之前必须征得父母的同意。另外，GDPR强调在处理儿童个人数据时对儿童的“特定保护”，特别是在出于营销或分析目的时。相比之下，POPIA关于处理儿童数据的规则适用于您处理数据的上下文——法律不区分不同的处理目的。这基本上意味着完全禁止处理儿童数据。此外，可以直接向南非的信息监管机构申请处理儿童数据的授权。
- 每个公司都必须任命一名高管级别的DPO。根据POPIA要求属于法律范围的每个企业都必须任命一名数据保护官（DPO），并且这种任命有一些严格的条件。这与GDPR对DPO的态度形成鲜明对比。根据GDPR，DPO充当独立顾问，来监督企业数据保护的合规性，而对于许多不定期监控数据主体或处理“特殊类别数据”的私营公司，并不需要任命DPO。

同时，相比GDPR， POPIA也有较宽松的三个方面：

- GDPR第25条规定了隐私设计(privacy by design)这一概念。POPIA并未体现这一概念，然而对于在南非实施隐私计划的人而言，隐私设计被视为最佳实践方案。
- GDPR第35规定了数据保护影响评估(the data protection impact assessment)的义务，然而POPIA对此并未有所体现。
- GDPR第20规定了数据可携权(the right of data portability)，这一权利为数据主体提供将其数据迁移至另一数据控制者或服务提供者的选择权。然而POPIA对此并未有所体现。

南非法规重点梳理

监管机构

南非负责监控与强制实施POPIA的信息监管机构主要包括南非国家消费者委员会、南非公司与知识产权局（CIPC）、南非标准局以及强制性技术规范国家监管机构（NRCS）。这些机构共同构成了南非信息监管的框架，旨在保护消费者权益、促进知识产权的保护、制定和执行标准，以及监督技术规范的实施，以确保信息的安全和合规性。

数据跨境

南非POPIA 的第 72 节允许在符合下列条件时将个人信息转移到南非境外：

- 作为信息接收者的第三方遵守能提供充足保护的法律，具有约束力的公司规章或具有约束力的协议。
- 数据主体同意转移。
- 转移对履行数据主体和责任方之间的合同，或应数据主体请求实施合同前措施而言是必要的。
- 转移对责任方和第三方之间订立或履行保护数据主体利益的合同来说是必要的；或者转移对数据主体有好处。

[1]https://www.gov.za/documents/protection-personal-information-act

数据本地存储

任何公共或私人机构或任何其他人（称为“责任方”）必须采取适当、合理的技术和组织措施，确保其拥有或控制下的个人信息的完整性和保密性，以防止个人信息的丢失、损坏或未经授权销毁；以及非法访问或处理个人信息。

责任方必须采取的合理措施包括：识别其拥有或控制的个人信息的所有合理、可预见的内部和外部风险；建立并保持针对已确定的风险的适当保障措施；定期核实保障措施是否得到有效实施；并确保保障措施不断更新，以应对以前实施的保障措施中的新风险或缺陷。

责任方必须适当考虑普遍接受的信息安全实践和程序，这些做法和程序可能普遍适用，或在特定行业或专业规则和条例方面适用。

个人数据保护

- 1996年《南非共和国宪法》第14条规定，人人有权享有隐私权；隐私权包括免受非法收集、保留、传播和使用个人信息的权利。
- POPIA规定个人信息必须直接从数据主体收集（除非POPIA另有规定），数据主体可以随时反对处理个人信息。
- POPIA第34条规定禁止处理儿童个人信息，但有一些情况下此规定不适用，例如经过主管人员事先同意；捍卫法律权利或义务的需要；处理符合公共利益并采取适当保障措施来保护儿童个人信息。
- 任何机构或个人在未得到客户书面允许的情况下，不得对外泄露他们的个人信息，例如手机号码、电子邮件地址等。此外，银行、保险公司、医疗保健机构、制药公司、市场营销公司、旅行社等商业机构也不能向个人电子信箱、手机等发送信息，除非获得使用者的许可。

南非数据合规案例

- 一家南非主要银行被罚款12万南非兰特（约82,000美元），因未能实施适当的安全措施保护客户数据，这些数据后被黑客盗取。
- 一家南非私人医疗机构被罚款50,000南非兰特（约34,000美元），因未能确保患者数据的保密性，这些数据后被未经授权的人访问。
- 一家南非流行零售连锁店被罚款20,000南非兰特（约14,000美元），因未能实施适当的安全措施保护客户数据，这些数据后被黑客盗取。
- 一家南非主要通信服务提供商被罚款1,000,000南非兰特（约68,000美元），因未能确保客户数据的保密性，这些数据后被未经授权的人访问。
- 一家南非主要雇主被罚款50,000南非兰特（约34,000美元），因未能确保员工数据的保密性，这些数据后被未经授权的人访问。

大洋洲 3.10

3.10.1 澳大利亚

澳大利亚法规要求概述

《澳大利亚隐私法》（Australia's Privacy Act，APA）于1988年颁布，是澳大利亚联邦层面的一部全面的数据保护法。APA包括一份适用于处理个人信息的组织的13项澳大利亚隐私原则的清单[1]。

APA不仅适用于澳大利亚境内，在澳大利亚境外，只要该组织拥有“澳大利亚联系”。所谓澳大利亚联系指的是此APP实体（Australia Privacy Principles 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在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。

APA在某些材料要求方面类似于GDPR，包括对个人数据有相似的定义、数据处理的要求，并为个人提供访问其个人信息的权利。但是，APA和GDPR还是有些不同之处，主要区别在于APA没有区分数据控制者和数据处理者，而是统一用APP实体来指代。此外，向澳大利亚以外发送个人信息的APA机制也有所不同。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。

澳大利亚法规重点梳理

监管机构

澳大利亚APA的监督机构是澳大利亚信息专员办公室（the Office of the Australian Information Commissioner，OAIC）。OAIC是一个独立机构，成立于2010年，负责监督和执行APA。其主要职责包括：隐私监管，投诉处理，指导和教育，审核和评估，政策制定。OAIC由澳大利亚信息专员领导，他负责确保OAIC按照APA履行其职能。

数据跨境

澳大利亚APA对跨境数据传输有3项具体要求，这些要求在《澳大利亚隐私原则》（Australian Privacy Principles，APPs）中进行了概述：

- APP 8.1规定在向境外接收方披露个人信息之前，APP主体必须采取合理措施确保接收方不违反APP。
- APP 8.2规定如果APP实体向境外接收方披露个人信息，必须确保接收方受到与APP 基本相似的法律或约束机制的约束。
- APP主体必须采取合理措施，确保境外接收方不违反APP，包括与海外接收方签订合同，要求他们遵守 APP；对海外接收方进行尽职调查，以确保他们有足够的隐私保护措施；实施技术和组织措施来保护个人信息。

另外，APA对跨境数据传输的要求存在某些例外情况，例如：个人已同意披露。为履行APP主体与个人之间的合同所必需的披露。在法律要求或授权的情况下进行披露。

数据本地存储

与其他一些国家/地区不同，APA不要求将个人信息存储在澳大利亚境内。但是，APP实体必须确保个人信息根据APA受到保护，无论其存储在哪里。

[1]https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

个人数据保护 澳大利亚的APA规定了保护个人数据的一些关键要求：

- 组织只能为收集时声明的目的收集和使用个人信息，并且必须确保信息与目的相关。
- 组织在收集、使用或披露其个人信息前，必须征得个人的同意。
- 同意必须是知情的、具体的和明确的。
- 组织必须采取合理措施确保个人信息准确、最新和完整。
- 组织必须采取合理措施保护个人信息免遭滥用、干扰、丢失、未经授权的访问、修改或披露。组织必须制定个人信息保留和处置政策，并且不得将个人信息保留超过必要的时间。
- 如果发生可能对个人造成严重伤害的数据泄露，组织必须通知受影响的个人和OAIC。
- 个人有权访问和更正其个人信息，组织必须提供访问和更正程序。
- 组织必须采取额外措施来保护敏感信息，例如有关个人健康、性取向或犯罪记录的信息。
- 组织必须在其系统和流程中实施隐私设计原则，并且在设计新产品和服务时必须考虑隐私。
- 组织在实施涉及高风险个人信息处理的新技术或流程时，必须进行隐私影响评估。
- 组织必须制定内部政策和程序，以确保遵守《隐私法》，并且必须能够证明遵守。

澳大利亚数据违规案例

2023年7月，澳大利亚联邦法院对某全球社交平台旗下两家子公司分别处以1,000万澳元罚款，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该社交平台以实现其他商 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。

2022年，澳大利亚公平竞争和消费者委员会（ACCC）发布消息称，因某全球互联网公司2017年1月至2018年12月期间，向用户展示了误导性信息，违规收集、储存并使用了澳大利亚境内约130万用户信息。因违反《澳大利亚消费者法》，该公司为此支付6,000万澳元罚款。

3.10.2 新西兰

新西兰法规要求概述

新西兰1993年颁布了《隐私法》（Privacy Act，PA），在2020年12月，为了加强数据保护方面的规定，实施新的《2020年隐私法》(2020 PA)。与世界各地的其他综合隐私和数据保护法相比，该法的一个关键特征是赋予“隐私专员”在制定和执行法律方面的核心作用和更大的权利，包括在个人或代表诉讼提交人权法庭之前，作为必要的“阻止”；发布全面的合规通知；禁止跨境传输个人信息等[1]。

《2020 PA》适用于任何设在新西兰的数据处理机构，以及任何从事与新西兰公民有关的业务或收集数据的海外组织。《2020 PA》和GDPR相同之处是企业任命一名隐私官来监督内部合规过程，并处理出现的任何问题。如果个人资料被泄露，他们将与隐私监管机构联系，并负责发布报告。和GDPR不同处是，尽管《2020 PA》旨在规范国家和公司之间的用户信息流动，但它缺乏GDPR和其他现代隐私法的力量。首先，它没有建立一个框架，让互联网用户选择加入或反对跟踪他们的数据。此外，它并没有赋予个人被遗忘的权利或数据可移植性的权利。最后，它没有赋予隐私专员对隐私泄露处以罚款的能力。

新西兰法规重点梳理

监管机构

新西兰的《2020 PA》由多个机构和组织负责执行：

- **隐私专员：**隐私专员是议会的独立官员，也是新西兰隐私的主要监管机构。专员负责确保遵守《隐私法》，并拥有一系列权力，包括调查投诉、提供指导、监督和审计组织，以及提高公众对隐私问题的认识。
- **隐私专员办公室（OPC）：**OPC是支持隐私专员工作的办公室。OPC为组织和个人提供有关隐私问题的信息和指导，处理投诉和查询，并与其他机构和组织合作，以提高隐私意识和合规性。
- **新西兰信息和隐私专员（NZIPC）：**NZIPC是根据2020年PA成立的新机构，旨在为新西兰的所有信息和隐私相关事务提供一站式服务。NZIPC负责提供有关隐私和信息管理的信息和指导，处理投诉和查询，并提高公众对隐私问题的认识。
- **数据保护局（DPA）：**DPA是根据2020年PA成立的新机构，旨在规范新西兰个人数据的使用。DPA负责确保组织遵守PA，并有权调查和执行违反该法的行为。

数据跨境

新西兰的《2020 PA》对数据出境的关键要求是：组织必须确保不会将个人信息传输到国外，除非接收国的法律提供类似于PA的保护标准。允许将个人信息传输到经济合作与发展组织（OECD）成员国，只要接收国的法律提供类似于PA的保护标准。组织确保个人信息根据PA的原则受到保护，即使它被转移到国外也是如此。组织必须采取合理措施，确保接收国的法律和做法为个人信息提供充分保护。

另外，PA允许在某些情况下进行跨境数据传输，例如，当传输是履行组织与个人之间的合同所必需的，或者为法律纠纷的目的而需要传输时。允许组织与外国接收者签订数据保护协议，以确保遵守该法案。这些协议必须包括确保接收国拥有为个人信息提供充分保护的法律和做法的条款。

数据本地存储

新西兰2020年PA中包括与数据本地化相关的几项规定，这些规定涉及在新西兰存储个人信息。关键要求有：

- 将个人信息存储在新西兰，除非出于合法目的有必要将其存储在新西兰境外，在这种情况下，组织必须确保个人信息根据《隐私法》受到保护，并且已将转移及其原因告知个人。
- 要求组织实施适当的安全措施，以保护个人信息免遭未经授权的访问、披露或使用，这包括确保将个人信息存储在安全的位置，例如上锁的柜子或安全的数字存储设备。
- 要求组织仅在收集信息的目的所需的时间内保留个人信息，并在不再需要时将其处理掉。
  要求组织安全、保密地处理个人信息，以防止未经授权的访问或使用。

[1]https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html

个人数据保护 2020 PA规定了组织在收集、使用、披露和存储个人信息时必须遵循的13项数据保护原则，这些原则主要包括：

- 个人数据的收集必须是合法、公平和合理的。
- 个人数据的收集目的必须明确，并且必须告知个人。
- 个人数据的收集范围必须合理，并且必须与收集目的相关。
- 个人数据必须准确、完整和最新。
- 个人数据必须存储在安全的地方，并且必须采取措施防止未经授权的访问。
- 个人数据必须保密，并且必须采取措施防止未经授权的披露。
- 个人数据只能用于收集目的，并且必须根据法律规定披露。
- 个人有权知道自己的个人数据是否被收集、存储和使用，以及有权访问和更正自己的个人数据。
- 新西兰设立了数据保护官（Privacy Commissioner），负责监督个人数据保护法的执行。
- 组织必须在发生数据泄露时通知受影响的个人和数据保护官。
- 个人数据只能传输到有适当数据保护水平的国家或地区。
- 数据处理者必须遵守个人数据保护法，并且必须对数据控制者负责。
- 组织必须定期进行数据审计和风险评估，以确保个人数据的安全。

根据2020 PA，数据处理者如果不遵守规定，将被处以最高1万新西兰元(7,000美元)的罚款。虽然这听起来似乎是一个相对较低的数字，但隐私专员办公室也可以向人权法庭提出正式投诉，最高可被处以23万新西兰元(16.2万美元)的罚款。

▶ 新西兰数据违规案例

新西兰某全球电信公司在2018年发生了一起数据泄露事件，导致大量客户数据被泄露，包括客户姓名、地址、电话号码、电子邮件地址和账户信息。经调查发现，该公司的第三方供应商未能采取适当措施来保护客户数据，导致数据泄露。具体原因包括：第三方供应商未能及时更新其系统的安全补丁，导致系统存在安全漏洞。第三方供应商未能采取适当的密码管理措施，导致黑客能够轻易猜测密码。第三方供应商未能采取适当的监控措施，导致黑客能够长时间地访问系统而不被发现。

这起数据泄露事件严重影响了客户的隐私和安全。同时，该电信公司的声誉也受到了严重影响，导致客户对公司的信任度下降。该公司在发现数据泄露事件后，立即采取了以下措施：通知受影响的客户，并提供相应的支持和帮助。与第三方供应商合作，采取措施来修复安全漏洞并防止类似事件发生。启动内部调查，查明事件原因并采取相应的改进措施。向新西兰隐私委员会报告事件，并接受委员会的调查和指导。

此次数据泄露事件表明，数据保护是企业运营中的重要环节，企业必须采取适当措施来保护客户数据，否则可能面临法律和声誉风险。同时，企业必须与第三方供应商合作，确保供应商采取适当措施来保护客户数据。

中国 3.11

3.11.1 中国数据出境法规要求概述

为促进数据依法有序自由流动，我国相继制定实施《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》，对数据跨境流动作出了明确规定。

《中华人民共和国网络安全法》：该法于2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过，2017年6月1日起施行。该法规定了网络安全的基本要求，包括网络产品和服务的安全要求、网络运营者的安全义务等，为数据出境提供了基本的法律框架[1]。

《中华人民共和国数据安全法》：该法于2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过，2021年9月1日起施行，是一部基础性、框架性的法律。该法确立了数据处理者的安全义务，包括数据出境的安全评估和管理，确保数据出境活动符合法律规定[2]。

《中华人民共和国个人信息保护法》：该法于2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过，2021年11月1日起施行，是中国首部个人信息保护专门法。该法规定了个人信息的收集、使用、处理和保护原则，对数据出境中的个人信息保护提出了明确要求[3]。

此外，为了具体实施这些法律，国家网信办还公布了《数据出境安全评估办法》、《个人信息出境标准合同办法》等文件，进一步细化了数据出境的安全评估和标准合同备案的要求。这些措施共同构成了中国数据出境的法律体系，旨在确保数据出境活动的安全性和合规性。

[1]http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm
[2]http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html
[3]https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm

3.11.2 中国数据出境法规重点梳理

《中华人民共和国网络安全法》

立法目的　该法的制定旨在保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展。

适用范围　该法适用于在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。

监管机构　根据《中华人民共和国网络安全法》，网络安全的监管机构主要包括以下，这些监管机构在各自的职责范围内，共同负责网络安全的监管和管理工作：

- **国家互联网信息办公室：**负责全国互联网信息内容管理和网络安全管理工作，负责制定和实施网络安全策略、规划和规范，负责组织和协调国家网络安全工作。
- **工业和信息化部：**负责工业控制系统安全、云计算安全和大数据安全等工作　，负责制定和实施工业控制系统安全标准和规范，负责组织和协调工业控制系统安全工作。
- **公安部：**负责网络安全保卫和打击网络犯罪工作，负责组织和协调全国公安机关网络安全保卫和打击网络犯罪工作。
- **国家安全部：**负责国家安全和网络安全工作，负责组织和协调国家安全和网络安全工作。

关键信息

- **基本方针：**国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。
- **网络运营者的安全保护义务：**包括制定内部安全管理制度、采取技术措施防范网络攻击、监测网络运行状态、采取数据分类和加密措施等，以保障网络免受干扰、破坏或未经授权的访问，并防止网络数据泄露或被窃取、篡改。
- **网络安全事件的应对与处置：**网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击等安全风险，并在发生危害网络安全的事件时立即启动应急预案，采取相应补救措施，并按规定向相关主管部门报告。
- **个人信息保护：**网络产品、服务的提供者应当明确告知用户其收集、使用个人信息的目的、方式和范围，并征得用户同意。同时，网络运营者应当采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损或丢失。
- **法律责任：**对于不履行网络安全保护义务、违反个人信息保护规定等行为，相关主管部门将责令改正并给予警告或罚款等行政处罚。对于构成犯罪的行为，将依法追究刑事责任。
- **国际交流与合作：**国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

通过这些规定，《中华人民共和国网络安全法》旨在构建一个安全、稳定的网络环境，保障国家网络安全和公民的合法权益。

《中华人民共和国数据安全法》

立法目的　该法的制定旨在规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

适用范围　本法适用于所有类型的数据处理活动，无论是在线还是离线，无论是个人数据还是非个人数据。

监管机构

根据《中华人民共和国数据安全法》，数据安全的监管机构主要包括以下，这些监管机构在各自的职责范围内，共同负责数据安全的监管和管理工作。

- **国家互联网信息办公室：**负责全国数据安全的统筹协调工作，负责制定和实施数据安全政策、规划和规范 ，负责组织和协调国家数据安全工作。
- **工业和信息化部：**负责工业和信息化领域数据安全工作，负责制定和实施工业和信息化领域数据安全标准和规范 ，负责组织和协调工业和信息化领域数据安全工作。
- **公安部：**负责数据安全保卫和打击数据犯罪工作，负责组织和协调全国公安机关数据安全保卫和打击数据犯罪工作。
- **国家安全部：**负责国家安全和数据安全工作，负责组织和协调国家安全和数据安全工作。

  各级人民政府：负责本行政区域内的数据安全工作，负责组织和协调本行政区域内的数据安全工作。

关键信息

该法共七章五十五条，涵盖了数据安全的多个方面，包括数据保护的域外法律效力、数据安全与发展、数据安全监管机制等。

- **数据保护的域外法律效力**

  考虑到全球经贸和技术交流的频繁，该法明确规定，无论数据处理活动发生在中华人民共和国境内还是境外，只要损害了国家安全、公共利益或公民、组织的合法权益，都将依法追究法律责任。
- **数据安全与发展**

  该法强调在保障数据安全的基础上促进数据的开发利用，明确了数据安全与发展的关系，并提出了相应的措施来促进数据开发利用和技术研究应用。
- **数据安全监管机制**

  国家建立了数据安全应急处置机制和审查制度，对影响或可能影响国家安全的数据处理活动进行国家安全审查。此外，还实施了出口管制措施，对关键信息基础设施运营者的重要数据出境安全管理进行了规定。
- **数据安全保护义务**

  数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施保障数据安全。重要数据的处理者需明确数据安全负责人和管理机构，落实数据安全保护责任。
- **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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者的重的数据出境安全管理办法由国家网信部门会同国务院有关部门制定。

该法的出台标志着我国在数据安全领域有了明确的法律依据，旨在提升国家数据安全保障能力，促进数字经济发展创新，同时扩大了数据保护范围，为各行业数据安全提供监管依据。

《中华人民共和国个人信息保护法》

立法目的

该法的制定旨在保护个人信息权益，规范个人信息处理活动，并促进个人信息的合理利用。该法明确了自然人的个人信息受法律保护，任何组织或个人不得侵害自然人的个人信息权益。它适用于在中华人民共和国境内处理自然人个人信息的活动，以及在中国境外处理中华人民共和国境内自然人个人信息，但满足特定条件的活动。个人信息的定义包括与已识别或可识别的自然人有关的各种信息，通过电子或其他方式记录，但不包括匿名化处理后的信息。个人信息的处理活动包括收集、存储、使用、加工、传输、提供、公开、删除等。

适用范围

个保法适用于在中国境内处理个人信息的活动，以及境外组织和个人处理中国境内自然人个人信息的活动，包括：向中国境内自然人提供产品或者服务、分析或者评估中国境内自然人的行为以及法律、行政法规规定的其他情形。

监管机构

根据《中华人民共和国个人信息保护法》，个人信息保护的监管机构主要包括以下，这些监管机构在各自的职责范围内，共同负责个人信息保护的监管和管理工作：

- **国家互联网信息办公室：**负责全国个人信息保护的统筹协调工作，负责制定和实施个人信息保护政策、规划和规范，负责组织和协调国家个人信息保护工作。
- **工业和信息化部：**负责工业和信息化领域个人信息保护工作，负责制定和实施工业和信息化领域个人信息保护标准和规范，负责组织和协调工业和信息化领域个人信息保护工作。
- **公安部：**负责个人信息安全保卫和打击个人信息犯罪工作，负责组织和协调全国公安机关个人信息安全保卫和打击个人信息犯罪工作。
- **国家安全部：**负责国家安全和个人信息保护工作，负责组织和协调国家安全和个人信息保 护工作。
- **各级人民政府：**负责本行政区域内的个人信息保护工作，负责组织和协调本行政区域内的个人信息保护工作。

关键信息

- **个人数据及敏感数据定义**
  - 个人信息是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，不包括匿名化处理后的信息。依据《民法典》第一千零三十四条规定，个人信息包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。
  - 敏感个人信息是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，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。
- **数据主体权利**
  - 该法还强调了个人信息的权利属性，将其定义为具体人格权益，并规定了知情同意权、信息查阅、访问与复制权、信息更正权、信息删除权（被遗忘权）、撤回同意权、限制处理权、数据可携权、反对权、自动化决策和分析权、投诉权等具体权益内容。个人信息的客体属性被视为天然内置财产价值的人格利益，其财产属性需要通过特定的法律程序性制度设计转化为被他人共享与利用的财产利益。
- **数据处理者义务**
  - 采取措施确保个人信息处理活动合规。
  - 指定个人信息保护负责人进行监督。
  - 定期对其处理个人信息情况进行合规审计。
  - 进行个人信息保护影响评估，并对处理情况进行记录。
  - 对个人信息泄露、篡改、丢失立即采取补救措施，并履行通知义务。
  - 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者应履行的义务。
- **数据处理原则**
  - 该法规定了个人信息的处理原则，包括通过自动化决策方式向个人进行信息推送、商业营销时，应提供不针对其个人特征的选项或提供便捷的拒绝方式。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等；处理个人信息要遵循合法、正当、必要和诚信原则、目的限制原则、公开、透明原则、质量原则以及责任与安全原则。处理敏感个人信息，如生物识别、医疗健康、金融账户、行踪轨迹等，应取得个人的单独同意。对于违法处理个人信息的应用程序，法律规定可以责令暂停或终止提供服务。

- **数据处理的合法正当理由**
  - 个人信息处理者方可处理个人信息。
  - 取得个人的同意。
  - 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。
  - 为履行法定职责或者法定义务所必需。
  - 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需。
  - 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。
  - 依照本法规定在合理的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。
  - 法律、行政法规规定的其他情形。依照个保法其他有关规定，处理个人信息应当取得个人同意，但是有上述第（2）至第（7）种情形的，不需取得个人同意。
- **本地化存储要求**
  - 关键信息基础设施境内运营过程中产生的个人数据和重要数据实施数据本地化的要求。
- **数据跨境传输规则**
  - 属于关键信息基础设施运营者和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，需就其向境外提供个人信息办理了网信部门组织的安全评估。
  - 属于经国家网信部门的规定经专业机构进行了个人信息保护认证即可出境的情形，需按照国家网信部门的规定经专业机构进行了个人信息保护认证。
  - 属于按照国家网信部门制定的标准合同与境外接收方订立合同即可出境的情形，需按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务。
  - 向个人告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项。

该法的实施，旨在加强个人信息保护的法制保障，回应广大人民群众对于个人信息保护的关切和期待，确保个人信息安全，维护公民在网络空间的合法权益。

3.11.3 中国数据出境法规重点梳理

《数据安全法》第31条规定：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

典型案例1

2021年12月，上海某信息科技公司接受一境外公司委托，在对方规定的北京、上海等16个城市及相应高铁线路上，采集了我国铁路信号数据（包括物联网、蜂窝和高铁移动通信专网敏感信号等数据），并在数据采集设备上为该境外公司开通了远程登录端口，方便境外公司实时获取对应的测试数据。经鉴定，两家公司为境外公司搜集、提供的数据涉及铁路GSM-R敏感信号。GSM-R是高铁移动通信专网，直接用于高铁列车运行控制和行车调度指挥，是高铁的“千里眼、顺风耳”，承载着高铁运行管理和指挥调度等各种指令。境内公司的行为是《数据安全法》《无线电管理条例》等法律法规严令禁止的非法行为。相关数据被国家保密行政管理部门鉴定为情报。

《数据安全法》第27条规定：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。

《数据安全法》第29条规定：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

典型案例2

2023年3月，浙江温州公安网安部门在查处一起涉数据安全违法案件时，发现浙江某科技有限公司为浙江某县级市政府部门开发运维信息管理系统的过程中，在未经建设单位同意的情况下，将建设单位采集的敏感业务数据擅自上传至租用的公有云服务器上，且未采取安全保护措施，造成了严重的数据泄露。浙江温州公安机关根据《数据安全法》第45条，对公司及项目主管人员、直接责任人员分别作出罚款100万元、8万元、6万元的行政处罚。

数据安全行政处罚案例中，涉及到的数据安全主要包含国家数据安全、企业数据安全、以及个人数据安全这三类。

- **在国家数据安全层面，**数据处理者未遵守数据交易安全的规定，擅自向境外提供重要数据，泄露涉及国家重要情报的数据，对国家安全带来潜在危害。这表明数据分类分级保护制度有待完善，需要加强对重要数据的保护。
- **在企业数据安全层面，**涉案企业均未及时落实数据安全保护义务，缺少数据安全风险评估和监测以及应急处置制度，系统存在重大数据安全隐患。但与此同时，对于企业“未履行数据安全保护义务”时，行政机关的处罚存在“类案不同罚”的情况，处罚结果轻至“责令改正”，重至“罚款15万”，如此可能会加重企业的合规负担。
- **在个人数据安全层面，**存在敏感数据违规收集以及数据泄漏风险的问题。数据处理者未履行数据安全保护义务、对敏感数据采取去标识化和加密措施等技术保护措施，导致平台数据泄漏或存在数据泄露风险。而一些平台以强制、诱导等恶意方式严重违法违规收集使用个人信息，侵害了公民的隐私权。

数据出境绝不仅仅是只关涉企业自身利益的企业行为，企业必须从国家安全、公共利益、个人信息主体权益保护等多重角度来监督和管理数据出境。对于需要进行数据出境的企业来说，需根据自身情况选择合法的数据出境合规路径，切不可因一时的利益追求置数据出境的合规安全于不顾。

04

数据合规体系建设

站在全球看全球

数据安全与合规体系

数据安全与合规嵌入研发流程

站在全球看全球 4.1

4.1.1 全球化框架

在全球化浪潮、经济低迷和激烈竞争的背景下，越来越多的中国企业将目光转向国际市场，寻求海外拓展的机遇。然而，国际化的道路并非一帆风顺，中国企业在这一过程中既面临严峻挑战，也拥有重要机遇。

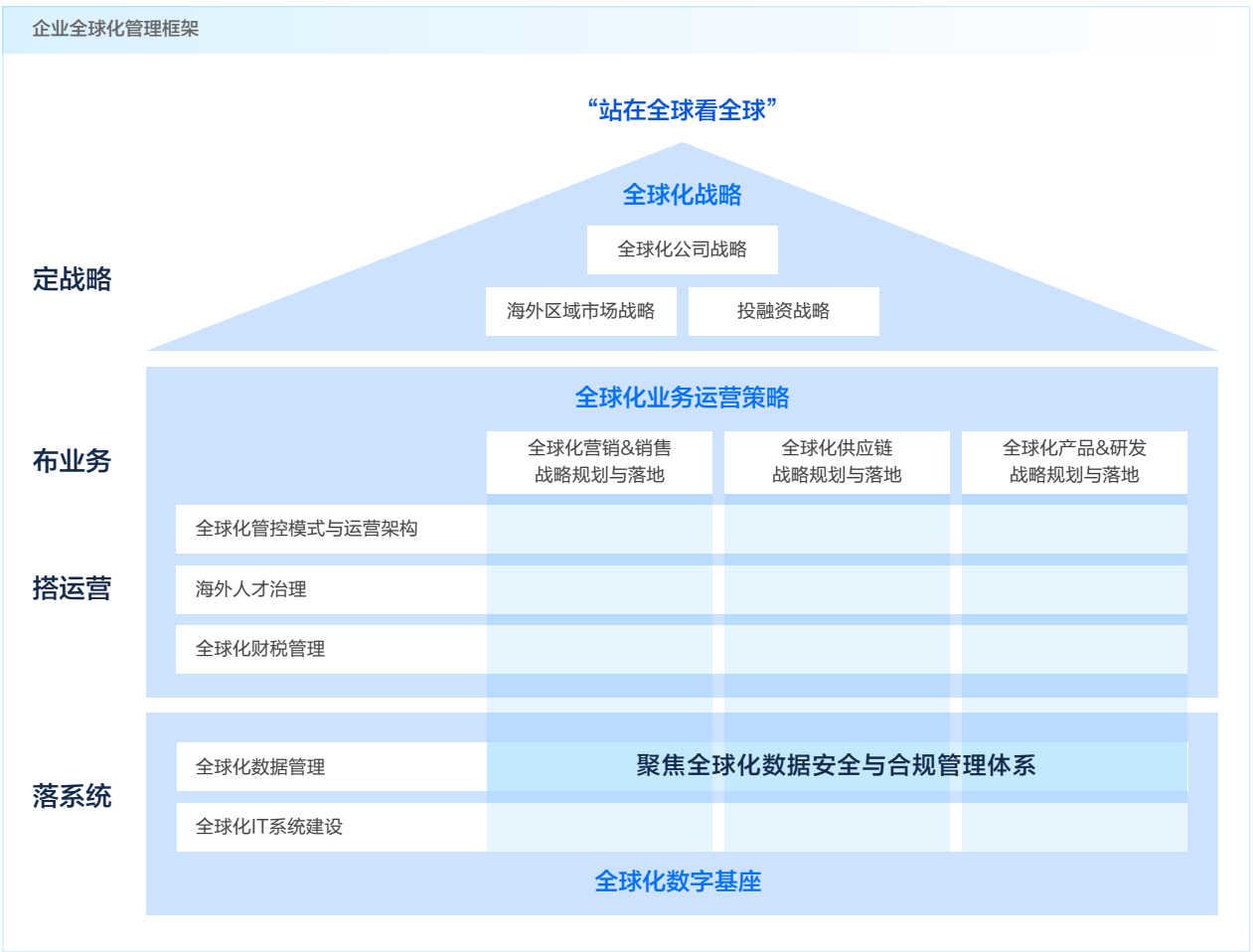
从外部环境来看，中国企业需要应对多重挑战以谋求经营的韧性。全球经济和市场环境的变化，使得企业在国际市场上面临着诸多不确定性，尤其是受“去中国化”和“中国+1”等产业链调整政策的影响，部分企业可能面临上游供应链的掣肘以及下游客户的流失。此外，国内市场竞争日益激烈，利润空间被大幅压缩，整体经济增长放缓，企业的生存和发展受到威胁。

然而，在内部驱动方面，中国企业仍然可以借助自身优势实现高速增长。中国拥有丰富且完善的产业配套体系，并且在移动互联网、新能源等领域具有全球领先的竞争力。这些优势使得中国企业在发展中国家市场能够以相对较低的成本和更高的效率展开竞争，从而占据市场主导地位。在发达市场，中国企业也能够通过抢占价值链中更有利的环节，甚至实现技术和市场上的“弯道超车”。

随着市场环境和竞争格局的变化，传统的出海策略已无法满足当前需求。企业必须制定新的出海战略和运营策略，以适应当下的国际环境，提升全球竞争力。为系统化解决企业出海过程中的各种难点和痛点，中国企业需要采用一体化的出海解决方案。该方案能够帮助企业全面规划和实施国际化战略，有效应对复杂的市场环境，提升竞争力，实现资源的高效配置，从而保障企业在全球市场中的成功和可持续发展。

我们认为，要成为一个真正的全球化企业，必须构建全球化的业务布局和管理体系。这需要从以下四个方面入手：**战略制定、业务布局、运营搭建和系统落地。**通过这些方面的系统构建，企业可以全面提升全球化能力。接下来，我们将详细介绍一体化解决方案的具体内容。

企业全球化管理框架



4.1.2 定战略

从战略视角而言，出海已成为中国企业无法回避的课题，其中首要的是出海战略规划，需要解决“为何出、去哪儿、怎么出、怎么赢”等关键痛点。全球化战略的核心是为决策层提供清晰的方向，涵盖战略意图、市场环境、业务组合及高阶财务目标。为确保战略的有效制定和执行，企业应聚焦如下关键领域：

战略视野

企业在制定出海战略时，能够从全球市场的角度进行长远的规划和布局。这种视野不仅限于当前的市场机会，还包括对未来趋势、技术演变、竞争态势的洞察，以及对不同文化和市场环境的深刻理解。

- **全球市场洞察**：企业需要具备对全球市场的深刻理解，包括目标市场的经济环境、政治形势、文化差异、法律法规、消费者行为等。这种洞察力能够帮助企业识别哪些市场具有潜力，哪些市场可能存在风险，理解和尊重当地文化、风俗和商业惯例，以实现市场的成功进入和持续发展。
- **前瞻性规划**：企业应能够超越短期利益，制定长期的全球化战略。通过战略规划明确国际化愿景、战略目标、市场组合、竞争优势和客户策略，企业可以在全球市场中找到自己的定位。通过海外布局开展市场潜力、进入难度和影响力的评估，企业可以选择和优先开发重点市场，明确资源投入、业务打法。

战略定力

国际化战略是一个需要长期投入、坚定不移的长期建设过程，并动态纠偏，构建科学的战略规划，在面对全球市场的复杂性和不确定性时，能够保持坚定的战略执行力和稳健的应对能力。这包括企业出海短期内出现市场波动、法规变化也要按照既定战略执行的坚持力、抗压力，以及当外部环境发生重大变化时，企业能够快速调整策略并落地执行的变通力。

通过以上能力建设，全球化公司战略的制定和实施变得更加清晰和具体，有助于领导者更好地理解并推动战略的执行，在全球市场中实现稳步发展，增强竞争力和可持续发展能力。国际化战略的实施是一个动态且持续的过程，它要求企业不断学习和适应新的市场环境，更好地规划和执行其国际化战略，实现在全球市场上的成功和持续增长。

4.1.3 布业务

从业务视角来看，随着企业出海低成本优势逐渐消失，传统的价格战策略和国内成功经验的简单复制在海外市场难以为继。对海外市场特点和用户需求的洞察不足，使得业务开展和运营困难重重。此外，面对多个海外市场时，企业缺乏明确的重点，策略均一化、投资分散化，既未能发挥区域规模化的协同效应，也无法满足各市场的个性化需求，严重影响了全球竞争力的提升。全球化业务布局核心是为决策层提供营销与销售、供应链和产品研发的全局视角与综合方案，确保公司在全球市场中的业务决策更加精准有效，为此企业应聚焦如下关键领域：

深度融合

企业在全球化过程中，将营销与销售、供应链、产品与研发等各个环节紧密结合，以实现全方位的业务协同。这种融合不仅包括内部各部门之间的协作，还包括企业与外部合作伙伴之间的深度协作。通过整合全球资源，企业可以更好地适应不同市场的需求，提升供应链的效率与灵活性，以及加快产品研发周期，从而在全球范围内保持竞争优势。

- **营销与销售**：企业需要整合全球市场的营销和销售资源，确保品牌定位和市场策略的一致性，同时针对不同区域进行本地化调整，以满足当地市场的特殊需求。通过构建全球销服一体化业务设计，实现品牌商与区域市场经销商，服务商之间的业务规范，通过流程体系和数据的打通和协同，为终端客户提供更为个性化的服务体验，提升品牌海外影响力。
- **供应链管理**：企业需要以集成供应链计划为主线，重塑供应链管理体系，优化全球供应链布局，构建系统平台一体化联动供应链各业务计划的制定和调整，并通过数据共享和实时监控，实现供应链的可视化管理，提高响应速度和成本效率，提高供应链服务水平。
- **产品研发**：为了在全球市场中保持竞争力，企业需要将全球研发资源进行有效整合，并通过全生命周期管理支持产品研发。通过全球各地研发团队的协同合作，企业可以加速创新过程，开发出符合全球市场需求的产品。进一步拓展本土化产品时，企业需要深入理解全球及各区域市场的用户需求并进行优先级排序，再针对不同区域市场进行本地化产品开发和适应。

产业抱团

企业通过与产业链上下游公司结成战略合作伙伴关系，共同拓展国际市场，提升整个产业在全球的领先地位和综合布局，促进产业链上的企业在国际市场上协同发展，形成竞争优势和协同效应。通过共享资源，提升产业链整体能力、分担海外不确定性风险，并在海外市场中形成更强的竞争力。

通过以上能力建设，全球化公司业务布局的制定和实施变得更加清晰和具体，企业可以实现全球市场的资源整合、业务风险的分散、市场份额的扩大以及品牌的国际化提升，从而在激烈的国际竞争中获得持续的增长和长期的竞争优势。

4.1.4 搭运营

从运营视角来看，中国企业在出海过程中面临诸多挑战。首先，总部与海外分支机构之间的管控模式不清晰，导致各市场各自为政，形成了大量个性化的业务场景、流程和管理方法，极大地增加了管理复杂度。其次，企业在海外拓展时往往侧重于业务扩展和人员外派，而忽视了运营体系的建设和国际化人才梯队的发展，这使得企业在全球运营中缺乏统一的标准和有力的支撑。最后，随着地缘政治和政策因素的影响日益加剧，企业由于对海外市场在财税、数据安全等领域的法律法规和政策走向缺乏深入了解，面临着较高的业务合规风险。这些问题共同导致企业在全球化进程中运营效率低下，风险增加，影响了企业的国际化发展进程。全球化公司运营战略的核心是为决策层提供全面的运营效率提升方案、资源配置优化建议，为此企业应聚焦如下关键领域：

标准化与本地化

企业应通过建立一套标准化的全球运营框架，同时赋予各地业务一定的自主权，以灵活应对本地市场的变化。这种双轨制的运营模式不仅能够保持全球统一标准，还能够充分发挥本地市场的优势，从而提升整体运营效率和市场响应能力。

- **管控模式与运营架构**：企业需要建立统一的管控模式和运营架构，以确保全球各地业务的一致性和协同性，包括制定全球化组织架构、海外组织的管控与分权，全球统一的管理流程、技术标准和运营规范。但企业也必须考虑到各个市场的独特需求和运营环境，在制定运营架构时赋予各地业务单元一定的自主权，允许其根据当地市场的实际情况进行调整。
- **海外人才治理**：全球化企业需要建立标准化的海外人才治理体系，以确保全球范围内的人才管理符合企业的整体战略，包括统一的招聘流程、绩效评估体系以及培训与人才梯队发展计划。但为了吸引和留住当地人才，企业需要制定符合当地市场的薪酬福利体系和职业发展路径，并积极推动跨文化管理，增强总部与各地团队之间的沟通与协作，以减少文化冲突和误解。
- **全球化财税管理**：企业为满足运营合规、财务稳健和税务优化目标，应开展全球核算体系标准化，建立全球资金管理体系管控资金风险，提升资金利率效率，建设财务共享中心将人力成本和技能组合提升财务运营效率，考虑到各国的税收政策、会计准则和法规存在差异，企业必须根据当地法律法规进行调整，在确保全球业务的合规基础上，优化税务和财务管理，以支持企业的长期可持续发展。

坚守合规底线

合规性是企业持续发展的基础。随着地缘政治的复杂化和各国政策环境的多变性，企业面临着越来越多的合规挑战。坚守合规底线要求企业必须严格遵守各地的法律法规，特别是在财税、数据安全、劳动法和环境保护等关键领域。

通过以上能力建设措施，全球化公司运营策略的制定和实施变得更加清晰和具体，有助于领导者更好地理解并推动运营策略的执行，企业能够有效提升全球运营的效率和适应性，增强竞争力和可持续发展能力。

4.1.5 建系统

从数字化基座而言，许多中国企业在海外扩展过程中，未能提前规划数字化的管控模式、架构设计和部署方式，而是随着业务需求的变化自由建设。这种缺乏前瞻性规划的做法，往往导致企业在业务发展到一定阶段后，发现架构问题已积重难返，不得不付出高昂的代价进行改造和整合。此外，许多企业对海外市场的数字化技术和工具应用了解不足，导致数字化体系和架构滞后于业务发展的实际需求，进而阻碍了企业的业务拓展和运营效率。全球化公司数字化基座的核心是为决策层提供实时、精准的数据支持与分析工具，帮助他们在全球范围内做出明智的战略决策，通过构建一个高度集成和灵活的数字化平台，企业可以实现全球运营的统一管控、资源的高效配置以及市场变化的快速响应。为确保数字基座的有效规划和执行，企业需聚焦如下关键领域：

顶层设计

在构建中国企业出海的数字化基座时，企业需要确保数字化基座的设计与公司整体发展战略紧密对接。顶层设计不仅要考虑企业当前的国际化需求，还要具有前瞻性，支持未来的业务扩展和技术创新。此外，顶层设计还需要明确数字化基座的总体架构规划，制定统一的技术标准、数据标准和安全。

- **全球化数据管理**：作为系统落地的基础，主要从数据治理、数据质量管理、数据安全合规、数据架构与技术架构、数据全生命周期管理等方面进行体系化建设，确保企业能够在全球范围内有效地管理和利用数据，支持业务运营、提升竞争力，并确保遵守全球和本地的数据法规。在这一过程中，数据安全和合规至关重要。企业必须确保在全球范围内的数据管理过程中，始终优先考虑数据安全，严格遵守各国和地区的数据法规与合规要求。这不仅是为了保护企业和用户的敏感信息，也是为了避免法律风险，确保企业能够在全球范围内稳健运营。
- **全球化IT系统建设**：为了支持企业在不同国家和地区的业务运营，确保系统的可靠性、可扩展性、安全性以及全球各地的无缝协作，通常从IT架构设计、基础设施布局、网络与通信、应用与服务管理、运维与支持等方面系统化地设计和实施IT建设框架，企业能够确保其全球业务在不同国家和地区都能高效、稳定、安全合规地运营，并且通过模块化设计和云技术来增强系统的弹性和适应未来技术变革的能力，灵活应对未来挑战的能力。

科技赋能

企业需要通过安全的混合云的架构，建设开放的互联互通的企业生态，借助标准化的智能流程和用户体验实现业务敏捷，借助AI来促进创新与突破。

- **安全与合规保障**：科技赋能还需高度关注数据安全和合规性。企业必须部署先进的网络安全技术，如数据加密、身份验证、多因素认证等，来保护全球范围内的数据安全。同时，数字化基座必须符合各地的数据保护法律法规，以避免法律风险。
- **安全的混合云架构**：企业在全球化过程中，需要构建一个安全的混合云架构，以支持不同市场的业务需求。混合云架构结合了公有云和私有云的优势，既能够提供灵活的资源调度和全球化的业务覆盖，又能够满足各地数据主权和安全合规的要求。通过混合云架构，企业可以实现IT资源的弹性扩展，快速响应业务变化，同时保障敏感数据的安全性。
- **先进技术应用**：在数字化基座的建设中，科技赋能是提升系统能力和业务敏捷性的关键。通过AI技术，企业可以在多个领域实现智能化的转型，如智能客服、精准营销、供应链优化、产品推荐和风险管理等。AI还可以通过大数据分析和机器学习模型，帮助企业更好地理解全球市场趋势、预测客户需求，从而做出更加精准的战略决策。
- **生态开放**：为了支持全球业务的协同和扩展，企业需要建设一个开放的互联互通的企业生态系统，包括建立开放合作平台、开放API接口，支持与合作伙伴、客户和供应商的系统集成，实现数据和业务流程的无缝衔接。

通过以上能力建设措施，中国企业可以构建一个强大而灵活的全球数字化基座，这一基座不仅能够支持企业在全球市场中的复杂运营，还能通过技术创新和数据驱动的决策，支持企业全球化运营的复杂需求，还为企业在国际市场中实现敏捷业务运营和持续创新提供了强有力的技术保障。

数据安全与合规体系 4.2

在当今全球化日益加深的经济环境中，各行各业都面临着前所未有的机遇与挑战，将目光投向海外市场，以实现业务的跨越式增长。在这一浪潮中，企业出海已不再是少数大型企业的个体行为，而是成为了众多企业转型升级、实现跨越式发展的必经之路，数据安全与合规成为了不可或缺的关键要素。

4.2.1 企业出海数据现状概览

企业出海已成为众多企业寻求新增长点、实现国际化战略的重要途径。然而，随着企业逐步深入全球市场，面临的安全与合规挑战也随之增加。为了更好地把握企业出海的脉搏，需要明确企业出海的数据现状概览，首先需要梳理企业出海的典型业务场景，从而明确企业出海过程中需要重点关注的数据对象，进而绘制企业出海的数据流转地图，满足企业出海的分类分级要求，规避风险，稳健前行。

企业出海典型业务场景

在深入梳理企业典型的出海业务场景时，我们需从企业战略、业务布局、运营搭建、系统落地的关键步骤出发，细致考察其全球化进程的每一步，全面分析企业的出海活动，并基于企业的出海活动识别数据出境的业务场景。通过这样系统性的分析框架，我们能够更加精准地识别出数据出境这一关键环节在不同业务场景下的具体需求，以下是企业出海的典型业务场景：

企业出海典型业务场景一览表

企业出海步骤	企业出海活动	数据出境业务场景	数据出境业务场景说明
定战略	境外资本市场活动	IPO、兼并收购	IPO披露、兼并收购披露等
布业务	跨境业务活动	营销与销售	市场调研、品牌推广、市场营销、公共关系管理等
		产品与研发	产品研发、技术研发、医学研究等
		供应链管理	订单调度、仓库发货、配送路线规划、物流运输等
		渠道管理	渠道合作伙伴选择与谈判、渠道运营支持、渠道冲突解决与关系维护等
搭运营	跨国企业管理活动	客户管理	潜客维护、客户签约、售后服务等
		供应商管理	供应商评估、供应商选择等
		采购管理	采购合同签订、采购订单跟进等
		人事管理	员工招聘、薪酬绩效考核、期权管理等
		财务管理	员工费用报销、个人薪资发放、税收申报等
		档案管理	档案存储与共享、档案销毁与处置等
落系统	境外第三方服务	海外部署	数据中心运营部署、应用系统运营部署等

企业出海关键数据类型

企业出海的业务场景丰富多元，每一个细分领域都蕴含着巨大的市场潜力。伴随着这些业务场景的深化与拓展，海量数据应运而生，包含了市场趋势、消费者行为、产品性能等关键商业信息，通过深入挖掘与分析，能够为企业精准定位市场、优化产品服务、制定高效运营策略提供强有力的支持，从而助力企业在激烈的国际竞争中脱颖而出。

值得注意的是，诸多的业务场景中均涉及到个人信息。不同国家对于个人信息保护、隐私安全及跨境流动的法律法规存在显著差异。因此，企业在出海过程中，必须高度重视并严格遵守属地及目标市场的相关法律法规，确保数据处理与流转的合规性。这要求企业深入了解并适应不同国家的监管要求，确保在拓展业务的同时，有效保护数据安全和用户隐私。具体国家的法律法规概述、合规重点梳理（监管机构、数据本地存储、数据跨境、个人数据保护）及违规处罚案例详见第三章各国家地区数据合规法规概览。

为了更直观的展示如何在业务场景中识别关键数据类型，以中国为例，分析其数据安全与合规方面重点关注的重要数据及个人信息。

- **重要数据**：重要数据监管是国家数据安全分类分级制度的核心，也是国家数据安全工作的重点。2021年9月1日，《数据安全法》实施，首次真正意义上明确了重要数据的内涵，提出了制定重要数据具体目录的要求。2021年11月14日，国家互联网信息办对《网络数据安全管理条例》公开征求意见，专门设立了“重要数据安全”章节，提出了重要数据的定义，并设立了一系列重要数据安全监管制度，是我国系统性建立重要数据保护制度的标志。全国网络安全标准化技术委员会在2024年3月15日发布《数据安全技术　数据分类分级规则》附录G (规范性)重要数据识别指南进一步详细指导重要数据的识别工作。
- **个人信息与敏感个人信息**：2021年8月20日，十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，规范了个人信息与敏感个人信息的定义，着重强调了个人信息与敏感个人信息的处理原则及保护义务。在探讨数据安全与合规议题时，明确区分“个人信息”与“敏感个人信息”显得尤为重要，这不仅关乎不同的法律法规要求，也是意味着采取不同的数据出境路径。2020年3月6日，中华人民共和国国家市场监督管理总局、中国国家标准化管理委员会发布《信息安全技术—个人信息安全规范》（GB/T 35273-2020）进一步详细指导个人信息的识别工作。2024年6月11日，全国网络安全标准化技术委员会发布了《网络安全标准实践指南—敏感个人信息识别指南（征求意见稿）》指导个人信息处理者识别敏感个人信息，规范敏感个人信息处理、出境和保护活动。

基于上述重要数据、个人信息及敏感个人信息识别方法作为指导，企业可以系统地梳理在跨国出境业务场景中可能涉及的重要数据、个人信息及敏感个人信息。这一过程不仅要求深入分析出境场景的具体环节，还需要细致梳理具体环节涉及的具体数据内容，以确保重要数据、个人信息及敏感个人信息识别的全面性和准确性。

企业出海典型业务场景数据类型识别表

数据出境业务场景	业务场景说明	重要数据识别	个人信息识别
IPO、兼并收购	IPO披露、兼并收购披露等	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等	【非敏感】个人基本资料、个人身份信息、个人财产信息、个人通信信息等 【敏感】金融账户信息等
营销与销售	市场调研、品牌推广、市场营销、公共关系管理等	N/A	【非敏感】个人基本资料、个人身份信息、个人通信信息等
产品与研发	产品研发、技术研发、医学研究等	1.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、制作方法等信息；源代码、集成电路布图、技术方案、重要参数、实验数据、测试报告等 2.未公开的科学考察、开发利用数据和影响人员安全进出的数据等 3.重要生物资源数据；微生物耐药基础研究数据等 4. 健康医疗资源数据、批量人口的诊疗与健康管理数据、疾控防疫数据、健康救援保障数据、特定药品实验数据，食品安全溯源标识信息等	【非敏感】个人基本资料、个人教育信息、个人通信信息等
供应链管理	订单调度、仓库发货、配送路线规划、物流运输等	危化品制作工艺、危化品储备地点等	【非敏感】个人基本资料、个人身份信息、个人通信信息等
渠道管理	渠道合作伙伴选择与谈判、渠道运营支持、渠道冲突解决与关系维护等	N/A	【非敏感】个人基本资料、个人身份信息、个人通信信息等
客户管理	潜客维护、客户签约、售后服务等	政府或军工单位客户清单等	【非敏感】个人基本资料、个人身份信息、个人财产信息、个人通信信息等 【敏感】金融账户信息等
供应商管理	供应商评估、供应商选择等	N/A	【非敏感】个人基本资料、个人身份信息、个人财产信息、个人通信信息等 【敏感】金融账户信息等
采购管理	采购合同签订、采购订单跟进等	未公开的产品和服务采购情况等	【非敏感】个人基本资料、个人通信信息等 【敏感】金融账户信息等
人事管理	员工招聘、薪酬绩效考核、期权管理等	N/A	【非敏感】个人基本资料、个人身份信息、个人健康生理信息、个人教育工作信息、个人财产信息、个人通信信息、联系人信息等 【敏感】医疗健康信息、金融账户信息、行踪轨迹信息等
财务管理	员工费用报销、个人薪资发放、税收申报等	N/A	【非敏感】个人基本资料、个人身份信息、个人财产信息、个人通信信息等 【敏感】金融账户信息、行踪轨迹信息等
档案管理	档案存储与共享、档案销毁与处置等	未公开的统计数据、重点企业商业秘密	【非敏感】个人基本资料、个人身份信息、个人财产信息、个人通信信息等
海外部署	数据中心运营部署、应用系统运营部署等	反映关键信息基础设施系统配置信息、核心软件硬件设计信息、系统拓扑、应急源、测评、监测、审计等情况的数据等	【非敏感】个人上网记录、个人常用设备信息等

企业出海数据流转地图

2024年3月22日，国家互联网信息办公室发布《数据安全出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》，两份指南均清晰明确的分解了“数据出境”行为，包含

- 数据处理者将在境内运营中收集和产生的数据传输至境外；
- 数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；
- 符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。

因此，企业开展数据跨境活动时应重点关注下述主要数据传输路径：

- 境内主体通过软件或硬件介质将数据传输至境外，软件介质包括电子邮件、即时通讯软件、FTP、跨境搭建的VPN、API等传输信道等，硬件介质包括U盘、硬盘、刻录数据的光盘、存储条、装载数据的笔记本电脑等；
- 境内主体通过服务器位于海外的信息系统、软件平台存储和上传数据，例如企业使用的信息系统、软件平台或数据库的服务器或云端部署在境外；
- 境内主体经由第三方向境外传输数据，例如境外主体委托境内或境外第三方供应商代为收集境内数据；
- 境外访问部署于境内的服务器/数据库/信息系统/网页，例如境外主体可以在境外对存储于境内的数据进行访问、调取、下载、导出；
- 境外主体数据回传境内。

基于上述主要数据传输路径作为参考，绘制详细的数据流转地图，需要涵盖数据类型、处理活动、处理位置、传输路径等具体内容，更直观地反映数据在国家地区、业务层面和系统层面的流动情况。以下是绘制数据流转地图时应重点关注要素：

- **数据类型梳理**：明确数据的具体内容及数量级，重点关注重要数据、个人信息及敏感个人信息；
- **数据处理活动**：记录数据在流转过程中经历的各类处理活动，如数据采集、存储、加工、传输、删除等。同时，需要标注数据处理的目的和依据的法律条款；
- **数据处理位置**：明确数据处理的位置，包括物理位置（所在国家或地区位置）和虚拟位置（云服务供应商数据中心所在位置）；
- **数据传输路径**：详细描绘数据传输的整个过程，包括数据在境内外的传输路径，以及数据在不同系统、服务器或云平台之间的传输。

企业出海数据分类分级

中国企业出海过程中，加强数据分类分级工作是构建全面数据合规体系的基础，也是保障企业国际化战略顺利推进的重要一环。通过精细化的数据分类分级管理，企业能够有效提升数据安全防护能力，降低合规风险，为国际化发展奠定坚实基础。

2016年11月7日，第十二届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国网络安全法》，明确规定“国家建立数据分类分级保护制度”，并要求对数据实行分类分级保护。2024年3月15日，全国网络安全标准化技术委员会发布GB/T43697−2024《数据安全技术数据分类分级规则》，规定了数据分类分级的原则、框架、方法和流程，给出了重要数据识别指南，指导数据分类分级工作有效开展。

- **数据分类**：按照明确数据范围、细化业务分类、业务属性分类、确定分类规则的“四步法”开展数据分类工作。数据按照先行业领域分类，再业务属性分类的思路进行分类。按照行业领域，将数据分为工业数据、电信数据、金融数据、能源数据、交通运输数据、自然资源数据、卫生健康数据、教育数据、科学数据等；再根据本行业本领域业务属性，对本行业领域数据进行细化分类，如涉及法律法规有专门管理要求的数据类别 (如个人信息等)，应按照有关规定和标准进行识别和分类。
- **数据分级**：按照确定分级对象、分级要素识别、数据影响分析、综合确定级别的“四步法”开展数据分级工作。数据级别一般根据重要程度和危害程度两个维度判断，重要程度是指数据在经济社会发展中的重要程度；危害程度是指一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度。

影响对象和影响程度参考表

影响对象	影响对象示例	影响程度		
		特别严重危害	严重危害	一般危害
国家安全	影响国家政治、国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等国家利益安全	直接影响政治安全	关系其他国家安全重点领域	直接危害国家安全
经济运行	影响市场经济运行秩序、宏观经济形势、国民经济命脉、行业领域产业发展等经济运行机制	关系国民经济命脉	直接危害宏观经济运行，或对行业领域或地区的经济发展造成严重危害	/
社会稳定	影响社会治安和公共安全、社会日常生活秩序、民生福祉、法治和伦理道德等社会秩序	关系重要民生	直接危害社会稳定	/
公共利益	影响社会公众使用公共服务、公共设施、公共资源或影响公共健康安全等公共利益	关系重大公共利益	直接危害公共健康和安全	/
组织&个人权益	**组织权益**：影响组织自身或其他组织的生产运营、声誉形象、公信力、知识产权等组织权益 **个人权益**：影响自然人的人身权、财产权、隐私权、个人信息权益等个人权益。	如果影响大规模的个人或组织权益，需要同时研判会否会对国家安全、经济运行、社会秩序或公共利益造成影响及影响程度		

不同行业在开展数据分类分级工作时，除了遵循通用的数据分类分级法律法规以及国家标准外，还应特别遵循各行业的法律法规及标准，行业法律法规及标准通常更加细致和具体，能够针对行业的特殊性和业务需求提供更有针对性的指导，以确保数据能够得到有效保护、合理利用和合规处理。

行业法律法规及标准梳理表

行业	发布时间	发布机构	文件名称	主要内容
金融行业	2018年	中国证券监督管理委员会	《证券期货业数据分类分级指引》（JR/T 0158-2018）	明确根据数据泄露或损坏造成的影响将数据分为不同级别，为证券期货业的数据安全提供分级方法
	2020年	中国人民银行	《金融数据安全分级指南》（JR/T 0197—2020）	明确金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程，指导金融业机构开展数据安全分级工作，以及第三方评估机构等参考开展数据安全检查与评估工作，建立数据分类分级标准
	2023年	国家市场监督管理总局和国家标准化管理委员会	《证券期货业数据安全风险防控 数据分类分级指引》（GB/T 42775-2023）	为证券期货行业机构提供一种规范的数据分类、分级方法，指导机构有效甄别数据类型，依据数据重要性或敏感度确定数据级别，从而对不同类别、等级的数据有针对性地采取适当、合理的管理措施和安全风险防控措施
	2024年	国家金融监督管理总局	《银行保险机构数据安全管理办法（征求意见稿）》	明确要求银行保险机构制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，并采取差异化的安全保护措施
汽车行业	2020年	工信部	《车联网用户个人信息保护要求》（YD/T3746-2020）	明确车联网信息服务用户个人信息保护的信息内容分类、敏感性分级和分级保护要求，适用于车联网相关的汽车厂商、零部件和元器件供应商、软件提供商、数据内容提供商和服务提供商等在提供服务过程中的用户个人信息保护
	2020年	工信部	《车联网数据安全技术要求》（YD/T3751-2020）	明确对车联网信息服务数据进行了分类分级，将数据划分为不同的敏感性等级，并按照等级的不同实施相应的安全保护措施，规定了数据生命周期内的安全保护要求

制造行业	2020年	工信部	《工业数据分类分级指南（试行）》	指导企业全面梳理自身工业数据，提升数据分级管理能力，促进数据充分使用、全局流动和有序共享
	2022年	国家市场监督管理总局和国家标准化管理委员会	《智能制造工业数据分类原则》（GB/T 42128-2022）	明确智能制造工业数据的分类要求、分类依据以及分类维度，适用于指导智能制造领域工业数据分类
	2022年	工信部	《工业和信息化领域数据安全管理办法（试行）》	明确工业和信息化领域数据分类分级、重要数据和核心数据识别认定、数据分级防护等标准规范，指导开展数据分类分级管理工作，制定行业重要数据和核心数据具体目录并实施动态管理
通信行业	2014年	中华人民共和国工业和信息化部	《电信和互联网服务 用户个人信息保护 定义及分类》	明确用户个人信息保护的术语和定义、保护范围、信息内容和分类，初步提出了用户个人信息分类的方法
	2020年	工业和信息化部	《基础电信企业数据分类分级方法》（YD/T 3813-2020）	进一步提出了数据分类分级的具体方法和要求，有助于电信企业更好地开展数据安全管理工作
	2022年	中国信息产业商会	《数据技术 数据 数据资源分类分级指南》（T/CIITA 409-2022）	明确数据资源分类分级总则、分类分级方法、分级管控措施以及分类分级的实施流程，适用于数据要素金库的设计、建设和运行过程中，对数据资源的分类分级进行管理，也可以为政府、组织和企业在开放和共享本单位数据资源时，构建科学合理的分类分级体系提供指导
	2023年	工信部	《电信网和互联网数据分类分级技术要求与测试方法》（YD/T 4244-2023）	明确电信网和互联网数据在分类分级过程中所需技术的相关要求和对应的测试方法，适用于企业、组织或机构在实施数据分类分级过程中对相关技术工具或产品的设计、开发、测试、评估
医疗行业	2020年	国家市场监督管理总局和国家标准化管理委员会	《信息安全技术 健康医疗数据安全指南》（GB/T 39725-2020）	明确数据分类范围、数据分级方法及数据安全管理原则，以信息安全为出发点，对健康医疗数据进行分类分级，促进信息开发利用
	2023年	国家卫生健康委员会	《卫生健康信息数据集分类和编码规则》	明确卫生健康信息数据集分类与编码需遵循的基本原则、技术方法以及应用规则，适用于卫生健康领域各类卫生健康信息数据集分类与编码方案的制定
互联网行业	2021年	全国信息安全标准化技术委员会秘书处	《网络安全标准实践指南-网络数据分类分级指引》	明确网络数据分类分级的原则、框架和方法，可用于指导数据处理者开展数据分类分级工作，也可为主管监管部门进行数据分类分级管理提供参考
	2023年	工信部	《电信网和互联网数据分类分级技术要求与测试方法》（YD/T 4244-2023）	明确电信网和互联网数据在分类分级过程中所需技术的相关要求和对应的测试方法，适用于企业、组织或机构在实施数据分类分级过程中对相关技术工具或产品的设计、开发、测试、评估
传媒行业	2022年	中国市场信息调查业协会	《媒体大数据分类分级指南》（T/CAMIR 003-2022）	明确媒体大数据分类分级原则、媒体大数据分类和媒体大数据分级的建议，适用于指导媒体大数据活动中的分类分级
航空行业	2022年	民航局	《民航领域数据分类分级办法》	旨在规范民航数据的收集、存储、使用、加工、传输、提供、公开等活动，保障数据安全，促进数据共享，激发数据价值，提升行业治理能力和服务水平
航洋行业	2023年	中国自然资源部	《海洋数据分类分级标准》（HY/T 0366-2023）	明确海洋数据资源的分类分级原则，给出了海洋数据的分类，描述了相应的分级方法，适用于海洋数据采集、处理、存储、交换以及海洋信息系统建设等工作

为了满足企业出海的安全与合规要求并推动安全与合规要求有效落地，企业需要从管理组织、制度流程、技术体系、运营体系等方面的全面布局，系统化地建立数据安全与合规体系。



4.2.2 全球化数据合规管理组织

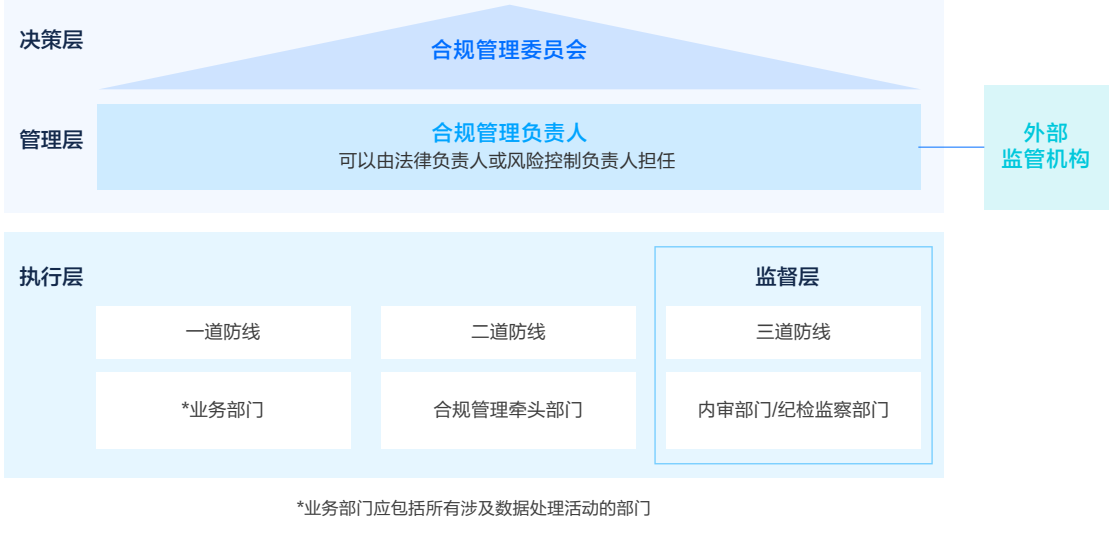
数据安全合规全球组织

中国企业在海外拓展业务时，构建数据合规的跨境组织结构至关重要。这需要在满足中国本地法规的同时，与境外分支机构建立紧密的联系，确保两者之间的有效协同与沟通，满足多地域合规要求。

数据安全合规组织

在发展改革委、外交部、商务部等部门共同制定的《企业境外经营合规管理指引》文件中，明确给出了在中国企业在开展境外经营时，对于合规管理架构的建议。结合实际经验，在构建数据合规组织时，可以采取分层管理的策略，在决策、管理、执行、监督四个层级上划分相应的合规管理责任。在实际执行过程中，企业也可利用现有资源，赋予已有团队与其它相关部门数据合规的工作职能，或通过第三方专业团队开展工作。

数据安全合规组织架构图



*业务部门应包括所有涉及数据处理活动的部门

- **决策层**：企业可结合实际设立合规委员会，作为企业合规管理体系的最高负责机构。合规委员会一般应履行合规职责包含：确认合规管理战略，明确合规管理目标；建立和完善企业合规管理体系，审批合规管理制度、程序和重大合规风险管理方案；听取合规管理工作汇报，指导、监督、评价合规管理工作。
- **管理层**：管理层应分配充足的资源建立、制定、实施、评价、维护和改进合规管理体系。在组织架构中发挥承上启下的重要作用，负责做好数据合规全面落地工作，是公司内开展数据合规工作最核心的部分，在资源不足的情况下，部分工作可能需要联合组织外部的专业团队来共同完成。其主要职责包含但不限于：基于决策层给出的合规策略，对数据合规实际工作制定详细方案；制定与各部门之间的数据合规工作机制，保障数据合规工作顺利开展，协调落实数据安全管理运作机制等。
- **执行层**：各执行部门以及境外分支机构与管理层在数据合规管理工作中需要建立一种协同紧密的关系，其职责主要是聚焦每一个数据合规管控的场景，逐一实现设定的安全合规流程，落实流程中的合规管控点。执行层主要包括负责数据合规的专职人员和各业务部门的数据合规接口人员、风险管理人员、数据所有者、数据使用者等，其主要工作包含但不限于：识别归口管理领域的合规要求，改进合规管理措施，执行合规管理制度和程序，收集合规风险信息，落实相关工作要求等。
- **监督层**：监督层应当确保独立性，监督层人员通常由企业审计部门成员组成，负责进行内部审计，或委托独立的第三方外部审计对数据合规管理工作开展审查监督，并对已发现的数据合规管理工作的缺失或不足提出改进建议。主要职责为审查监督各项数据合规方针、制度与规范、指南与细则的执行情况。

数据合规关键人员

- **中国总部关键人员**

  数据安全责任人：根据《中华人民共和国数据安全法》以及相关法律法规的要求，对于以经营为目的收集重要数据或个人敏感信息的网络运营者应当设立数据安全负责人，并非所有企业都需设置该角色。数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，并且有权直接向网信部门和主管、监管部门反映数据安全情况。

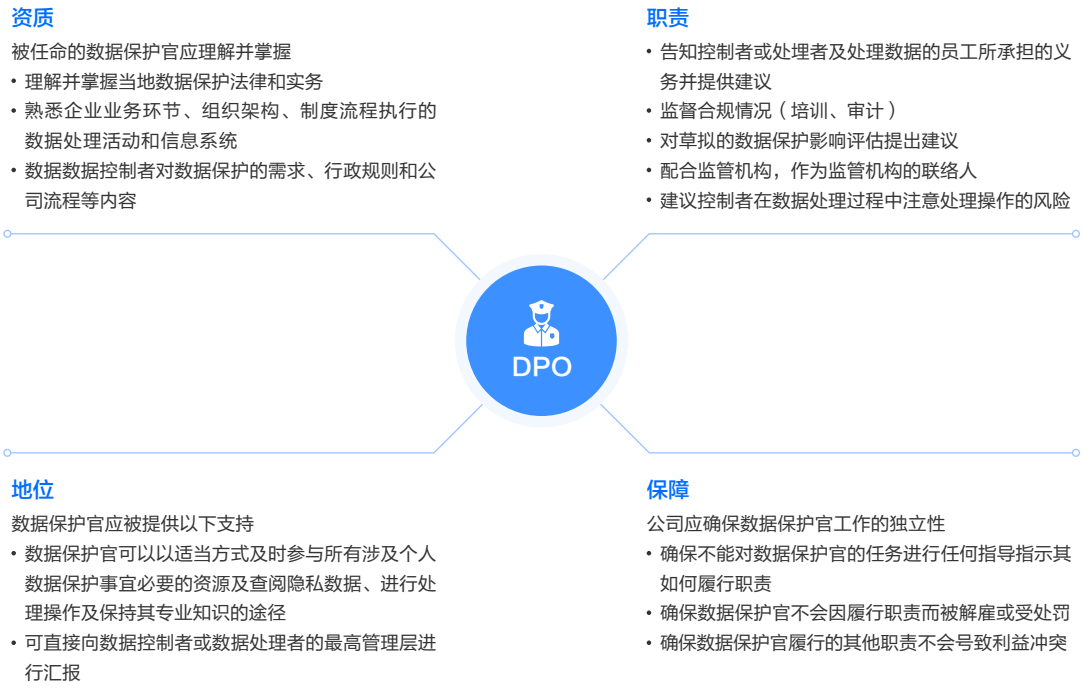
  个人信息保护负责人：根据《中华人民共和国个人信息保护法》第52条规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当设立个人信息保护负责人，但“国家网信部门规定数量”目前尚未明确。考虑到合规风险，建议企业设立个人信息保护负责人以满足合规要求。个人信息保护责任人主要负责对个人信息处理活动以及采取的保护措施等进行监督。同时，法律要求个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

  在实务中，数据安全负责人与个人信息保护负责人的工作职责存在一定的交叉和重合，“数据安全”和“个人信息保护”概念存在包含、重叠的关系，企业在权衡合规成本等多重因素后，可以考虑选拔一名具备相应资质的员工，使其同时担任两个关键职位。

- **境外分支机构关键人员**

  数据保护官（DPO）：根据出海目标国家/地区的法律要求，应设置境外分支机构DPO。在实践过程中，若该国家/地区境外分支机构确定无需设立 DPO，公司可以选择在有此要求的不同司法管辖区内任命一名或多名 DPO为无需设立 DPO的分支机构提供合规指导。

境外分支机构关键人员



数据安全合规职责矩阵

数据安全合规工作不应仅由数据合规管理团队独立承担，企业应当树立全员参与的安全合规文化，将数据安全合规视为每个部门、每位员工的共同责任。建议企业对安全合规任务进行细致的拆解后，利用RASI模型，如下图所示，明确每个部门的职责所在，并进一步将这些职责落实到具体的岗位职责中，形成数据安全合规职责矩阵。这样，从顶层设计到日常操作，每个环节都能够体现对安全合规的重视，确保企业在各个层面上都能够达到法律法规的要求，构建起一张严密的数据安全合规网络。通过这种自上而下、由内而外的整合，企业能够更有效地管理和降低运营风险，保障企业的可持续发展。

RASI模型图



数据安全合规人员教育

数据安全合规培训和教育是构建安全、可靠工作环境的基石，对公司和个人都具有长远的影响。通过人员培训和教育有助于提升公司员工个人对数据保护法规和公司政策的理解，且增强了他们识别和预防数据违规行为的能力，从事数据安全合规的人员能够更好地保护公司免受数据泄露和不当使用的风险，从而维护公司的声誉和客户信任。此外，安全合规教育还有助于确保业务流程的顺畅和法律遵从性，避免因违规而产生的潜在罚款和法律诉讼。

结合NIST SP 800-50的建议以及实践中的需求，对人员的培养建议分为意识、培训、教育三种类别，三种类型的安全学习培训特点如下图所示。

- **“意识教育”**专注于某一具体的主题，目的是将注意力集中在合规性上，旨在让个人认识到数据合规问题并做出相应的响应。
- **“培训”**致力于培养相关且必要的技能和能力，为相关领域的从业者提供所需的安全技能和能力。
- **“教育”**则是将各种职能专业的所有安全技能和能力整合到一个共同的知识体系中，增加了对概念、问题和原则（技术和社会）的多学科研究，目标是培养具有远见和主动响应的合规安全专家和专业人员。

意识、培训与教育之间的特点比较

三种类型的安全培训学习的特点比较			
方式	意识	培训	教育
属性	What	How	Why
级别	Information 信息	Knowledege 知识	Insight 洞察
学习目标	认知和记忆 意识演示旨在让个人认识到 IT安全问题并做出相应的响应	素养与技能 指个人对保护数据和系统所需的IT安全基础知识的熟悉程度和应用能力	理解 进行基于角色的安全技能教育
教学方法示例	媒体 ☒视频 ☒简报 ☒海报	实践指导 ☒讲座/演示 ☒案例研究 ☒动手练习	理论指导 ☒研讨会 ☒研究 ☒阅读和学习
测试手段	真/假；多选题（识别性学习）	解决问题（运用性学习）	小论文（解读性学习）
影响时间	短期	中期	长期
价值	IT安全意识计划的基本价值在于，它们通过改变改变组织文化的态度，为培训奠定了基础。文化变革是认识到IT安全是关键，因为安全故障可能会对每个人产生不利影响。因此，IT安全是每个人的工作。	所有使用计算机技术或产品的个人，无论其具体工作职责如何，都必须了解IT安全基础知识并能够应用它们。	IT安全培训的需求随着角色的变化而变化

在实践过程中，建议公司对全体成员定期进行数据合规意识培训，确保全体成员了解所在国家数据保护合规要求以及公司数据合规保护策略。同时，应具体区分数据合规工作角色（如：数据保护官、法务顾问、技术专家/IT安全专家、数据合规专员、合规审计师等），建立基于角色的学习体系，针对不同角色提供差异化的培训内容。在可行的情况下，公司内部提供的培训可以扩展到业务合作伙伴和供应商，要求其同意遵守公司的制度和适用的法律，确保公司数据合规方针、策略有效传递至各利益相关方。

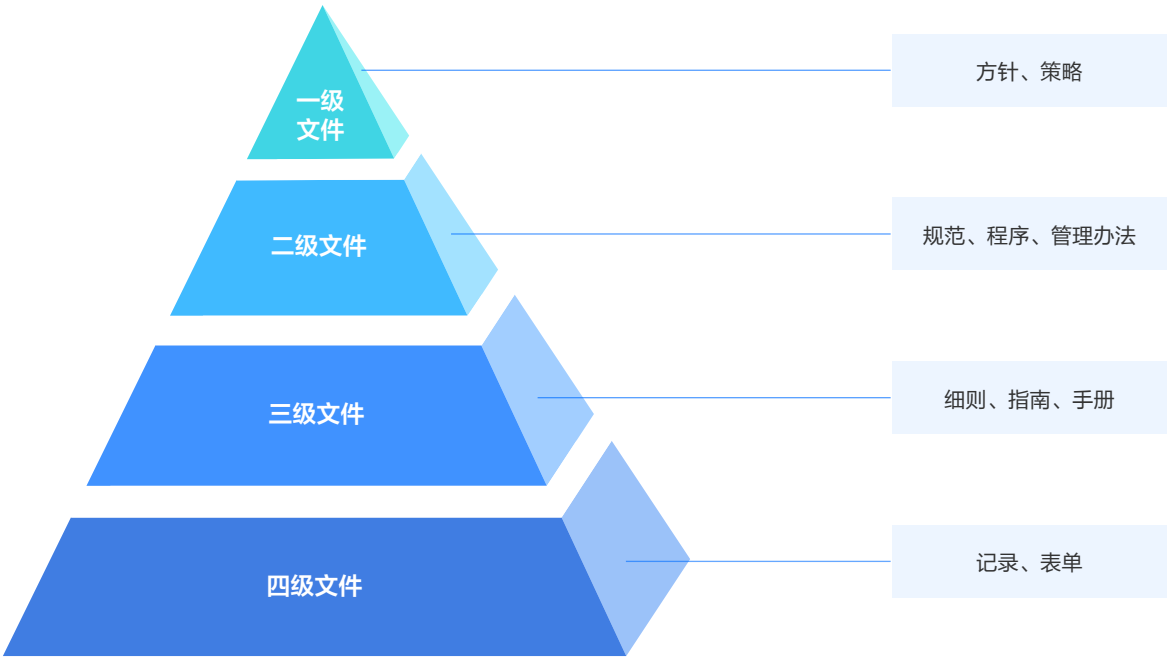
除此之外，对于全体员工，可通过在线考核系统或其他途径定期发布测验和评估任务，以此来衡量员工在通用数据安全合规理论知识上的掌握程度。同时，对于数据安全合规团队而言，建议适当进行合规实战演练，将团队成员在模拟实战环境中的操作表现纳入关键考核要素，综合评定数据安全合规团队的专业技能和实践能力。这种综合评估机制有助于完成人员培养的循环建设，确保团队能力的全面提升和持续改进。

4.2.3 数据合规管理制度与流程

数据安全与合规管理制度体系

在建立全球标准化的企业统一数据合规管理制度与规范体系时，应全面覆盖跨境数据的整个生命周期，从数据的收集、存储、处理、传输、使用到最终销毁或归档的每一个环节。企业应当识别数据合规管理的法律法规要求，并深入参考行业标准和公司顶层战略规划，结合企业实际情况制定适用于企业内部环境的制度规范。这些制度规范旨在明确界定相关人员的职责与权限，明确数据管理目标和范围，规范日常工作中涉及数据处理的行为，并赋予管理人员必要的监督与管理职责，以确保企业数据合规工作的有效执行与持续优化。

数据合规管理制度体系



在构建数据合规管理制度体系时，需要全面考虑并设计结构化的体系框架，如下图所示，一般分为四个层级，各级之间逐层细化，同级不同模块之间相互关联。

- **一级文件**：规定了数据合规管理与数据跨境的方针、策略、战略目标、基本原则和总体管理要求；
- **二级文件**：是对一级文件的支撑和细化，在数据合规管理、个人信息保护和数据跨境合规方面展开，主要内容包括但不限于：数据资产管理和数据分类分级要求、数据及个人信息生命周期阶段划分和各阶段管理要求和流程、数据合规管理违规处理、个人信息保护影响评估、个人信息主体权利响应等、数据跨境管理要求等。
- **三级文件**：是对二级文件的扩展和补充，包含数据合规管理各生命周期及某个特定领域的管理要求细则、实施流程、相应的作业指导书、指南等。管理要求细则是对二级管理要求的细化和展开，详细规定了某个特定领域的具体要求；实施流程规定了开展某项工作的内部流程；作业指导书和指南属于指导性文件，并非强制要求，为执行者开展某项工作提供指导和建议。
- **四级文件**：指执行数据合规管理过程中产生的模板、表格、报告、各种运行或检查记录等，与二级和三级文件配套使用，确保执行一致性。

建议的数据安全与合规管理制度体系包含内容如下图所示：

数据合规管理制度内容

数据安全与合规管理制度体系			
一级	数据合规治理总体政策		
二级	数据合规管理规定	个人信息保护管理规定	数据跨境合规管理规定
三级	数据生命周期安全管理细则 数据分类分级管理细则 数据安全审计细则 数据安全风险评估细则 数据脱敏指南 数据共享及外发审批流程	个人信息生命周期管理细则 个人信息影响评估指南 个人信息主体权利响应指南	数据出境安全管理细则 数据出境安全评估流程 数据出境合规审计指南 数据出境申报指南 ……
四级	数据保护协议 数据安全风险评估报告 数据安全审计报告 数据导出申请表 数据安全关键岗位责任书模版	个人信息主体权利响应处理记录 个人信息处理活动清单 个人信息影响评估报告 个人信息删除记录	数据出境业务识别表 数据出境安全自评估表 数据出境评估报告 数据出境安全评估申报材料 数据出境合规审计报告 ……

各国家/地区分支机构制度体系本地化建设

在建立企业海外分支机构本地化数据合规管理制度与规范体系时，需要重点识别海外分支机构所在国家的法律法规要求，依据集团统一的制度规范，建立本地化的数据合规管理制度体系。具体方法如下：

- **明确法律法规要求**：深入研究分支机构所在国家的数据保护法律、隐私法规以及其他与数据跨境流动相关的法律要求，关注不同国家之间的法律差异，特别是对数据定义、分类、处理、存储、传输等方面的具体要求。并识别并分析在数据跨境过程中可能面临的合规风险，包括违反当地法律、监管处罚、损害公司声誉等。
- **制定本地化策略**：根据目标国家的法律法规要求，对国内总部的数据管理制度进行必要的调整和优化，确保调整后的制度能够完全符合当地法律要求，并保持与总部整体数据管理体系的一致性。针对数据跨境流动的具体环节（如数据收集、处理、存储、传输等），制定符合当地法律要求的操作流程和规范，并引入必要的审批和监控机制，确保数据跨境流动过程的合规性。
- **落实制度要求并监督**：对分支机构员工进行数据保护法律法规和合规制度的培训和教育，提高员工的合规意识和能力。定期对分支机构的数据跨境流动活动进行合规审查，确保各项制度和流程得到有效执行，并对发现的问题及时进行整改和纠正，防止合规风险的发生。建立数据跨境流动的持续监督机制，关注当地法律法规的更新和变化，及时调整和优化合规策略和措施。

4.2.4 数据合规技术体系

数据安全合规技术需求

目前，在全球数字化浪潮的推动下，各国政府及立法机构均深刻认识到数据安全与合规的重要性，纷纷通过制定和完善相关法律法规，明确要求采用先进且有效的技术措施来保障数据处理活动的安全合规性。这一趋势不仅体现了对公民个人数据权益的尊重与保护，也促进了数字经济健康有序的发展。

以欧盟为例，其颁布的《通用数据保护条例》（General Data Protection Regulation， GDPR）堪称全球数据保护领域的标杆。GDPR不仅规定了严格的个人数据保护原则，还明确提出了技术与组织措施（Technical and Organizational Measures，ToMs）的概念，要求数据控制者和处理者必须实施适当的技术和组织措施，以确保数据处理活动的合法、公平、透明，并保护个人数据免受未经授权的访问、泄露、篡改或损坏。这些措施包括但不限于数据加密、访问控制、定期安全审计、员工培训以及应急响应计划等，旨在构建一个全方位、多层次的数据安全防护体系。

同样，中国作为数据大国，也高度重视个人信息保护。在《中华人民共和国个人信息保护法》中，明确规定了个人信息处理的基本原则，特别是针对敏感个人信息的处理，提出了更为严格的要求。该法要求个人信息处理者在处理敏感个人信息时，必须采取加密、去标识化等安全技术措施，以降低数据泄露和滥用的风险。此外，还强调了个人信息处理活动的透明度、目的明确性、最小化收集以及个人同意等原则，为个人信息保护提供了坚实的法律基础。

通过对数据安全合规领域的主要法律法规和监管文件进行深入分析，为了更好地指导企业实践，我们可以从数据生命周期和数据级别两个维度进行映射，从而识别出主要的数据安全与合规技术原子化需求：

数据生命周期中的合规技术需求

	收集	传输	存储	使用	删除
核心数据	• 数据源合规 • 个人信息收集告知同意 • Cookie授权 • 数据分类分级 • 完整性校验 • 设备/系统增强验证 • 缓存清理 • 数据与通道加密 • 日志记录	• 通讯网络安全 • 接口认证 • 双向身份认证 • 抗抵赖、完整性校验 • 数据与通道加密 • 缓存清理 • 日志记录	• 本地化存储 • 数据保密性(整库、字段与文件) • 数据完整性 • 不同类别个人信息隔离存储 • 访问控制 • 数据恢复测试 • 数据防泄漏	• 访问控制、多因素认证 • 数据导出跟踪溯源 • 数据脱敏与匿名化 • 接口安全 • 隐私影响评估 • 数据处理活动记录 • 隐私计算 • 日志记录与分析	• 数据主体请求删除 • 达到保存期限删除 • 系统下限删除 • 数据安全擦除 • 物理销毁 • 日志记录与审计
重要数据	• 数据分级 • 完整性校验 • 设备/系统增强验证 • 数据源合规 • 个人信息收集告知同意 • Cookie授权 • 缓存清理 • 采集通道加密 • 日志记录	• 通讯网络安全 • 终端准入 • 抗抵赖、完整性校验 • 传输通道加密 • 缓存清理 • 物理介质传输加密/脱敏 • 日志记录	• 数据保密性 • 数据完整性 • 不同类别个人信息隔离存储 • 访问控制 • 数据恢复测试 • 数据防泄漏	• 访问控制、多因素认证 • 数据加密(导出、委托) • 数据脱敏(导出、公开、外发、展示、委托)与匿名化 • 数据水印(展示、委托处理) • 接口安全 • 隐私影响评估 • 隐私计算 • 日志记录与分析	• 数据主体请求删除 • 达到保存期限删除 • 数据安全擦除 • 物理销毁 • 日志记录与审计
一般数据	• 完整性校验 • 设备/系统真实性验证 • 个人信息收集告知同意 • Cookie授权 • 采集通道加密 • 日志记录	• 通讯网络安全 • 抗抵赖、完整性校验 • 传输通道加密 • 缓存清理	• 数据保密性 • 不同类别个人信息隔离存储 • 访问控制 • 数据恢复测试	• 访问控制、身份认证 • 超范围使用再次征得同意 • 接口安全 • 隐私影响评估 • 隐私计算 • 日志记录与分析	• 数据主体请求删除 • 达到保存期限删除 • 数据安全擦除 • 物理销毁 • 日志记录与审计

数据安全合规技术支撑

企业在面对日益复杂且碎片化的数据合规要求时，往往面临着一系列挑战。为了有效应对这些挑战，企业应当采取一种更为高瞻远瞩的策略，站在企业级视角来审视和规划其数据安全与合规体系，避免形成孤立的“竖井式”系统，充分复用已有的网络安全能力，结合数据隐私合规个性化要求，统筹考虑集约化、共享化数据安全合规技术支撑建设，从而实现资源的优化配置和效率的最大化。

为了实现这一目标，企业可以基于NIST IPDRR（识别、保护、检测、响应、恢复）框架模型，从体系化、结构化的视角出发，设计一套全面而灵活的数据安全合规管理工具，够覆盖数据生命周期的各个阶段，确保每个环节都符合合规要求，并建设数据安全合规管理系统，形成纵深防御的战线，为数据本地合规、数据跨境合规、数据共享合规等场景供应技术保障能力。



- **数据资产分级与打标**

  - 痛点与问题

    企业出海涉及数据跨境、数据合作、数据共享、自动化决策等数据处理活动时，业务部门往往不确定针对哪类数据采用何种措施确保数据处理的安全合规，即使已有数据分类分级标准，但仍然难以落实到具体的数据场景中，导致相关的合规评估与审批流于形式，未能实际控制数据安全与合规风险。

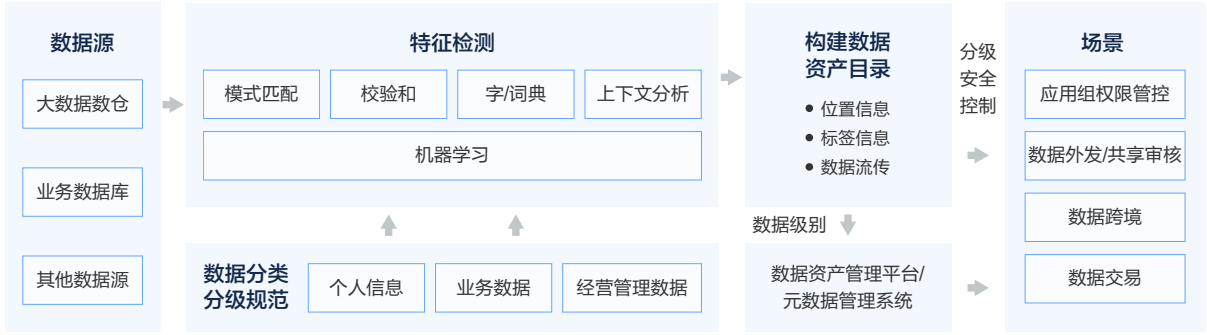
  - 目标与定位

    对数据跨境场景中涉及的数据资产进行盘点和分类分级是开展合规动作的基础，分类分级是对企业范围内的数据资产进行盘点并依据分级标准识别安全等级，从而在各类数据处理场景中实现基于数据等级的差异化安全与合规管理。

  - 功能与内容

    数据分类分级的过程包括数据资产识别，基于分类分级规范分析数据资产，开展分类分级形成数据资产分类分级清单，以及对数据资产进行打标。

分类分级打标模块示意图



数据资产发现：

数据资产发现的主要实现方式为利用自动化技术手段对数据进行筛选与分析，找出符合数据资产定义的数据集，自动化梳理和识别出资产保护目录。数字资产的识别技术主要包含关键字、正则表达式、基于文件属性识别、精准数据比对、指纹识别和支持向量网络等；

数据资产分析处理：

数据资产分析处理指在数据清洗的基础上，针对已采集和识别的重要数据资产和个人信息进行合规和安全处理。通常，数据资产处理（分析）要首先对数据内容进行识别，然后再进行安全性分析、合规性分析、重要性（敏感性）分析等，能够为了对敏感数据进行控制和管理。如在数据传输时，部署数据过滤网关类工具，发现和拦截违规、异常数据；

数据分类分级：

数据分类指根据数据的属性或特征，将其按照一定的原则和方法进行区分和分类，并建立起一定的分类体系和排列顺序，以便更好地管理和使用组织数据的过程。数据分级指按照一定的分级原则对分类后的数据进行定级，从而为数据的跨境传输和共享安全策略提供支撑。

  - 落地工具

    结合自动化工具，将分类分级的专家经验和方法固化为规则模型和识别引擎，辅助人工核验的方式，实现高效分类分级。数据分类分级主要实现方式为依据标签库、关键词、正则表达式、自然语言处理、数据挖掘、机器学习等内容识别技术，进行数据分类，根据数据分类的结果，依据标签进行敏感数据的划分，最终实现数据分级的效果。关于数据资产分级分类的具体技术方案和产品实现，请参考5.3.6.1小节“资产管理与分级分类”的内容。

- **数据主体授权管理**
  - 痛点与问题

    告知同意规则作为个人信息处理中最基本的法律规则，是在处理个人信息时，均应向其个人信息告知相应的事项，并在取得该个人（或者其监护人）的同意后，方可从事相应的个人信息处理活动。然而数据主体授权管理面临的主要问题在于透明度不足、流程复杂及权利保护挑战。数据主体常因信息告知不充分而难以做出明智授权决策，复杂的授权流程又增加了操作难度和成本。同时，权利保护机制的不完善让数据主体担忧数据滥用与泄露，影响信任度。
  - 目标与定位

    数据主体授权和偏好管理应作为隐私工程的一部分，旨在管理获取数据主体同意的流程，并与数据主体就其现有和未来的偏好进行沟通。
  - 功能与内容

    创建收集点：

    收集点定义最初收集和记录同意的交互点，并且可以设置它们以反映数字交互（例如Web表单和网站横幅、自定义API，线下或大批量数据导入、移动应用等）和模拟交互（例如电话交谈、物理邮件或面对面交互）。可以集成托管SDK以通过Web表单收集点收集同意记录；

    管理数据主体：

    集成收集点后，数据主体与收集点的每次交互都将生成一个凭据，可以使用收据ID或数据主体标识符搜索该凭据。该功能访问用户授权的凭据、交易和数据主体详细信息；

    数据主体偏好管理：

    偏好管理是数据主体用来授予和撤销对目的、主题和自定义偏好的同意，以便数据主体能够在与偏好中心交互时根据需要给予或撤销同意；

    管理数据主体授权：

    人工管理数据主体添加、修改和撤销的同意偏好，以便于数据主体通过模拟方式如电话、书面等，传达所需更改。
  - 落地工具

    数据主体授权的实现主要通过业务应用代码实现，再配合以隐私协议声明的明文提示。可以使用腾讯云的开发者工具来辅助实现，详情请参考官网链接：https://cloud.tencent.com/product/tcap
- **Cookie授权管理**
  - 痛点与问题

    Cookie授权管理面临的痛点在于用户隐私保护与个性化体验之间的平衡难题。一方面，用户担忧Cookie跟踪侵犯隐私，要求更强的控制权和透明度；另一方面，企业依赖Cookie收集数据以优化服务和广告推送。此外，跨域Cookie管理复杂，合规风险高，增加了企业的管理负担。
  - 目标与定位

    Cookie 授权允许发现企业网站上提供的Cookie、本地存储和标签，了解访问者浏览企业网站时收集他们个人信息的方式，可以使用此信息来构建网站横幅和偏好中心，使访问者能够直接控制哪些类别的Cookie可以捕获和处理其信息。

- 功能与内容

  扫描分类：

  扫描网站所使用的Cookie信息，并对Cookie进行分类，是Cookie授权管理的首要任务。这一过程通过自动化的扫描工具实现，能够全面识别并捕捉网站运行中涉及的所有Cookie，包括它们的来源（第一方或第三方）、作用、存储期限等关键信息。系统会根据预设的标准或用户自定义的规则，对这些Cookie进行科学分类；

  统一管理：

  统一管理多个网站的第一方、第三方Cookie，则进一步提升了管理的便捷性和效率。该功能允许用户在统一的平台上，对旗下所有网站或服务的Cookie使用情况进行集中监控和管理。无论是更新Cookie政策、调整授权策略，还是响应合规要求，都能快速部署至所有相关网站，有效避免了逐一手动操作的繁琐和可能导致的遗漏；

  禁止跟踪：

  在用户拒绝Cookie后，系统能够自动禁止第三方Cookie跟踪，保护用户的隐私权益。这一功能通过智能识别用户的偏好设置，在接收到拒绝Cookie的指令后，立即切断与第三方服务的连接，阻止其通过Cookie进行用户行为追踪和数据收集。这样，用户就能在不牺牲浏览体验的前提下，享受到更加安全的网络环境；

  个性化配置：

  为了提升用户体验和降低企业的实施成本，Cookie授权管理也可以提供丰富的模板定制功能。用户可以创建网站模板，为Cookie横幅、偏好中心和Cookie列表等关键界面设计统一的视觉风格和交互逻辑。这些模板不仅支持快捷使用内置的标准化设计，还允许用户根据自身需求进行深度定制，如调整字体大小、颜色搭配、布局结构等。此外，系统还能根据用户选择的地理区域/法域规则，自动适配不同国家和地区的合规要求，确保在全球范围内都能实现合规运营；

  授权脚本：

  实现Cookie授权脚本的部署，是确保上述功能在网站上有效实施的关键步骤。Cookie授权脚本通常是一段嵌入到网站代码中的JavaScript代码，它负责在用户访问网站时执行Cookie扫描、分类、提示用户授权等任务。通过在企业网站上部署这样的脚本，企业就能轻松地实现Cookie的合规使用和管理，为用户提供更加透明、安全的网络浏览体验。

- 落地工具

  企业可以选择腾讯云生态合作伙伴的Cookie授权管理工具实现Cookie授权管理。

• APP合规评估

- 痛点与问题

  随着移动应用作为用户数据收集的主要入口之一，然而APP合规评估面临多重痛点与问题：法规频繁变动，企业难以迅速适应确保全面合规；评估标准复杂，涉及多领域，增加实施难度与成本；技术实现与合规要求间存在差距，易引发风险；跨平台、跨国界合规挑战大，需应对多样法律环境；用户反馈与监管信息不对称，影响违规问题及时处理。这些难题共同构成APP合规评估的严峻挑战。

- 目标与定位

  App数据处理活动中的可能导致数据合规风险，进行App隐私合规评估可以帮助组织识别潜在的隐私风险，确保数据安全性和透明度，并维护受影响个人数据主体的权利和利益。

- 功能与内容

梳理评估项：

依据企业在海外各个法域数据合规相关的法律法规、指南及标准中针对App/个人数据的隐私合规要求，形成检查清单。完成App隐私合规评估清单梳理后，需要综合利用人工自查、静态分析和动态调试技术分析和检查，得出关于App隐私合规性的全面评估；

隐私政策人工检查：

隐私政策人工检查包括审查隐私政策文本，检查隐私政策是否符合适用的法律法规和隐私标准，是否清晰易懂，数据收集目的明确，隐私政策应明确用户的选择权，如何管理第三方共享和访问，采取的安全性措施，隐私政策变更通知等内容；

静态分析：

APK静态分析旨在仔细研究应用程序的安装包（APK文件）以识别潜在的隐私和安全风险，确保应用程序在设计和开发阶段就具备隐私合规性。包括权限分析、代码审查、数据流分析、第三方库检测，数据安全保护等；

App动态调试：

App动态调试通过模拟用户交互使用应用程序的场景，跟踪数据和权限验证等，来检查其合规行为，以确保其符合隐私和安全标准。

- 落地工具

腾讯云提供的App合规评估服务，能够帮助企业开发团队实现与应用、产品的默认隐私合规设计开发。腾讯云应用合规平台（Application Compliance Platform）是一款提供小程序、移动 App 应用隐私合规检测的产品，基于相关法律法规、国家标准、行业标准等，对小程序、移动 App 应用进行静态、动态的技术检测，结合腾讯灵犀隐私合规专家团队专业意见，帮助企业识别应用的数据隐私合规问题，助力企业安全合规。

它可以实现小程序和应用app的合规检测：





详细信息可以参考官网链接：https://cloud.tencent.com/product/acp

- **身份认证与访问控制（IAM）**

  - 痛点与问题

    敏感数据泄漏事件时有发生，其主要原因之一是因为用户身份验证和权限授权不当，例如：未启用MFA认证、第三方云平台DB中存在未授权的活动、访问权限设定不合理等。因此，对于数据处理者和数据接收方，用户身份认证和访问控制是数据安全的关键技术手段，也是在数据隐私合规管理中必要和有效的ToMs措施之一。

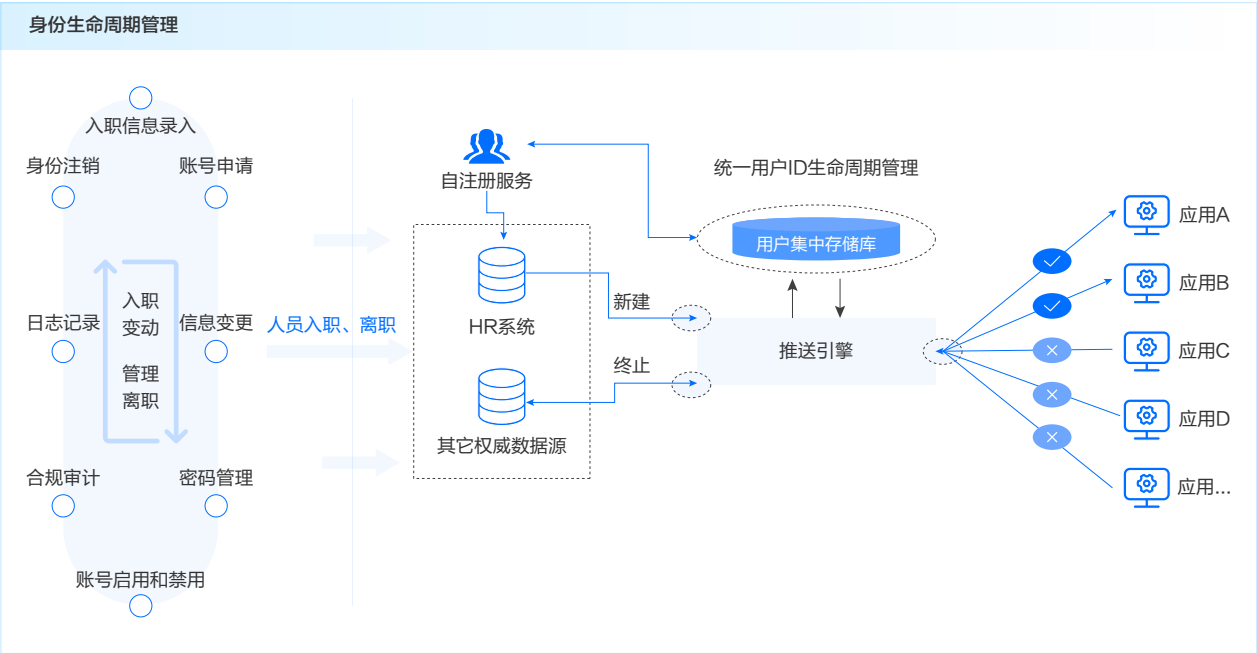
  - 目标与定位

    企业在海外运营业务时，涉及到海外用户、海外终端对本地系统以及中国总部、云上应用等混合访问模式，身份认证是数据安全的第一道防线，用以确保对服务和应用程序等被访问资源的安全性。

  - 功能与内容

    身份生命周期管理：

    对企业内部员工、第三方用户等不同类别用户提供用户身份与账号ID的映射，对账号ID的创建、供应、存储、集中管理、身份信息同步、统一密码策略等进行管理；



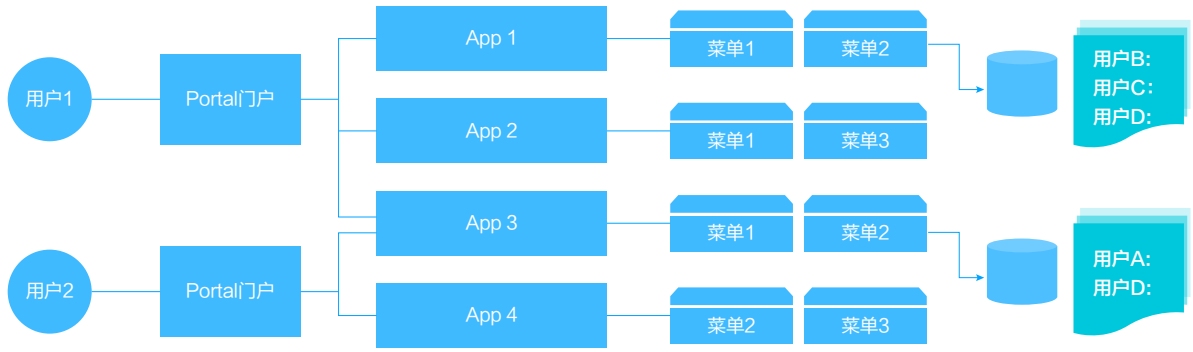
身份认证管理：

是对访问者的合法性验证，身份认证的方式可以有多种，如用户名/密码、邮箱/密码、手机号/密码、证书登录、生物特征识别、手机或APP辅助登录等方式，构建身份认证方式时，应结合业务应用的安全需求，综合考虑“所知、所有、所是”三方面用户属性，采用合理的、认证方式，确保访问者身份的真实性。同时，认证服务能够与AD、微信或海外本地的同类技术生态进行集成，支持扩展其他认证方式；

权限管理：

访问授权管理可以有不同等级，一种是粗颗粒度的系统级别授权，如常见的机遇Portal实现的应用列表。同时，系统基于RBAC模型，IM通过向各业务系统返回用户角色，角色与权限匹配，实现中粒度如菜单级别授权。另一种是更为精细的授权，通过梳理各业务系统建立统一的授权策略，并将权限粒度精确到对象，实现细粒度权限，例如针对数据划分用户权限是一种细颗粒度的划分方式，当不同用户进入同一页面/菜单时，所访问的数据是不同的。

权限管理



实时地根据来自不同本地或外部来源（如Web服务和数据库）的数据触发安全评估，以决定是否授权访问。这种基于环境的评估方法可以提供更为精细的访问控制。此外，授权策略可以与外部系统（例如风险控制、终端安全等）集成，以实现更全面的安全措施。

- 落地工具

关于身份认证与访问控制（IAM）的技术方案与工具实现，请参考5.3.2.2节“账号与身份管理最佳实践的内容。此外，腾讯云生态合作伙伴IBM Verify 通过提供身份架构的基础构建块来解决当前身份和访问管理 (IAM) 挑战，从而降低混合身份的复杂性。

- **数据脱敏与匿名化**

  - 痛点与问题

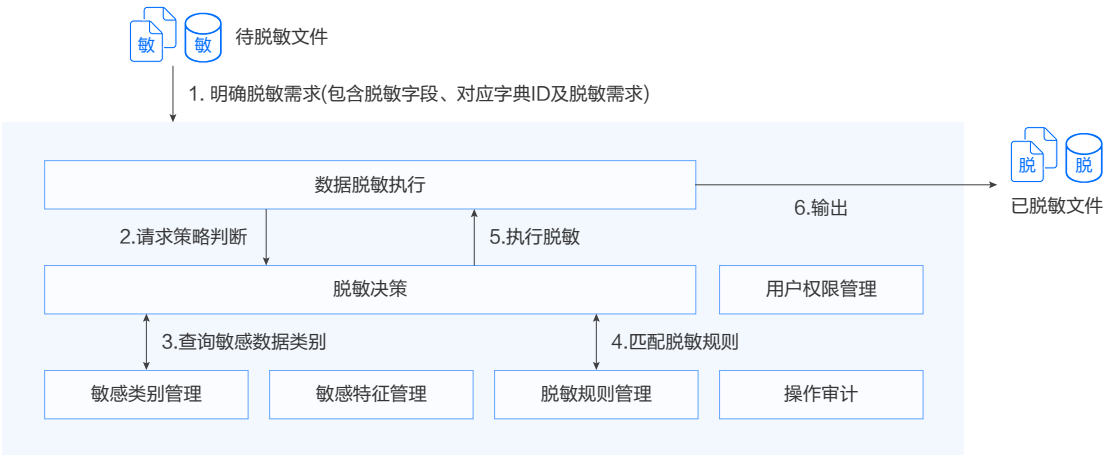
在企业数据出海过程中，不同国家和地区对匿名化数据的法律地位和监管要求存在差异，增加了企业在跨境数据传输中的合规难度。一些国家对数据出境设置了严格的限制和审查机制，对个人隐私数据的保护做了特别要求，如欧盟的《通用数据保护条例》(GDPR)等，要求企业在处理跨境数据时必须确保数据的隐私性和安全性。

  - 目标与定位

数据脱敏通过对敏感数据进行处理，使其无法直接识别特定个体，从而保护用户的个人隐私，并且可以显著降低数据在传输、存储和处理过程中被泄露或滥用的风险，满足数据出境合规要求。

  - 功能与内容

数据脱敏平台功能



数据脱敏平台应具备脱敏执行、脱敏决策、敏感类别管理、敏感特征管理、脱敏规则管理等功能，支持敏感数据自动发现与分类、利用认知分析和威胁检测分析、监控和审计所有数据活动。

- 落地工具

  腾讯云有多套方案可以提供数据脱敏能力。

  可以使用腾讯云数据脱敏解决方案，开箱即用，适合企业内部数据迁移与外部数据共享的场景。主要用于数据库中数据外发时的数据脱敏，详细信息可以参考5.3.1.4节“数据脱敏”的内容。

  此外腾讯云在大数据体系中也提供了数据脱敏的能力，详见5.3.6.4节的内容。

  最后，对于进出对象存储的数据和内容，可以通过腾讯云对象存储COS+云函数SCF的组合方案，实现数据的实时脱敏。此方案具有较大的灵活性和适用性，可以自定义脱敏规则。如下图所示，对于从摄像头上传到COS存储桶的数据，可以毫秒级触发云函数进行脱敏（如摄像头采集到的人脸数据，进行人脸的马赛克处理）之后再传入到数据库中。



- 数据水印

  - 痛点与问题

    数据跨境传输过程中，一旦发生数据泄露或非法使用，难以追溯数据来源和责任人。数据水印技术的实施涉及多个技术环节，包括水印的嵌入、隐藏、检测与提取等，且不同类型的数据（如文本、图像、视频等）对水印技术的要求各不相同，增加了技术实施的难度。此外，跨境环境中数据处理的多样性和复杂性也进一步加大了技术实施的挑战。

  - 目标与定位

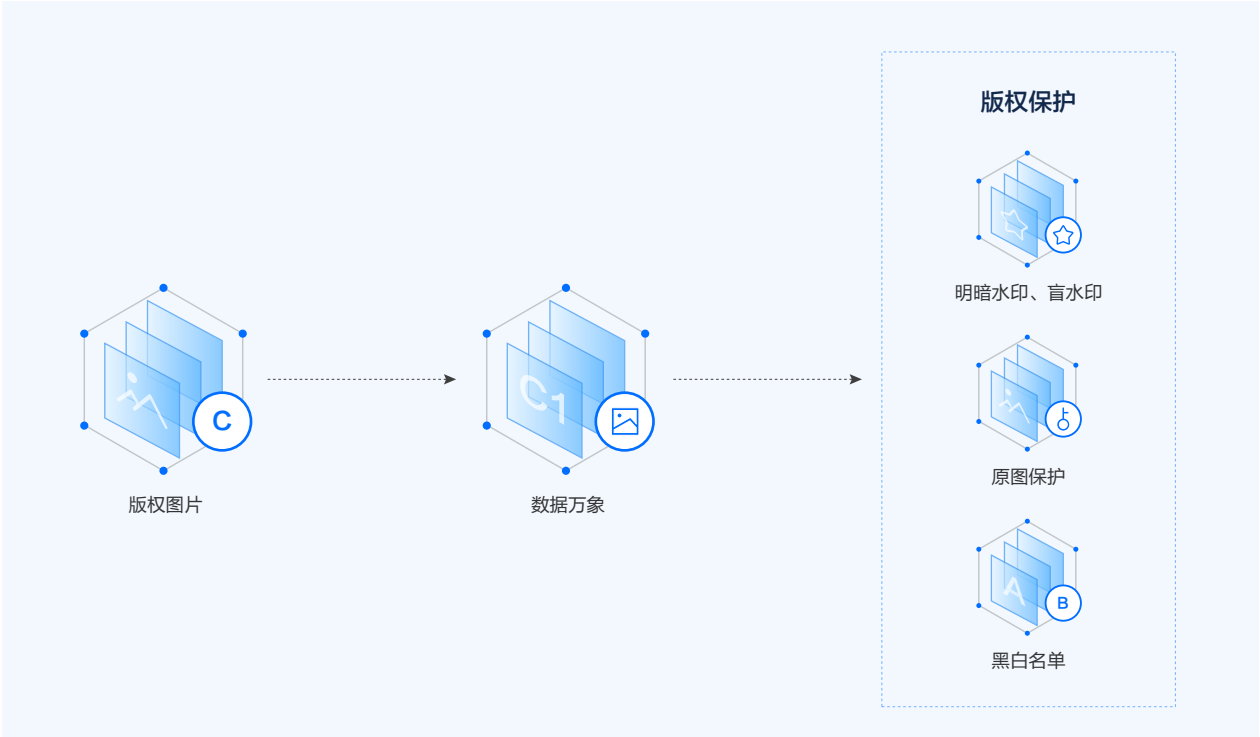
    数据水印技术使得数据在跨境传输和使用过程中能够被有效追踪和溯源。一旦数据泄露或非法使用，企业可以依据水印信息迅速定位数据的原始来源、传输路径和使用情况，从而采取必要的法律和技术手段来应对。另外，数据水印技术通过向数据中嵌入难以察觉但可验证的信息，增加了数据被篡改或伪造的难度，从而提升了数据的安全性。

- 功能与内容

数据水印平台应具备策略管理、显示水印、隐示水印、水印生成、水印记录、水印溯源等功能，通过对对需添加水印的任务文件进行标记和记录，确保数据在展示、外发等各环节中的安全可控与有效追踪。

- 落地工具

企业可以选择腾讯云多媒体处理（Multimedia Processing，MMP）产品来实现数字水印的功能。数据万象不仅支持对图片、视频、文档资源添加图片或文字水印，还针对图片提供了盲水印功能，将水印信息以不可见形式添加到图片频域，在资源泄漏后优先鉴权追责；对于资源的访问，您可以使用原图保护、签名下载、黑白名单控制等安全策略进行快速且全方位的控制。



详细信息可以参考腾讯云官网：https://cloud.tencent.com/product/ci

- **数据防泄漏**

  - 痛点与问题

    在数据跨境传输过程中，由于涉及多个环节和广泛路径，数据易成为被截获、篡改或不当利用的目标。特别是跨境流动的数据中常包含个人信息、商业秘密以及关键的知识产权等，这些信息一旦泄露，将威胁到企业的数据安全给企业带来损失。

  - 目标与定位

    数据防泄漏工具通过先进的技术手段，全面识别、监控并保护在跨境过程中传输的敏感数据，如个人信息、商业秘密及知识产权等，防止数据被未经授权的第三方截获、篡改或滥用。同时，数据防泄漏工具还助力企业遵循全球各地的数据保护法规，如欧盟的GDPR、美国的HIPAA等，通过提供合规审计与报告功能，确保数据传输的每个环节都符合法律法规要求，降低企业因违规操作而面临的法律风险和巨额罚款。

  - 功能与内容

    企业通常在邮件、Web、网络、存储、终端等位置部署数据防泄漏工具，监控外发文件或扫描本地文件，发现敏感数据进行阻断，实现数据防泄漏。数据防泄漏主要通过关键词、正则表达式等定义敏感内容模板，运用加密技术、权限控制、文档透明加密、数据安全隔离、内容智能识别、网络拦截等实现。

  - 落地工具

    腾讯云提供多种产品组合，实现上述数据防泄露的场景。

    首先在权限管理与安全监测上，腾讯云提供的零信任方案可以有效提高办公场景和生产场景数据方案的安全性，降低数据泄露的风险，详细信息可以参考5.3.2.5节“零信任方案”内容。

    其次，腾讯云的数据安全产品族数盾可以提供一套基于数据流的数据安全解决方案，帮助客户解决云上数据安全治理问题，满足等保合规要求的同时，也能提升数据隐私保护能力。详情可以参考官网链接：数据安全



最后在数据加密、密钥管理层面，腾讯云也提供了完整的工具矩阵，使数据即便泄露也能大大降低资损与违规风险。详细信息可参考5.3.1.1节“密钥管理”与5.3.1.2节“数据加密”相关内容。

- **密码服务**

  - 痛点与问题

    针对传输通道中流动的数据加密和数据库、服务器中静态存储的数据，企业往往采用独立且分散的加密机制，这些机制往往通过硬编码或独立的软件解决方案来实现，导致企业内部不同应用之间在密码管理、加密标准及应用集成上形成 “孤岛” 。这不仅增加了管理的复杂性，还可能因加密标准不一致导致安全风险，阻碍数据在不同系统间的共享。

  - 目标与定位

    建立企业级统一的加解密措施，提供统一的密码技术服务，满足应用建设、日常业务中对于密码运算、密钥协商、密钥存储的需求，对密码服务进行高效、安全的管理，确保服务效率与密码应用过程安全，同时满足合规要求。

  - 功能与内容

    密码服务平台提供全面的加密解决方案，涵盖对称及非对称加解密服务，确保数据传输与存储的安全性。该平台还集成了对称密钥管理服务，实现密钥的生成、存储、分发、更新与废止的全生命周期管理，保障密钥的安全性与可控性。此外，该平台还包括数字证书管理服务，数字证书的生成、申请、颁发、撤销及验证流程。

  - 落地工具

    腾讯云密钥管理服务（ Key Management Service，KMS ）能够帮助创建和管理密钥，保护密钥的安全。腾讯云 KMS 可以与大多数腾讯云上的云产品进行无缝集成，在已集成 KMS 的云产品中，仅需要选择一个从 KMS 托管的密钥，即可实现对其云产品内的数据进行加解密。详细信息可以参考5.3.1.1节内容。

- **隐私计算平台**

  隐私计算平台也叫可信计算平台，它通过先进的隐私计算技术，如安全多方计算、联邦学习等，构建一个安全、高效的数据合作环境，使得不同地域、不同机构的数据可以在不直接交换明文的情况下进行合作与共享，实现多源数据的跨域合作与共享。同时允许在保护数据隐私的同时，对数据进行深度分析和挖掘，从而发现数据中的潜在价值，为企业决策提供支持。

  腾讯云提供了可信计算环境与可信计算服务，详情请参考5.3.4节“可信计算”的内容。

- **数据安全事件监控**

  - 痛点与问题

    不同国家/地区都对公司如何响应数据泄露事件作出了规定，如在欧盟GDPR中规定发生事件的72小时内通知到个人或监管机构等。因此，为满足企业境内外合规要求，需要针对数据安全事件建立监控机制。

  - 目标与定位

    数据安全事件监控功能通常融合进SIEM/SOC类产品，帮助企业可视化呈现安全状况，结合威胁事件预警、追踪溯源和漏洞处理，进一步提升数据异常行为的监测和告警功能，对安全事件及时响应和处置。

  - 功能与内容

    采用一体化的SIEM/SOC平台，利用跨境数据处理活动流量和日志的自动化采集，结合传统的安全事件分析、威胁情报、漏洞管理以及响应阻断系统的能力，通过可视化图表模板，精确识别和响应数据安全事件，引导企业作出快速决策，满足企业出海面临的境内外监管要求。

  - 落地工具

    腾讯云的T-Sec安全运营中心以云原生技术为基础，仓湖一体化大数据平台为底座，结合腾讯领先的威胁情报能力、AI和可视化技术，聚焦TDIR（Threat Detection， Investigation and Response），打造智能化安全运营平台，提升安全运营效率，实现企业全网安全态势可知、可见、可控。

    此外，腾讯云的生态合作伙伴IBM　Qradar结合实时监测、事件响应与管理、高级威胁监测、业务威胁情报、用户监控等功能，为企业提供一体化部署服务或根据需求选择不同功能组件。

- **数据跨境流量分析**

  - 痛点与问题

    随着企业国际化业务的扩展，其面临着来自不同国家和地区对数据安全和个人隐私保护日益增长的监管挑战。境内外监管机构都需要了解跨境数据的处理活动、数据类型以及涉及的数据量，因此企业需要准确、及时地识别出跨境数据的流量和路径，以满足监管要求。

  - 目标与定位

    满足企业出海活动所涉及到的各类境内外监管要求，明确掌握业务数据、个人/敏感信息，重要行业的重要数据等的动态流向，以及从境内到境外的数据跨境传输路径、传输数据类型、数据量、传输方式等多个因素。

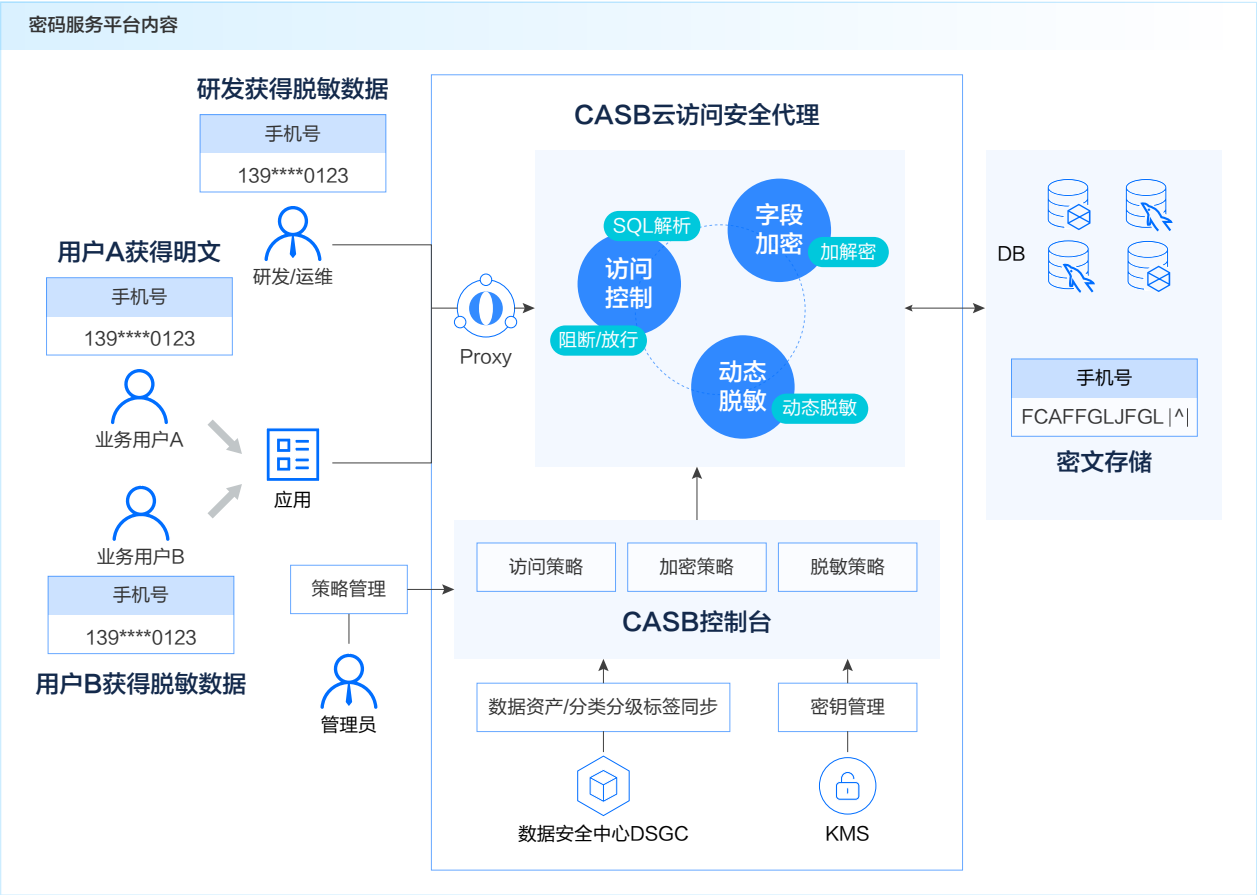
  - 功能与内容

    数据跨境流量分析平台的流量采集与还原功能可实时、定制化策略地捕获网络流量，对结构化、半结构化以及非结构化的数据进行多维度解析和还原。其跨境数据内容识别功能可利用深度分析技术，对各种文件类型和内容进行检测和分析，判断是否包含个人/敏感信息或重要数据。同时，还具备跨境敏感数据传输检测功能，平台内置个人/敏感信息标签，通过协议解析和应用识别，深度分析那些含有敏感标签的数据。除此之外，跨境数据检测功能则通过监测数据的源ip和目的ip，精准检测并分析境内到境外的数据传输活动、数据类型和规模，进行统计分析和可视化呈现。

  - 落地工具

    腾讯云有多种方案可以实现数据跨境的合规性分析与治理。

    首先可以直接使用腾讯云数据安全中心这款产品，在跨境访问的场景中应用云访问安全代理的能力，识别非法的跨境访问来做相应的权限管控，从而可以实现跨境场景的合规。



关于数据安全中心的能力可以参考官网链接：https://cloud.tencent.com/product/dsgc

此外，在大数据场景中，可以利用WeData实现敏感数据的识别、规则模板与脱敏的一体化功能。详情可参考5.3.6节“大数据与数据湖“的内容。在数据场景中，可以通过5.3.1.4节介绍的Dmask的能力来对跨境的数据进行识别与脱敏。

上述方案属于事前和事中的技术方案，同时腾讯云提供的审计能力，能够在事后对复杂的合规问题进行集中分析与溯源，便于客户跨境场景数据合规能力的迭代。详见5.3.3节“数据合规审计”的内容。

- **数据库审计**

  - 痛点与问题

    企业在数据库运行过程中，需要针对数据异常行为进行监测和分析，识别潜在风险、数据泄露和合规性问题，提高数据安全管理效率。同时，在企业出现数据安全事件时，需要借助平台或工具进行事件还原、取证、审计和追溯，确保事件定责、复盘和防止再次发生。

  - 目标与定位

    数据库审计系统通过自动化工具平台，全面解决企业合规性、监管和责任追溯问题。它支持等保标准，实时检测并智能发现潜在威胁，提升监管效能，并通过精确追踪简化责任追溯，确保数据库安全合规并提高内部控制能力。

  - 功能与内容

    数据库审计系统具备全面资产覆盖、全量数据审计、智能威胁识别、多种风险告警、定期统计报告等五大核心功能。支持云数据库、自建数据库等统一的资产审计管理，能够全面监控数据库所有SQL操作，便于操作行为详细溯源，为数据安全事件提供便利的追责依据，提供精准的威胁分析和告警，并通过短信、邮件等多种方式及时通知安全管理人员。系统还提供周期性统计报告，帮助管理员掌握全局安全信息，同时具备高性能网络和SQL语句分析引擎，确保海量数据的高效检索与分析。

  - 落地工具

    腾讯云的T-Sec数据安全审计DSAudit是一款基于人工智能的数据库安全审计系统，可挖掘数据库运行过程中各类潜在风险和隐患，为数据库安全运行保驾护航，是企业的等保合规利器。此外，腾讯云的生态合作伙伴IBM Guardium具备一套完善的数据安全防护的解决方案系统，拥有包括：数据库、文件系统和大数据平台的审计、监控、保护和分析的能力，且IBM Guardium自身具有对数据安全威胁分析的能力，内建机器学习引擎，能够将宝贵的数据访问活动分解成可处理、可理解的元素，并有效保存，随后可以将其导出至企业大数据平台，无论是进行独立分析还是与其它信息融合进行关联性分析，对于企业来讲都将会带来非常大的价值。

- **操作审计**

  - 痛点与问题

    作为数据处理者或数据接收方，数据处理环境安全是基本要求，是对高风险的用户行为和重要的安全事件进行审计，保存审计日志等。从企业内部使用的视角，用户在云平台和系统上的操作行为不透明、不可追踪，易造成企业内部的违规操作、数据非法访问或攻击等安全事件。同时，缺乏对设施资源的实时监控，难以发现异常操作并防止潜在的安全威胁。事后无法追溯操作用户的身份和细节，责任难以界定。

  - 目标与定位

    操作审计系统可以追踪并记录云平台及各类系统的操作日志，满足企业内外部的审计需求，帮助企业检测来自内部的违规操作、鉴别正在发生的数据非法访问、通过异常行为分析发现非法攻击，且系统提供快速溯源能力，通过深度日志检索迅速定位数据泄露源头和操作用户，同时采用多级缓存和自动限流等机制保障在高流量攻击下审计数据的完整性和设备的稳定性。同时能够覆盖日常查询和监控运维人员操作的需求。

  - 功能与内容

    借助操作审计系统，可以自动捕获和记录账号中所有已执行的操作，包括管理活动和数据访问事件。操作日志将安全存储，支持长期保留策略，以满足不同的合规审计要求。同时系统详细记录各用户每一次的操作细节，包括具体的操作类型、操作对象以及操作的结果。此外，操作审计系统详细记录了所有API调用，包括发起方调用源ip、调用参数、返回结果、时间戳等。同时，通过记录资源的创建、修改和删除操作，帮助企业监控资源的使用情况和生命周期。当资源出现异常变更，操作审计记录可以帮助用户快速定位问题，操作审计会对用户操作行为进行详细的记录，通过操作记录可以判断账号是否存在安全问题。同时，可以创建多个跟踪分别追踪不同时间类型、区域范围，以满足境内外各类合规要求。

  - 落地工具

    对于云上账号较少，组织规模不大的企业，可以直接使用腾讯云提供的云上账号的操作审计能力，详情请参考5.3.3.2节“操作审计”的内容。

    对于账号较多，组织角色较复杂的企业，可以使用腾讯云的运维安全中心（堡垒机）。它是一套综合完善的事前预防、事中监控、事后审计的安全管理体系，集用户、授权、认证及综合审计功能于一体，支持多云、线下资产的统一管理以及各种主流操作系统和数据库。其中的安全事故追溯和高危命令阻断的功能模块可有效解决数据库审计的痛点与问题。

- **数据主体权利响应管理**

  - 痛点与问题

    企业在海外的运营越来越依赖处理个人数据来创造价值，同时个人数据主体也越来越意识到自己的权利保障，各个国家不断发布的新法规都给数据主体的定义带来了新的复杂性，增加了隐私权实现过程的复杂性，响应数据主体的请求是一个耗时的过程，大量工作是手动完成，这使得企业出海在遵守海外监管要求成为一项挑战。

  - 目标与定位

    数据主体权利响应在使企业能够自动化响应数据主体请求流程，包括接收、身份验证、数据发现、删除、数据编辑和安全响应。综合起来，企业可以确保履行准确性，缩短响应时间，并在请求量增加时能够按需扩展其响应能力。

  - 功能与内容

    数据主体请求门户：

    支持数据主体在线发起访问、更正、删除、撤回授权同意、注销账户等请求；

    请求管理：

    集中管理数据主体的请求，支持管理者下发请求响应任务，跟踪请求处理进度，查看请求处理结果；

    请求自动化响应：

    实现数据主体请求的自动化响应，通过脚本自动完成获取数据副本、删除个人信息、撤销授权等重复性工作；

    请求处置：

    分解请求响应任务，提供标准化的请求处置流程，支持多人协作完成响应任务。

    自动化数据主体行权管理能够为DPO，数据合规团队，风险团队，个人数据主体包括员工等提供行权渠道，自动执行GDPR、LGPD、CPRA 等各个法域的细微差别的时间表和要求。

  - 落地工具

    企业可以选择腾讯云的SoC安全运营产品来作技术实现。SoC安全运营中心可以实现安全日志管理 /复杂事件管理 /资产信息管理 /用户实体行为分析/安全事件处置流程。构建一体化安全运营体，实现安全运营“大闭环”，全面感知网络安全事件，统一分析。

    此外SoC具备云原生的高性能、低成本、纯自研的安全大数据分析平台，为企业提供一体化的泛安全数据接入、加工、存储、分析、告警、可视化等服务，具备“插件化”应用开发能力，助力企业构建云原生湖仓一体安全分析平台。

    详细信息可以参考官网链接：https://cloud.tencent.com/product/soc-private

    此外，由于海外部分国家的复杂场景，企业也可以选择腾讯云海外生态合作伙伴的隐私合规管理服务组件实现与应用、产品的默认隐私合规设计开发。

- **数据安全事件处置**

  - 痛点与问题

    各司法管辖区关于数据安全事件报告义务存在差异，除此之外企业在事件处置中应遵循相关原则，包括损害预防、收集限制、可问责性质以及监督和执行。因此，全球性企业需具备发现事件、按时响应以及正确处置事件的能力，才能有效应对数据安全事件。

  - 目标与定位

    及时处置数据安全事件，可以帮助企业遵守法律法规，以避免法律责任和经济损失。同时，通过及时控制和处置数据安全事件，企业可以防止损害的进一步扩散，减少潜在的财务和运营损失。

  - 功能与内容

    智能化自动化：

    在检测到威胁时管理整个安全事件生命周期，并在企业响应工作与预定义用例一致时自动执行流程。

    隐私合规：

    可以根据企业所在区域的不同，配置相应的合规模板，一旦发生隐私事件，工具能够指导相关人员开启隐私事件流程，包括通知相关机构、客户等。

    可视化监控：

    通过仪表板将关键事件和环境数据转化为直观图形，便于相关人员迅速把握情况并作出决策。

  - 落地工具

    腾讯云可以依靠SoC安全运营中心来提供数据安全事件的处置功能。前面章节已有关于腾讯云SoC安全运营中心的介绍，此处不再赘述。详细信息可以参考官网链接：https://cloud.tencent.com/product/soc-private

    此外，腾讯云生态合作伙伴IBM QRadar SOAR解决方案具备丰富场景化能力与行业经验，能有效优化安全团队的事件处置决策流程，提高安全运营效率，并确保通过智能自动化和编排解决方案来满足事件响应流程的要求。该工具通过动态行动手册、可定制的自动化工作流以及推荐响应来缩短响应时间。同时，可为关键操作添加时间戳，并辅助威胁情报和响应，简化事件响应流程。

- **数据安全事件溯源**

  - 痛点与问题

    在全球化背景下，数据安全事件可能涉及跨国问题，需要不同国家和地区之间进行合作和信息共享，在一定程度上增加了溯源的难度。此外，企业应当在数据安全事件发生时及时保存电子证据，并建立监管链条，以支持事件的调查和处理，并降低监管处罚风险。

  - 目标与定位

    数据安全事件溯源的目的是彻底理解事件的起因和影响，进而采取有效措施防止同类事件再次发生，以减少潜在的业务损失和法律风险。通过有效溯源，企业能够识别安全漏洞和弱点，加强安全控制，提高对威胁的响应速度和处理能力。此外，溯源还有助于确定责任归属，为法律诉讼和追责提供支持。

  - 功能与内容

    深入的取证调查：

    可以追溯潜在攻击者的逐步行动，对疑似恶意数据安全事件进行深入调查。

    数据恢复：

    允许企业索引和搜索捕获的网络数据包（PCAPs），并具有将这些数据恢复成原始形式的功能，包括电子邮件、文件、图片附件、VoIP电话和网站等。

    数字印象：

    通过分析交互的标记标识符来生成数字印象报告，帮助调查人员识别攻击者或网络实体。

    数据恢复：

    可以从一个或多个 IP 地址或端口检索原始数据包捕获数据，并将其恢复到取证库中。

    案件和集合管理：

    使用案件和集合来逻辑地组织和管理导入的文档和数据包捕获文件，便于调查人员进行案件特定数据的管理。

- 落地工具

  腾讯云在数据安全问题溯源方面主要依靠各类审计工具来实现。具体可以参考5.3.3.5节“数据合规审计”的内容。溯源能力的实现能够有效降低数据安全事件发生后的风险，并帮助企业快速定位问题根源。同时也能给监管机构提供电子证据链，帮助企业降低受到处罚的风险。

  通过腾讯云生态合作伙伴IBM QRadar Incident Forensics（事件取证）可以追溯潜在攻击者的分步行动，并对可疑的恶意数据安全事件进行取证调查，以了解网络安全事件的全貌。同时，工具支持允许用户从取证库中提取与特定线索或假设相关的文档，并通过搜索和过滤功能快速缩小与案件相关的文档范围。QRadar事件取证可减少安全团队调查犯罪记录所需的时间，还可以帮助企业修复网络安全漏洞，并防止其再次发生。

- **数据留存**

  - 痛点与问题

    数据留存是数据合规管理中的重要环节，它涉及到数据的安全性、合规性以及有效管理。各国法律对不同类型的数据保留期限都有明确规定，以确保数据在合法和必要的时间内被保留。例如，中国PIPL、 GDPR等多项法律规定个人数据的存储期限不得超过实现处理目的所必需的时间。由于企业在运营中涉及的数据种类繁多，因此，企业应当梳理各类数据资产，综合考虑法律法规、行业监管要求、合同要求以及公司业务需求等多项因素，确认各类数据的留存期限，形成清单，进行有效管控。

  - 目标与定位

    管理数据留存期限是确保企业在数据保护和隐私方面满足法律法规要求的关键措施，同时也是合理管理存储资源，降低成本，优化数据存储效率的手段，通过减少不必要的数据留存来降低数据泄露风险，从而提高数据合规管理水平和运营效率。

  - 功能与内容

    数据留存工具可以用于结合数据分类分级的结果，追踪和记录企业所持有的数据类别、位置和使用情况，以便更好地遵守数据留存期限，主要的系统功能包含：

    数据分类与标识：

    工具能够依据数据种类及其敏感性对数据进行有效分类和标识，进而实施相应的保留策略和安全防护措施。

    自动化备份与数据还原：

    提供自动化备份解决方案，定期对数据进行备份，并定期检测数据恢复流程，确保在数据发生丢失或损坏情形下能够迅速进行数据还原。

    保留期限管控：

    允许用户设定数据的保留期限，并依据设定期限自动审查及更新数据保留政策，以符合相关法规与组织策略。

    数据整理与优化：

    支持对存储数据进行定期整理与优化处理，剔除无价值或已过时的数据，从而提高存储效率，节约存储资源。

  - 落地工具

    通过数据留存与删除系统，能够帮助企业实现数据留存期限管理自动化，实现数据留存策略与企业现有系统的无缝整合。例如，在邮箱管理中，若为特定父文件夹配置了为期一年的数据保留策略，那么该文件夹内所有邮件及子文件夹将得到为期一年的自动保护。期满后，系统将自动清除这些数据。

    腾讯云在数据库、对象存储与大数据产品中均提供了数据留存相关的系统化能力。详细信息可参考5.3.5节和5.3.6节的内容，以及对象存储COS的官网链接：https://cloud.tencent.com/product/cos

- **数据删除**

  - 痛点与问题

    根据各国法律规定，企业在数据超出使用期限或数据主体提出删除请求时，有责任对相关数据进行删除，以维护个人隐私和防止敏感信息泄露。然而，常规的文件删除或硬盘格式化操作仅是将数据标记为可覆盖空间，并非真正彻底清除。若不采取彻底的数据擦除措施，通过数据恢复工具仍有可能恢复这些信息。

  - 目标与定位

    数据删除的主要目的是确保数据的彻底和安全删除，遵守法律法规、防止数据泄露以及维护数据主体权利，从而保障数据安全合规。

- 功能与内容

  通过数据删除工具可以实现彻底删除现有文件、擦除整个分区或硬盘、擦除已删除文件　、进行自动化擦除任务、对数据擦除的验证等。

- 落地工具

  云上数据删除或擦除通常由云平台提供的API或工具来远程执行，可能涉及虚拟机的快照删除、云存储中的数据清除等。云服务供应商通常难以实现对客户数据的物理删除，企业在私有化部署的环境中可以使用专业的数据擦除软件对PC　笔记本、一体机等本地系统或移动存储介质进行数据擦除。

  腾讯云控制台提供了内置的数据擦除工具，用户可以在服务器列表页面选择需要清除数据的服务器，并按照提示进行操作，以确保数据无法恢复。

  腾讯云在数据库、对象存储与大数据产品中均提供了数据删除（即数据生命周期设置）相关的系统化能力。详细信息可参考5.3.5节和5.3.6节的内容，以及对象存储COS的官网链接：https://cloud.tencent.com/product/cos

- **数据备份容灾**

在数据跨境合规中，通过建立数据备份与恢复机制、构建应急响应与灾难恢复能力、设计高可用架构等，企业可以确保在跨境数据传输和存储过程中的数据安全和业务连续性，有效应对潜在的法律风险、技术故障和自然灾害等威胁。腾讯云提供基于存储桶复制的容灾备份方案、云上数据备份方案和本地数据备份等多种解决方案，帮助企业实现备份容灾。

- **数据合规管理系统**

数据合规管理目前已成为企业业务部门、安全部门、法务合规部门、IT等部门需要处理的常态化工作，包括监管政策的跟踪解读、下发执行与反馈，数据处理活动审批与记录，各类高风险数据处理场景的影响评估与审批，对数据安全事件的演练与响应，以及日常数据风险监测，数据合规认证与备案等，这些零散事务在企业中往往处于无序、人工处理、被动应对的状态，呈现出工作效率低下、统计数据不准确、职责难以界定的情况。

在建设数据安全合规技术体系的过程中，企业需要构建一系列安全组件和服务，旨在通过自动化、智能化方式解决上述问题，作为各部门开展数据合规管理工作和跨部门协作的工作台，完成数据合规需求基线定制、数据合规评估、数据处理活动审批、数据主体权利响应管理以及数据合规风险监测等日常合规管理任务。

系统用户主要有业务部门的数据处理人员、GRC部门以及信息安全部门人员、涉及数据合规的项目经理，以及DPO等人员。系统主要功能模块包括数据合规基线管理，数据处理活动管理，数据合规评估，数据主体权利响应管理以及数据合规风险监测等。

数据合规基线管理：
致力于数据合规基线的精细化构建，通过紧密追踪并整合最新的监管政策与法规解读，将这些复杂信息转化为用户易于理解的基线控制清单，确保每位用户都能迅速把握政策动态，并据此采取及时有效的合规措施。

数据处理活动管理：
对数据处理活动进行记录，记录内容包括控制者或处理者信息、数据保护官 （DPO） 和数据保护代表的姓名和联系方式，处理目的，个人数据分类说明，数据主体类别（适用于控制者）或处理类别（适用于处理者）等，为数据流转的每一步提供清晰可查的依据。

数据合规评估：
针对数据跨境流动及本地合规需求，引入自动化与流程化工具，高效执行隐私影响评估、传输影响评估等关键步骤，确保合规评估工作既全面、高效。

数据主体权利管理：
为个人信息主体打造便捷、透明的权利行使渠道，支持一键更新授权状态，让数据主体随时掌握并管理自己的个人信息，增强用户信任与满意度。

数据合规风险监测：
构建先进的合规风险监测体系，专注于跨境及边界数据流动的实时监控，结合智能告警、深入统计分析与直观可视化展示，为管理层提供即时、全面的风险洞察，助力企业精准应对合规挑战。

腾讯云生态合作伙伴 IBM Openpages是一套综合GRC平台，包括风险管理，合规管理，安全风险管理、供应商安全管理、业务连续性管理、财务风险管理和IT审计管理等模块，可以为企业提供全面的自动化、智能化数据合规管理能力。

4.2.5 数据合规运营体系

数据安全合规风险评估

数据安全合规的目标之一是降低安全合规风险，因此建立有效的风险防范手段，对于预防数据安全事件发生有重要作用。

- **周期性风险评估**

  在实践中，大多数企业至少每年至少执行一次全公司范围的数据安全风险评估，全面了解公司风险分布情况、风险等级。同时，建议企业根据自身的行业、业务活动，梳理高风险数据处理活动列表，在开展高风险数据处理活动前，由相关部门组织开展专项数据安全风险评估，高风险数据处理活动包括但不限于：承载重要数据处理活动的信息系统发生架构调整（如：从单体架构调整为分布式架构）、下线等重大变更、基于不同业务目的的数据汇聚融合、利用生物特征进行个人身份认证等。

- **日常运营风险评估**

  在数据合规领域，有三种典型的风险评估类型贯穿于数据合规管理工作中：隐私影响评估（PIA）、数据保护影响评估（DPIA）、数据传输影响评估（TIA）。尽管在日常使用中，这些术语有时可能会被指代相似的概念，但它们各自具有独特的含义和应用场景。

  - 隐私影响评估（PIA）

    PIA 主要用于分析与项目、产品或服务相关的个人信息处理的隐私风险。PIA 有助于推进隐私保护设计 (PbD)，PbD 是一种将隐私保护作为设计阶段核心要素的理念，它强调在技术开发、系统构建和实践应用的早期阶段就将隐私保护纳入考虑。这种方法确保了隐私保护不是事后的补救措施，而是从项目启动之初就融入其中。

    在实践中，PIA 建议尽早完成，才能起到应有的效果，执行PIA时机包括：

    - 在涉及个人信息收集的项目、产品或服务的构思阶段或范围界定期间；
    - 出现新的或修订过的法律法规、行业标准、公司政策时；
    - 企业因改变个人信息处理方式而产生新的隐私风险时。

    PIA的具体内容、使用方式以及评估格式、方法和流程，因行业、所处国家或地区要求以及数据敏感度或类型的不同而有所差异。数据合规管理人员应根据此类因素确定合适的方法和方式，并针对企业的具体需求定制模型。

    在实践管理中，一个核心挑战是确定哪些项目、产品或服务应优先进行PIA。为了识别那些存在较高隐私风险的数据处理活动，部分企业选择采取一种分阶段的方法：首先进行初步的快速隐私评估，评估方式可以为简短的调查问卷，再确定该项目、产品或服务是否需要进一步开展全面且深入的PIA。通过这种方法，能够让企业将资源集中投入到那些对个人隐私构成最大威胁和潜在损害的领域，从而创造更好的结果，并对个人形成更有效的保护。

  - 数据保护影响评估（DPIA）

    进行DPIA评估目的都是为了用于确认因个人数据处理而导致的风险，以及尽早且尽可能多地减少此类风险。根据GDPR的规定，DPIA适用于可能使个人面临高风险的处理。若在处理中未执行DPIA，以不正确的方式执行DPIA，或未按要求咨询主管监管机构，可能导致最高1,000万欧元的行政罚款，若为企业，罚款金额最高为上一财政年度全球年收入总额的2%，具体以金额较高者为准。若企业受GDPR约束，则需要执行DPIA，尽管“PIA”一词在其他情况下经常用于指代相同的概念，但GDPR下的DPIA有着特定的触发条件和要求。

    如GPPR第35(3) 条所示，可知道什么情况下的处理操作属于“可能导致高风险”，继而针对此种情况执行DPIA：

    - 以自动处理（包括用户画像）为基础，对与自然人有关的个人方面执行系统和广泛的评估，并在此基础上作出对自然人产生法律效力或产生类似重大影响的决定；
    - 大规模处理“特殊”类别的数据或与刑事定罪和违法行为相关的个人数据；或对可公开访问区域执行大规模的系统性持续监测。

    但上述清单并非全面，第29条工作组（WP29）文件中提供了更具体的场景示例，在下图场景中需执行DPIA，如果数据处理活动满足上述触发条件的1-2项，数据控制者应考虑执行DPIA。

执行DPIA的场景示例

- **评估或评分行为**，例如用于预测目的（包括工作表现、经济状况、健康、个人爱好或兴趣、位置活动等），以便创建或使用个人资料的
- 基于**自动化决策评估**产生法律效力或类似重大影响
- **系统性监控**，用于观察、监测或控制数据主体的处理，其中包括通过网络收集的数据或对可公开访问区域的系统性持续监测
- 涉及**特殊种类**个人数据以及有关刑事定罪和犯罪的个人数据处理，如可能导致歧视、身份盗用或欺诈、经济损失、名誉损害、受专业秘密保护的个人数据
- **对个人数据进行大规模处理**，涉及大量个人数据并影响大量数据主体的情况
- **匹配或整合数据集**，例如，该处理源自以某种方式出于不同目的和/或由不同数据控制者执行的一项或多项数据处理操作，其中所采用的方式可能超出数据主体的合理预期
- 涉及**易受伤害的自然人数据**的处理，尤其关注儿童的个人数据
- **使用创新技术或采用新技术性或组织性措施**，例如，通过指纹和面部识别功能的联合使用，完善物理门禁控制
- 处理会**阻止数据主体行使权利**或者使用服务或合同

同时，GDPR 第 35(7) 条规定了要DPIA评估的最低要素主要内容包含：

– 对设想的处理操作和处理目的的系统描述，包括在适用情况下控制者追求的合法利益；

– 评估与目的相关的处理操作的必要性和相称性；

– 评估处理操作中的数据主体的权利和自由的风险；

– 为应对风险而设想的措施，包括保障措施、安全措施和机制，以确保保护个人数据并证明遵守本条例，同时考虑到数据主体和其他相关人员的权利和合法利益。

○ 数据传输影响评估（TIA）

TIA是由数据控制者或处理者对传输个人数据至第三国所产生的安全和隐私风险进行的分析。TIA能够帮助企业识别数据转移活动中的潜在风险，分析该数据转移是否合法，并确保数据转移按照企业预期的形式进行。GDPR对将个人数据传输到欧洲经济区之外的数据转移施加了严格的规定。根据GDPR的规定，依赖GDPR第46所列出的传输工具进行个人数据传输的企业，有义务评估数据转移目的地的保护水平以及是否需要采取额外的保护措施。是否需要进行TIA以及TIA的执行步骤如图xx所示。

TIA执行步骤



TIA包含的内容有：

- 数据转移的细节和具体情况；
- 合同保障措施在数据转移目的地（即第三国）的可执行性；
- 数据转移目的地国家或地区的数据保护法律框架；
- 第三国当局是否可以在数据传输方不知情的情况下通过法律、惯例或其他方式访问被转移的数据；
- 第三国当局是否可以借助其可支配的立法、法律权力、技术、财务和人力资源以及报告的先例，通过数据输入者或电信提供商或通信渠道访问数据；
- 为保护传输数据所采取的补充措施。

第三方数据安全合规管理

此章节第三方主要指与主要交易或活动双方无直接关联，但提供支持、服务或介入的独立实体。第三方在交易中保持中立地位，旨在提供客观、公正的服务或解决方案，第三方可以是个人或企业。对于第三方数据安全合规管理主要包含：合作前管理、合作中管理以及合作结束管理。

合作前管理

评估第三方资质与能力

根据各国数据保护法律规定，企业应该对第三方代表其从事的数据处理活动负责。通常情况下，公司的采购部门需要建立一套具体的选择标准和流程。应该根据此类标准，通过问卷调查、PIA 或其他审核清单的形式评估潜在第三方。第三方选择标准可能包括：声誉、财务状况和保险、信息安全控制措施、传输点、事件响应计划、审计权、政策和程序、DPO设置情况等。

签订第三方合同/协议

与第三方签署合同/协议旨在确保第三方都能遵守公司数据合规的要求。在实务中，应当明确数据保护和法规要求，并将这些要求具体化到服务水平协议（SLA）中。这样做可以确保在数据安全合规职责、数据泄露应对、事件处理、与泄露相关的媒体报道、潜在的罚款风险以及其他相关事项上，促使第三方与公司管理保持一致。合同/协议中的内容建议包括：

- 关于第三方有权在远程地点访问的个人信息类型的详情；
- 第三方的数据保护策略；
- 数据使用限制，确保仅将数据用于特定目的；
- 合同终止后的数据处理；
- 审计和调查权；
- 第三方在发生数据泄露的情况下的职责；
- 数据泄露责任。

合作中管理

企业应建立第三方管理清单，记录内容包括但不限于第三方名称、可以访问的数据类别、双方签署的协议或其他具有法律约束力的文件类别、数据处理状态、合同有效期等内容，并对清单进行长期维护。

在合同有效期内，应按照合同及相关协议所协定的内容对第三方所提供的产品或服务进行监督、检查及管理。应特别注意，在合作过程中，如存在接收第三方数据的情形，应对第三方的数据来源进行必要的审核，防止来源不合法而导致法律风险。

合作结束管理

执行数据删除：合作结束后，存储在第三方的数据应当及时删除。特别是当处理敏感数据时，应在合同到期时发布服务下线和数据清理的通知。第三方需提供并盖章的数据清理证明，以确保所有数据得到妥善处理。

清除外包人员账号及权限：对于合作期间涉及的外包人员账号和权限，建议首先停用这些账号，并至少保留该账号半年的操作记录，以备后续审计或调查需要。后期应彻底删除这些账号，以确保不会有未授权的访问或数据泄露的风险。

数据主体权利响应

数据主体权利响应类别

数据主体权利是指数据主体对自己的个人数据所享有的一系列权利，包括访问权、更正权、删除权、数据携带权等，这些权利的设立旨在要求公司加强对个人数据的保护，提高数据处理的透明度，同时也是企业合法、负责任地处理数据的基础。部分核心的数据主体权利类别及定义如下表所示。

数据主体权利类别及定义

权利类别	定义
知情权	数据控制者在收集隐私数据时，应当告知数据主体数据控制者的身份信息与联系方式、处理隐私数据的目的与法律依据、被处理的隐私数据的类型、隐私数据储存的期限以及隐私数据转移情况等
访问/查阅权	数据主体有权访问已被数据控制者收集的隐私数据，以便了解和验证有关数据处理行为的合法性。数据控制者应当在合理的时间内满足数据主体的这种访问请求。在可能的情况下，数据控制者应当向数据主体提供远程访问其隐私数据的便利
变更/纠正权	数据主体有权要求数据控制者变更其隐私数据，也有权要求完善不完整的隐私数据，或纠正不准确的隐私数据
可携带权	数据主体有权要求数据控制者提供其隐私数据集，这种数据文件应该是结构化、通用的、机器可读以及不同操作系统中都可以执行的格式，并且数据主体有权将这些隐私数据传输给另一个数据控制者
自动化决策权	数据主体有权拒绝接受以自动化决策或者“用户画像”的方式处理其隐私数据。自动化决策，是指通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，并进行决策的活动
限制处理权	数据主体在对数据处理有异议或在特定情况下需要保护其隐私数据时，有权要求数据控制者限制对隐私数据的处理
删除/被遗忘权	数据主体有权在对实现处理目的所不再必需、撤回同意、发现隐私数据被非法处理等特定情形下，要求数据控制者及时删除与其有关的隐私数据
拒绝权	数据主体有权在任何时候基于其特定的情况，对基于合法利益进行的隐私数据处理提出反对。如果数据主体行使拒绝权，除非数据控制者能够证明有超过数据主体利益、权利和自由的合法理由，或者数据处理是为了提起、行使或辩护法律主张所必需，否则数据控制者必须停止处理隐私数据
撤销同意权	数据主体有权随时撤回其授权同意，数据控制者不得对此设置障碍。撤回同意不得影响撤回之前基于授权同意进行的合法的数据处理活动
投诉权	数据主体在认为其隐私数据被违法处理时，或认为其数据权利被侵犯时，有权向数据保护机构提出投诉

数据主体权利响应实施路径

- 准备阶段

  公司应当建立数据主体权利响应程序文档、制定响应流程、编制数据主体权利请求表、数据删除确认表、数据更正确认表、流程审批表等模板，为后续实施阶段做好准备。

- 实施阶段

  公司相关部门在收到数据主体行使权利的请求时，必须在规定的时间内（不同国家/地区响应期限不同）响应并采取相应的措施。响应过程通常在数据处理系统内进行，包括查找、标记、提取、修改或删除数据的操作，并与数据主体进行沟通。当短期内无法通过系统实现数据主体权利响应时，也可以通过人工的方式处理数据主体的请求。通过上述措施，企业不仅能够遵守数据保护法规，还能够建立和维护客户对其数据处理活动的信任。

数据泄漏事件管理

在全球范围内，不同司法管辖区的法律（如：美国、欧盟、中国等）通常要求公司在数据泄露发生时必须向受影响的个人和/或监管机构发出通知。通知的时机、方式以及内容均依据各司法管辖区的具体法律而定。公司若未能及时并正确地发出通知，可能面临诉讼、名誉责任和潜在的监管审查。

除了法律风险和责任外，企业面临的另一个重大风险是数据事件的潜在成本。根据 IBM 的《2024年数据泄露成本报告》，数据泄露给全球组织带来的平均成本在2024年达到了488万美元，相较于去年增长了10%，这是自疫情以来最大的年度涨幅，70%的受访企业表示，数据泄露造成了重大或非常重大的干扰。因此建立综合的预防措施、检测机制和响应计划至关重要，企业能够提高对数据泄露的韧性，同时满足监管要求和合规标准。

事件响应规划中的职能角色

对于全球性企业，数据泄露的应对策略至关重要，特别需要关注具有最严格且财务影响最大的泄露通知要求的国家，如美国。在数据泄露事件发生时，企业需要迅速识别并履行各种角色和职责，以确保合规性和减少损失。

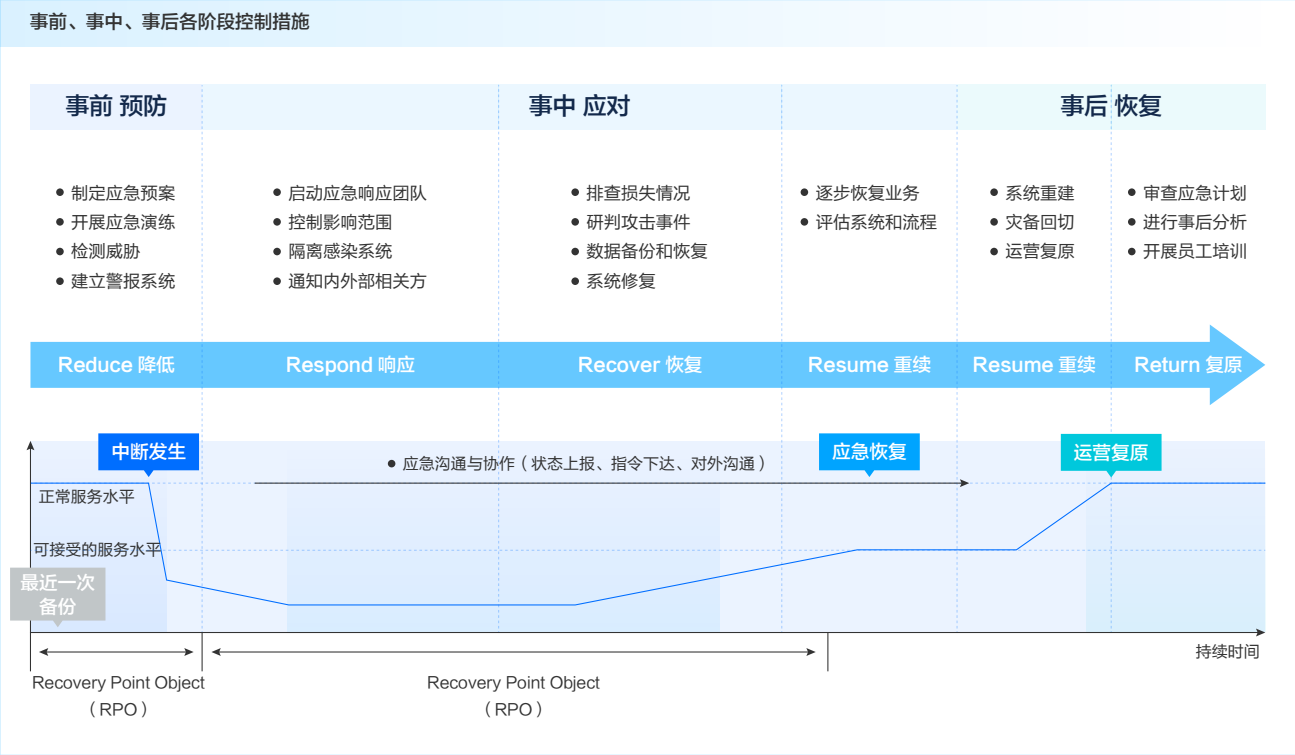
数据泄漏事件中各部门/角色职责的示例如下表所示，但企业应根据自身的业务模式和需求，考虑如何将职责进行调整和定制，以符合企业的具体环境和目标。

数据泄漏事件中部门/角色职责

职能部门/角色	职责
信息安全	就公司如何检测、隔离、删除和保留受影响的系统提供指导
法务	在考虑和设计程序时着眼于限制法律责任，并就数据泄漏事件是否符合通知监管机构或数据主体的要求提供建议
合规/隐私	就公司如何在事件期间履行职责提供建议和指导，管理数据映射以及帮助公司记录受影响的数据主体
公共关系	制定战略性和策略性沟通计划，以便告知信息和发挥影响力
财务	计算并管理遏制和纠正活动对盈亏的影响
客户服务	洞察有关客户/来电者行为
总裁/首席执行官	通过自身积极响应的行动，向公司全员展示防止数据泄露的重要性

- **事件响应融入业务连续性计划（BCP）**

许多公司都倾向于通过制定BCP来帮助其在危机时期顺利运营，了解响应规划及其实施前的准备对于事件响应至关重要，尤其是在知晓事件发生的最初24小时内。该计划通常由关键的利益相关者起草和维护，并阐明部门职责以及团队在事件发生之前、发生期间和发生之后必须采取的行动，事件管理中各阶段的控制措施如下图所示。



- **数据泄露通知**

不同司法管辖区的事件通知要求各有不同，如中国、欧盟、美国、新加坡都将政府监管机构和数据主体规定为通知对象，但优先通知顺序则有所差异。中国PIPL并未明确要求通知时限，而是采取“立即采取补救措施”+“及时通知”的要求；GDPR要求数据控制者一般在72小时内通知监管机构，只有在高风险的情况下才需要通知数据主体，并且没有规定通知的时限；美国各州法均要求企业尽快通知受影响的消费者，加州规定只有影响超过500名加州居民时，必须报告州检察长，部分州则没有向政府监管机构报告的规定；新加坡PDPA则要求企业必须尽快通知监管机构，且不得晚于企业对数据泄露进行评估日后的3个日历日。同时企业应关注自身所处行业，在特殊行业，如金融行业，因其数据泄露更有可能危及国家安全和公共利益，故上报义务的触发门槛更低。

- **事件监测工具**

对于全球性企业，能迅速发现并应对安全事件是保障数据合规的关键。通过部署安全运营平台，企业能够实现集中式监控、自动化的安全响应机制和一致的操作流程，构建起一个敏捷且具备扩展性的安全防护体系。这样的体系不仅能够及时识别和减轻潜在的安全风险，还有助于企业遵守日益严格的合规规定，并持续优化其风险管理策略。安全团队借此可以专注于解决更为棘手的安全问题，保障企业宝贵资产与数据的安全，同时应对法规的演变和挑战。具体内容详见腾讯云T-Sec安全运营中心。



数据合规审计

数据合规审计用于衡量企业是否遵守相关法律、法规、适用标准以及内部政策和程序。数据合规审计可以由企业内部审计职能部门、DPO或业务职能部门牵头执行，或通过外部第三方执行。具体执行时，评估的时机可以是定期安排的，也可以是应对特定的安全或安全事件，或者是响应执法机构的特定要求。数据合规审计是一种监督活动，包括审查和评价两个部分，审查和评价的对象是公司进行的数据处理活动，审查和评价的基线可以是法律、行政法规、公司内部制度要求，评价的结果应当体现公司是否遵守法律、行政法规、公司制度的内容。

在实务中，企业通常会结合人工审计和工具审计两种方式，利用人工审计的深度和经验以及工具审计的广度和效率，以实现更全面和有效的数据合规审计。

人工审计

人工审计在需要专业判断和经验分析的情况下尤为重要。它通常关注于流程有效性、合规性评估、风险管理和对复杂问题的深入分析。例如，在测试控制有效性时，审计组成员会采用询问、观察、检查和重新执行等程序判断控制措施是否满足既定标准。

工具审计

工具审计主要应用于自动化和大数据处理，快速处理和分析大量数据，如日志分析、数据分析和风险预测。详情可参考5.3.3节“数据合规审计”的内容。

监管沟通

在数据安全合规管理过程中，全球性企业面临着满足不同国家/地区的监管要求的挑战。有效的监管沟通策略对于企业至关重要，它不仅包括主动向监管机构提出合规问题、寻求正确的合规做法，也包括接受监管机构的问询和检查。

向监管请求合规指导

在多数国家或地区，数据合规管理规定通常需要监管机构的介入，比如在数据跨境传输前获取监管审批和对标准合同条款的备案等。当前，一些国家或地区的监管机构已经制定了详细的报批报备操作流程，如中国对于数据出境的评估要求、欧盟对于约束性公司规则（BCRs）的审批程序等。然而，也有一些国家或地区的监管机构尚未对外公布明确的监管报批报备流程指引，这要求企业主动与监管机构进行有效沟通以获取必要的指导。

接受监管问询与检查

全球性企业应在全球各分支机构指派专员负责与当地监管机构建立并维护沟通渠道。一旦监管机构发起问询或检查，应需迅速响应，及时提供监管所需的信息和材料。同时，在日常的数据合规管理过程中，企业应确保详尽记录所有数据处理活动，并妥善保存这些记录，以备监管机构审查或在必要时进行查询。通过上述措施，有利于企业向监管机构展现对数据合规的严肃态度，也确保了在监管互动中的透明度和响应效率。

数据安全与合规嵌入研发流程 4.3

数据安全与合规的贯彻落实依赖于在应用系统&产品研发流程的每一个环节，都严格遵循既定的数据安全标准和法律法规要求，确保数据在处理、存储、传输和访问过程中的安全性、完整性和合规性。这一过程要求研发团队将数据安全与合规性视为质量的核心要素之一，通过引入自动化工具、制定详细的安全规范、开展定期培训以及实施严格的审计机制，确保所有开发活动都能在满足业务需求的同时，有效抵御潜在的数据安全威胁，保护用户隐私和企业资产安全，从而构建出既高效又安全可靠的应用系统&产品。

4.3.1 Security and Privacy by Design

隐私设计（Privacy by Design）的概念强调了在应用系统设计初期就应主动融入隐私保护措施，确保隐私安全要求纳入到从数据收集到销毁的每个环节，避免事后补救。

- **隐私设计的七大原则（详见下图）：**



- 积极预防，而非被动救济；
- 默认隐私保护；
- 将隐私嵌入设计之中；
- 功能完整——正和而非零和；
- 全生命周期的保护；
- 可见性和透明性；
- 尊重用户隐私——以用户为中心。

- **隐私工程的目标**

隐私工程是一种将隐私保护原则和要求整合到产品或服务的整个生命周期中的方法。它旨在确保个人信息的安全和隐私得到妥善处理，同时满足特定领域的隐私需求。根据我国2022年正式发布的GB/T 41817-2022《信息安全技术 个人信息安全工程指南》，该标准为隐私工程提供了具体的指导，强调了以下五个目标（详见下图）：

隐私工程的五大目标

合法正当	遵循个人信息安全相关法律法规要求，处理个人信息具有明确、合理的目的，不通过误导、欺诈、胁迫等方式处理个人信息。
最小必要	处理个人信息与处理目的直接相关，采取对个人权益影响最小的方式，收集个人信息限于实现处理目的的最小范围。
公开透明	公开个人信息处理规则，明示处理的目的、方式和范围，提高产品服务个人信息处理的透明性。
不可关联	采用去标识化、匿名化等手段，减少个人信息关联到个人信息主体引起的安全风险。
可管理性	提供个人信息处理的管理机制，使用户和组织能够适当干预产品服务处理个人信息的过程。

4.3.2 IT系统开发生命周期中的安全隐私管控

IT系统的安全开发生命周期共涉及五个阶段，包含了需求分析、安全设计、安全开发、安全测试和安全发布。各阶段的数据安全与个人隐私合规要点详见下图。



- 需求分析
  - 描述

    确保应用系统在规划和建设阶段满足数据安全和个人隐私保护的要求。
  - 输入

    功能需求清单、适用的法律法规和政策标准等。
  - 主要活动

    a）安全合规基线：

    研究和梳理应用系统应满足的合规要求，形成一组预先定义的安全控制措施和标准，用于评估和确保应用系统的需求符合特定的安全要求和法规标准。来源包括法律法规、国家标准、行业标准、企业内部个人信息或数据安全管理目标和制度要求等。

    b) 数据分类分级：

    企业需要结合具体的业务功能、应用场景、流程等，对所涉及的数据进行分类分级，具体的标准可参考4.2.1.2章节。

    c) 需求分析：

    根据功能需求清单，识别应用系统中涉及到个人信息或重要数据处理的场景并分析其处理需求的必要性，包括但不限于：

    - 与业务功能或流程相关的个人信息或重要数据种类、数量、处理活动（包括处理目的、方式等）；
    - 可能涉及的系统和区域、存储方式、权限管理和保护方式；
    - 可能涉及的数据提供、共享、公开或出境活动。

    d) 需求评估：

    需求评估包括但不限于个人信息保护影响评估、个人信息保护合规评估、数据安全风险评估等。对需求评估过程中发现可能存在的安全风险，判断需求是否合理或风险是否过高，评估要点包括：

    - 个人信息或重要数据处理目的和处理方式是否合法、正当，是否超出用户授权或约定范围等；
    - 预期收集的个人信息或重要数据对实现产品服务功能的必要性。
  - 输出

    安全合规基线、调整后的功能需求清单

- 设计阶段
  - 描述

    基于需求分析，结合PbD原则，设计应用系统的安全功能和实现机制。

- 输入

  安全合规基线、功能需求清单、架构图、接口文档、功能组件清单等。

- 主要活动

  a) 制定安全设计规范，明确应用系统的安全功能设计要求或实现指南。

  b) 确定系统内所有数据处理活动的流程及其对应的系统模块。识别数据处理活动中涉及的相关方，并定义他们之间的数据流动，绘制数据流图。

  c) 在设计应用系统时，需围绕功能架构、数据处理活动和数据流图，细化并实施以下关键安全功能，包括身份认证与授权、账号与权限管理、密码与口令的安全策略、会话管理、组件与框架安全、网络访问安全控制、API安全、密钥管理、日志安全等。其中，在设计个人信息安全时，关键点包括常见的个人信息安全设计要点包括告知同意、撤回同意和账号注销、自动化决策、未成年人个人信息和个人生物识别信息保护等。

  d) 安全设计检查与评估：
  基于需求阶段确定的安全标准，制定检查清单，验证各功能模块的合规性。发现不合规或高风险问题时，进行调整并重新评估，直至满足安全要求。

- 输出

  应用安全设计文档（Security Design Document）。

- **开发阶段**

  - 描述

    在应用系统的开发阶段，针对安全设计进行开发实现，确保满足安全合规的要求。

  - 输入

    应用安全设计文档。

  - 主要活动

    a) 制定安全编码规范：为开发人员制定安全编码规范，避免在应用系统开发的早期阶段引入不安全的编码缺陷，降低后期修复的成本，提高整体的代码质量。其中，隐私合规重点关注以下方面：
    - 避免将敏感个人信息直接嵌入到代码；
    - 对输入个人信息的准确性、完整性等进行测试，并过滤恶意代码；
    - 在服务端进行输入和输出校验等。

    b) 编写安全测试用例：
    针对应用系统的安全需求，编写对应的安全测试用例，并梳理用例编号、用例名称、测试点描述、测试步骤描述、预期结果、测试结果等。

  - 输出

    安全编码规范、安全测试用例表。

- **测试阶段**

  - 描述

    在应用系统的测试阶段，对其安全功能进行测试，并对测试结果进行分析。

  - 输入

    安全需求、应用安全设计文档。

- 主要活动

  a) 代码审计：在安全测试环节，企业通常采用代码审计工具与人工审计相结合的方式，找出代码中存在的安全错误。常见的危险函数类型包括：SQL、文件上传、文件读写、文件删除、文件包含、命令执行、代码执行、XSS、变量覆盖、反序列化等。其中，隐私合规的重点包括：

  - 利用安全测试工具进行白盒测试，发现系统在编码、数据脱敏等方面的问题；
  - 利用安全测试工具进行黑盒或灰盒测试，发现产品服务在安全漏洞、权限控制等方面的问题；
  - 利用隐私测试工具对个人信息收集、敏感权限申请调用等进行静态和动态测试等。

  b) 漏洞扫描：

  利用自动化工具识别和分析目标系统、网络、应用的安全漏洞，尽可能早地发现安全漏洞并进行修补，包括端口扫描、服务识别、操作系统检测和漏洞探测并形成漏洞报告。

  c) 渗透测试：

  使用渗透测试工具如IBM Security X-Force，通过模拟恶意人员对系统应用的真实攻击，检验网络和应用的安全性，测试步骤包括范围界定、信息收集、识别和利用漏洞、系统复原、总结与报告。

  - 输出

    代码审计报告、漏洞扫描报告、渗透测试报告。

- **发布阶段**

  - 描述

    在应用系统的发布阶段，对安全发布进行评审，评审通过后对应用系统进行发布和部署。

  - 输入

    应用安全设计文档、测试阶段报告。

  - 主要活动

    a) 安全需求验证：根据项目安全管控活动中识别出的安全需求，由项目组成员进行书面确认，并由安全专家进行验证。对于不满足的安全需求，安全评审团队会针对SDL周期中各阶段发现的风险点进行汇总梳理，形成风险清单并追踪整改情况。风险清单包括风险等级、风险描述、建议修复方案、预计修复日期、负责人等。

    b) 发布准备和评审：

    产品服务发布前需通过安全发布评审，评审内容包括但不限于：

    - 发布前是否完成安全基准测试；
    - 发布前是否完成需求符合性测试；
    - 发布前是否完成安全合规性测试；
    - 发布前是否完成安全残余风险测试等。

    c) 安全配置检查：

    应用上线的安全管控活动均是在测试环境下进行验证的，而测试环境和生产环境的基础设施，共享服务、应用配置由于多种因素存在不一致的情况。因此在应用上线前，需要对生产环境的安全配置进行检查。

    d) 安全监控：

    应用系统发布后，宜对个人信息或重要数据安全风险进行监测，包括但不限于：

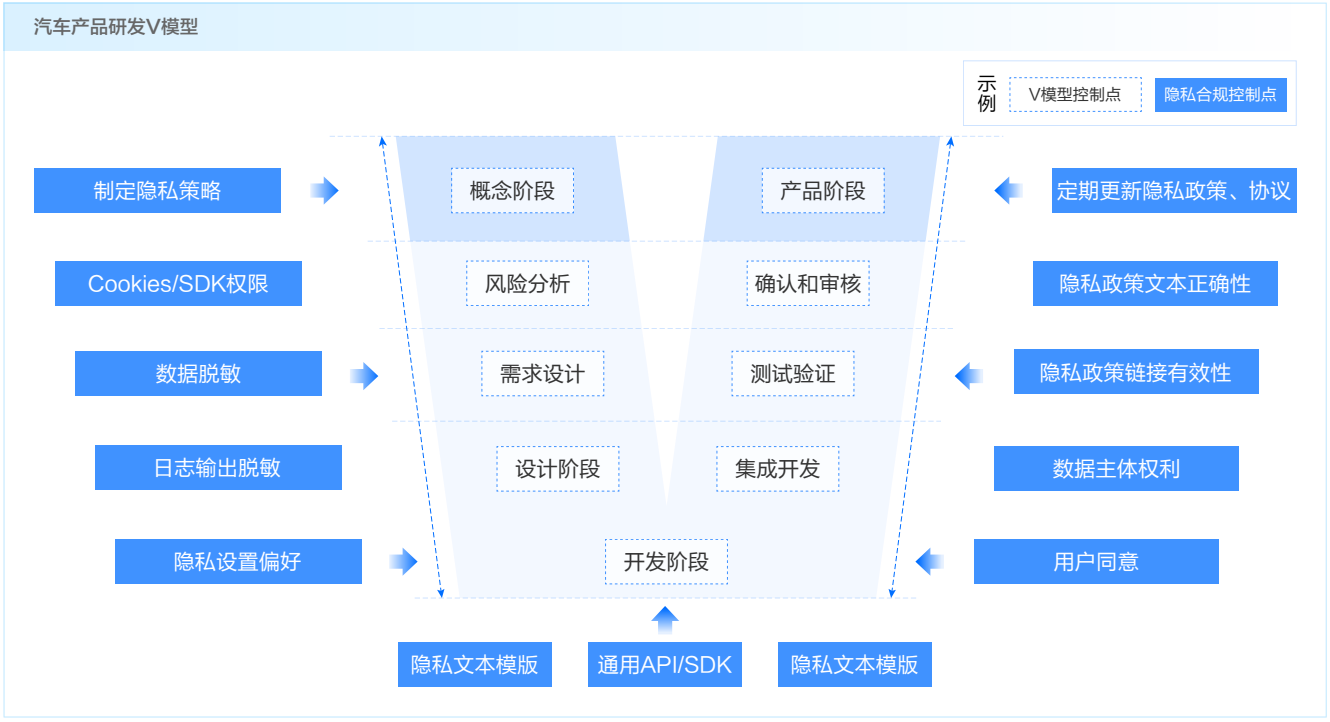
    - 外发数据流量监测，发现未授权个人信息传输，出境等风险；
    - 敏感API调用监测，发现超范围收集、未授权使用个人信息等风险；
    - 个人信息处理违规行为监测，发现个人信息使用过程中信息泄露、欺诈、恶意营销等行为；
    - 第三方应用个人信息处理行为监测，发现其未授权收集、使用、回传个人信息等行为等。

  - 输出

    安全配置基线、完成部署的应用。

4.3.3 工业产品（汽车为例）V模型的安全与隐私设计

本章节以汽车行业为例，详细阐述汽车产品研发V模型如何与安全隐私合规点相结合。



企业应将数据安全与个人隐私保护融入到汽车企业产品开发全生命周期V模型的各个环节中（如上图），包括：

- 在产品研发的概念及需求分析阶段，关注识别车辆与用户隐私相关的需求，如车内摄像头、位置追踪、用户数据管理等。明确车辆数据收集、存储、处理和传输的隐私要求，并制定相应隐私保护策略。
- 在产品研发的系统与架构设计阶段，针对隐私安全，应将PbD原则贯穿整个设计过程，考虑到包括隐私通知与交互界面分层设计、隐私政策更新通知、Cookies与SDK识别与权限收集设计、Cookies横幅设计、数据主体访问请求界面与对接、数据展示脱敏、日志输出脱敏、数据库设计和隐私设置偏好中心设计等。
- 在产品研发的开发与集成阶段，需要将隐私设计阶段的技术规范正确实施，参考隐私设计模式，建立可复用的技术组件、沟通话术、隐私文本模板、通用API/SDK等方法等都是良好的隐私工程集成实践。
- 在产品的测试验证阶段，还需要确保系统的隐私功能与后端的隐私管理平台或通用组件之间集成的正确性，包括后端平台是否能够正确收到用户同意记录、数据主体权利请求流程是否通畅、隐私政策文本正确性、隐私政策链接跳转是否有效、Web Cookies 是否与政策保持一致等。
- 此外还可以引入外部第三方隐私合规检测机构，通过模拟用户遍历产品功能、代码审查、动态监测、隐私政策内容提取分析等手段，从产品交互界面隐私设计，产品自身及第三方SDK获取用户数据的时间节点、频次、具体种类，获取系统权限的时间节点、频次，隐私政策披露用户数据收集和使用的真实、准确、完整性等多个维度对产品用户数据处理和隐私设计状况进行全面扫描， 并在此基础上验证其是否符合合规基线。

在产品的发布及后续运营阶段，主要进行规范跟踪，定期评估和更新隐私政策、用户协议和其他隐私相关的文件，确保其与最新的法律要求和企业隐私策略一致。

05

腾讯出海/数据合规服务产品及解决方案

腾讯云在数据合规中的责任与建议

腾讯云平台数据合规保障

腾讯云数据合规工具箱

腾讯云助力数据重要环节的安全合规

腾讯云在数据合规中的责任与建议 5.1

5.1.1 腾讯云全球合规资质认证

国际权威认证

CSA STAR 云安全认证

STAR云安全评估是由国际权威的非盈利组织云安全联盟（Cloud Security Alliance）推出的，针对云安全特性的一项国际性认证。它将ISO/IEC 27001信息安全管理体系进行拓展，结合云安全控制矩阵（Cloud Control Matrix， CCM），将云安全的特有问题可视化，为用户提供了直观的安全架构评估总览。

基于腾讯公司多年积累的安全实践，腾讯云于2016年9月获得CSA STAR全球金牌云安全认证，进一步确定了其国内领先的云服务提供商地位。

SOC审计

服务组织控制报告（SOC 报告）作为独立的审计报告，涵盖腾讯云平台的安全性，可用性与保密性相关控制点。根据不同的鉴证服务类型，可提供给云用户以及其审计师，以满足相关需求。

SOC 报告（System and Organization Controls Reports）是由专业的第三方会计师事务所依据美国注册会计师协会（AICPA）的相关准则出具的服务机构内部控制相关的系列报告。

腾讯云 SOC 1报告是参照 AICPA 审计准则 SSAE No. 18中的 AT-C section 320，针对腾讯云云服务体系的控制环境出具的报告，该报告与用户财务报告的内部控制相关。

腾讯云 SOC 2和3报告是参照 AICPA 审计准则 SSAE No. 18中的 AT-C section 205 以及 TSP section 100 2017版，针对腾讯云云服务体系的安全性、可用性和保密性相关的控制设计适当性出具的独立评估报告。

AICPA 在2017年4月发布了最新的2017版信托服务标准，并明确在新信托服务标准过渡期（2017年4月15日至2018年12月15日止），服务机构可以自行选择遵循最新的2017版信托服务标准或2016版信托服务标准。腾讯云作为领先的云服务提供商，在2017年 SOC 审计过程中已经使用了2017版的信托服务标准，是国内率先遵循了2017版信托服务标准的云服务提供商。

SOC 系列报告可以为腾讯云用户提供有价值的信息以供云用户评估和解决与服务机构相关的风险：

- **SOC 1报告：**云用户机构及其独立审计师可以结合 SOC 1报告及云用户自身运行的控制来评估用户机构财务报表的重大错报风险。
- **SOC 2报告：**云用户机构、独立审计师、监管机构、公司股东及其他相关利益方可以根据 SOC 2报告评估云服务商相关的内部控制（覆盖安全性、可用性、过程完整性、保密性和隐私性）的设计适当性和运行有效性。
- **SOC 3报告：**是 SOC 2报告的部分，简要介绍腾讯云产品和服务体系。云用户机构可以根据 SOC 3报告了解云服务商相关的内部控制。

ISO/IEC体系认证

ISO/IEC 22301：2012认证

ISO/IEC 22301是第一份以业务连续管理（Business Continuity Management，简称BCM）为主题的国际标准，提供了一种完整通用的BCM方法论，让企业能够达到国际上公认的最佳实践。该认证适用于所有行业中的大、中、小型公有及私有组织，并且特别适用于处于高风险和高度监管环境下的行业，例如金融业、IT通信业、制造业等。在企业业务的运行过程中，往往会受到各种内在或外在因素的影响，严重时甚至会导致中断业务，而意外的中断会给企业带来重大损失。为了降低风险，业务连续性管理受到了越来越多的重视。

腾讯云是国内第一批通过该项认证现场审核的云服务商，通过构建正式的业务连续性管理流程，保障自身业务的连续与稳定；同时，腾讯云为您提供一个具有组织弹性和有效响应能力的框架，与建设恢复能力框架的整体管理过程，以保障客户的业务不中断，维护您的利益、声誉、品牌以及价值创造活动。

ISO/IEC 27001：2013认证	ISO/IEC 27001：2013信息安全管理体系是国际上针对信息安全领域最权威、严格，也是最被广泛接受及应用的体系认证标准。通过该认证，就意味着企业已经建立了一套科学有效的信息安全管理体系，以统一企业发展战略与信息安全管理的步伐，确保相应的信息安全风险受到适当的控制与正确的应对。 腾讯云是国内首家获得ISO/IEC 27001：2013认证的云服务提供商，通过这套“量体裁衣”的信息安全管理控制措施和保护信息资产的制度框架，遵循PDCA持续的改进路线，对您的信息安全做出承诺，提供可靠的信息服务与相关安全保障。
ISO/IEC 20000-1：2018认证	ISO/IEC 20000-1：2018是针对IT服务管理制定的一套国际标准。该体系规范了企业的信息技术服务管理，从建立、实施、运作、监控、评审、维护与改进的模式，协助企业持续地识别与管理相关信息技术问题，强化与用户的沟通，建立一套自我完善的标准化服务体系。 腾讯云通过ISO/IEC 20000-1：2018新版标准认证，包含云计算服务、托管服务及灾备服务等方面的认证范围。腾讯云严格以服务至上的态度，完善与您之间的信息技术服务与沟通的机制。
IISO/IEC 9001：2015认证	SO/IEC 9001：2015是迄今世界上最为成熟的质量管理体系。该体系围绕企业产品或服务，提供指导性的纲领及规范，促进企业产品或服务完善全过程质量管理框架，是企业发展与成长的根本。 腾讯云是国内首家在云计算领域获得ISO/IEC 9001：2015 CNAS（中国合格评定国家认可委员会）和ANAB（美国注册机构认可委员会）认可的企业，认证范围含云计算服务、托管服务及灾备服务等。
ISO/IEC 27017：2015	ISO/IEC 27017：2015是一种国际标准，也是ISO/IEC 27002：2013的补充，加强了云计算漏洞的威胁和风险的控制。这项认证提供了37条 ISO/IEC 27002 指导以及7条ISO/IEC 27002中不具备的控制方案。云服务提供商和云服务客户都可以利用这个指导进行有效的设计和实施云计算信息安全控制。 腾讯云的ISO 27017指导证书不仅表明了我们会始终采用国际公认的最佳实践，也证明了腾讯云拥有专用于云服务的高精度控制系统。
ISO/IEC 27018：2014	ISO27018是一个由国际标准化组织（ISO）于2014年颁布的国际标准协议，是首个专注于云中个人信息保护的国际行为准则。通过ISO27018认证可证明企业在保护企业数据、知识产权、文档和云端IT系统安全等方面达到了高标准的行业最佳实践。 腾讯云的个人信息保护管理体系已进入了全球范围内云服务商的先进行列，为腾讯云客户带来充分信任的基础和坚实的云安全保障。

区域认证

德国C5审计

2020年08月31日，腾讯云产品通过德国 BSI C5：2020云安全基础及附加标准审计，证明腾讯云在云平台的安全策略制定和技术应用方面的全球领先性。云计算合规性标准目录（Cloud Computing Compliance Criteria Catalogue，简称C5），是由德国联邦信息安全局（BSI）制定，旨在基于标准化的检查和报告验证云服务提供商的信息安全符合性。

C5：2020标准包含了信息安全组织、安全政策和工作指引、人员、资产管理、物理安全等17个控制域的目标，并规定实现目标的一般原则、程序和措施。相比于2016年的版本，C5：2020基于《欧洲网络安全法》扩展云服务产品信息安全方面的标准，新增云服务提供商“处理政府机构查询”等方面的标准，对云服务商的安全管理水平提出了更严格的要求。

C5：2020标准不仅是云服务商与德国公共部门合作的必要云安全基准，更广泛地被欧洲乃至全世界的私营部门所采用，是云服务领域备受行业认可的高级别安全标准，也是云服务商符合《德国联邦数据保护法》（BDSG）和欧盟《通用数据保护条例》（GDPR）的重要途径。

通过 C5：2020基础及附加标准审计意味着腾讯云在数据保护和信息安全方面达到了德国政府设定的高标准，以及腾讯云遵循了严格的信息安全管理体系，确保符合GDPR等相关法律法规的要求。同时也意味着腾讯云在审计、资质、透明度等方面达到了德国政府要求，可以承载欧盟与德国市场的绝大部分企业乃至政府机构客户。

新加坡MTCS T3认证

腾讯云成功通过了新加坡多层云安全 (MTCS) T3级别标准的认证。新加坡多层云安全 (MTCS) 标准在新加坡资讯通信发展管理局 (IDA) 信息技术标准委员会 (ITSC) 的指导下拟定。 由 ITSC 负责推动国家 IT 和通信标准化项目的开展，并协助新加坡参与国际标准化活动。

MTCS 具有不同安全级别的云安全标准，涵盖第1级别中的基本安全性、第2级别中更严格的管理和租赁控制，以及第3级别中高效信息系统的可靠性和可复原性。其建立在公认的国际标准（例如 ISO/IEC 27001）基础之上，覆盖的领域有数据保存、数据主权、数据可移植性、可用性、业务连续性、灾难恢复和事件管理。MTCS 作为云的常用标准，云服务提供商 (CSP) 可采用该标准来解决客户对云端数据的安全性和机密性，以及使用云服务对业务的影响的顾虑。此认证意味着腾讯云提供了可验证的操作透明度，以及对客户在使用云服务时所面临的风险的洞察。

韩国KISMS认证

腾讯云通过了韩国信息安全保护管理体系（以下简称“KISMS”）认证，成为中国首家通过 KISMS 认证的云服务提供商，证明腾讯云建立的信息安全管理体系和能力满足相关韩国法律和标准合规性要求。

KISMS 认证是韩国政府支持的信息安全认证，由韩国互联网与安全局 (KISA) 主办，隶属于韩国科学与信息通讯技术部 (MSIT)，以韩国信息通信网相关法律为依据，旨在帮助韩国组织始终安全地保护其信息资产。KISMS 作为一个特定于韩国的信息安全保护框架，它定义了一组严格的控制要求，内容涵盖资产管理、访问限制、认证及权限管理、加密、灾后修复等领域，重点关注审核企业组织对企业信息、个人信息等重要信息及资产管理的安全性和可靠性。

腾讯云获得这一认证意味着，韩国的云上客户更易证明其遵守了本地法律要求，从而保护关键数字信息资产，并更容易满足 KISA 合规性标准。 也意味着腾讯云信息安全应对措施和威胁应对程序的能力得到进一步提升，能更加有效地减少安全漏洞的影响。

马来西亚金融行业IT合规遵从性审计

马来西亚国家银行（BNM）、马来西亚证券委员会（SC）等马来西亚金融监管机构，颁布了针对金融服务行业的7部相关法规条例，涵盖了包括金融科技风险管理、外包管理、数据安全和客户信息保护、业务连续性管理方面的监管要求，以规范信息科技在马来西亚银行、保险、证券等金融服务中的应用，从而保证金融信息系统的可靠性、安全性、稳定性。

腾讯云马来西亚金融行业 IT 合规遵从性审计，由独立第三方审计机构参照上述马来西亚金融监管机构颁布的法规条例的适用要求执行，审计方法遵循国际审计与鉴证准则理事会 IAASB 发布的 ISAE3000 准则的相关要求。

通过独立第三方审计报告可证明，腾讯云在马来西亚为金融客户提供的云服务，严格遵守了马来西亚金融行业的监管要求。客户也可通过获取腾讯云审计报告知晓腾讯云在金融服务领域的安全控制，对腾讯云安全控制的设计合理性与执行有效性进行全面快速的了解，可有效减轻使用腾讯云金融服务时对安全合规的顾虑。

泰国金融行业IT合规遵从性审计

泰国金融行业机构需遵守泰国央行（BoT）、 证券交易委员会办公室（OSEC）、保险委员会办公室 （OIC）等金融监管和相关法定机构所颁布的18部相关法规条例，其监管要求涵盖：信息技术运用中的风险管理、个人信息保护、信息技术在银行、保险、电子政务系统等系统、电子货币、支付系统基础设施、支付服务提供商等中的应用和安全控制等。

泰国金融行业IT合规遵从性、合规性审计是由独立第三方审计机构参照上述泰国金融监管和相关法定机构颁布的法规条例的适用要求执行，并遵循国际审计与鉴证准则理事会 IAASB 发布的 ISAE3000准则的相关要求。

通过独立第三方审计报告行可证明，腾讯云在泰国为金融客户提供的云服务，严格遵守了该国金融行业的监管要求。客户可通过获取腾讯云审计报告知晓腾讯云在金融服务领域的安全控制，对腾讯云安全控制的设计合理性与执行有效性进行全面快速的了解，可有效减轻使用腾讯云金融服务时对安全合规的顾虑。

印度尼西亚金融行业IT合规遵从性审计

印度尼西亚中央银行（Bank Indonesia）、金融服务管理局（Otoritas Jasa Keuangan，OJK）等印尼金融监管机构，颁布了针对金融服务行业的16部相关法规条例，涵盖了包括信息科技风险管理、个人数据保护、信息技术在银行、保险、电子政务等系统中的适用及安全控制、电子货币、支付系统基础设施、支付服务提供商等。

腾讯云印度尼西亚金融行业 IT 合规遵从性合规性审计，由独立第三方审计机构参照上述印度金融监管机构颁布的法规条例的适用要求执行，审计方法遵循国际审计与鉴证准则理事会 IAASB 发布的 ISAE3000 准则的相关要求。

腾讯云通过专业的由独立第三方审计机构执行的印度尼西亚金融合规性审计，证明腾讯云在印尼为金融客户提供的云服务严格遵守了印尼金融行业的监管要求，客户也可通过获取腾讯云审计报告知晓腾讯云在金融服务领域的安全控制，对腾讯云安全控制的设计合理性与执行有效性进行全面快速的了解，可有效减轻使用腾讯云金融服务时对安全合规的顾虑。

菲律宾金融行业IT合规遵从性审计

菲律宾金融行业机构需遵守 BangkoSentral ng Pilipinas（BSP）等金融监管和相关法定机构制定的8部相关法规条例，其监管要求涵盖：信息技术运用中的风险管理、个人信息保护、信息技术在银行、保险、电子政务系统等系统、电子货币、支付系统基础设施、支付服务提供商等中的应用和安全控制，确保金融信息系统的可靠性、安全性、稳健性和稳定性。

菲律宾金融行业 IT 合规遵从性、合规性审计是由独立的第三方审计机构参照上述菲律宾金融监管和相关法定机构颁布的法规条例的适用要求执行，并遵循国际审计与鉴证准则理事会 IAASB 发布的 ISAE3000准则的相关要求。

通过独立第三方审计报告行可证明腾讯云在菲律宾为金融客户提供的云服务严格遵守了该国金融行业的监管要求，客户可通过获取腾讯云审计报告知晓腾讯云在金融服务领域的安全控制，对腾讯云安全控制的设计合理性与执行有效性进行全面快速的了解，可有效减轻使用腾讯云金融服务时对安全合规的顾虑。

▶ 行业认证

PCI DSS 认证

PCI DSS（支付卡行业数据安全标准）是由 PCI SSC （支付卡产业安全标准委员会）开发并维护的。PCI SSC 是由美国运通（American Express）、美国发现金融服务（Discover Financial Services）、JCB、万事达（Master Card World-wide）和 Visa 国际组织五家支付品牌在2006年秋共同筹办设立的统一且专业的信息安全标准委员会。

PCI DSS 全称 Payment Card Industry （PCI） Data Security Standard，支付卡行业数据安全标准，是目前全球范围唯一且最为权威的支付卡产业数据安全标准。为增强持卡人的数据安全，PCI DSS 针对保护账户数据的技术和操作要求提供了全球统一的基准，适用范围涵盖所有涉及支付卡处理的实体，像商户、处理商、收单机构、发卡机构和服务提供商，以及储存、处理或传输持卡人数据的其他实体。

腾讯云已经通过 PCI DSS 认证审核，获得 PCI DSS 1级服务提供商资质。在 PCI DSS V3.2认证标准规范之上，针对云计算领域，发布了 PCI DSS 云计算领域指南 V2.0。腾讯云联合第三方测评机构 ATSEC 提供安全合规服务，为腾讯云上的用户在全球范围提供安全可靠的支付服务。

美国电影协会 MPAA

美国电影协会（MPAA）建立了一套安全存储、处理和传递受保护的媒体内容的最佳实践标准。MPAA 最佳实践旨在让与 MPAA 协会成员保持合作关系的应用程序和云服务供应商了解在内容安全方面应遵循的要求。媒体公司可以利用这些最佳实践，对内容管理进行风险评估和安全性审计。腾讯云已通过自评估的方式，确保其对客户内容的管理程序遵守美国电影协会（MPAA）内容安全模型指南。

MPAA 电影内容安全模板的组件参照了相关的 ISO 标准 （27001-27002)、安全标准（即 NIST、CSA、ISACA 及 SANS）和行业最佳实践。而 ISO 27001、ISO 27017、ISO 27018、PCI DSS以及 CSA STAR 等是腾讯云的重要合规项目，已通过第三方审计认证。

HIPAA 法案

1996年，美国颁布《HIPAA 法案》（Health Insurance Portability and Accountability Act/1996，Public Law 104 - 191，HIPAA），其立法目的之一在于推动电子健康记录的使用，以通过加强信息共享的方式，实现提高医疗保健系统效率和质量的提升。HIPAA 关注及保障实体及其商业伙伴在创建、接收、维护和传输等环节中，受保护的健康信息（Protected Health Information，PHI）的安全性（包括可用性、完整性和保密性）和隐私性。受 HIPAA 监管的实体及其商业伙伴需要在处理、维护和存储 PHI 等场景中提供相应的安全措施。

在腾讯云所提供的服务中，PHI 主要以电子的形式存在，我们称之为 ePHI（electronic Personal Health Information，ePHI）。ePHI 包含一系列非常广泛的可用于识别个人身份的健康数据及其相关数据。

腾讯云发布 HIPAA 自评估报告，阐述腾讯云对于用户个人信息的安全保护能力及控制的有效性。

5.1.2 腾讯云的合规资源与能力准备

腾讯云的合规资源主要以如下三个方面呈现：

- 腾讯云各类合规要求的遵从性报告或实施指引，这一方面表明腾讯云本身的合规性，使客户可以放心使用腾讯云；另一方面也能让客户在做自身的业务合规性建设时有更坚实的依托。详情请参考腾讯官网说明：
  https://cloud.tencent.com/act/event/compliance#mod4
  https://cloud.tencent.com/act/event/compliance#mod4
  https://cloud.tencent.com/act/event/compliance#mod4
  https://cloud.tencent.com/act/event/compliance#mod4
  除此之外，腾讯云也提供各类合规文档的下载，如各类SOC报告，以支持客户通过各类相关审计，下载链接为：
  https://cloud.tencent.com/act/pro/Tencent_Cloud_Compliance_Documents
- 白皮书：腾讯云为客户提供的各类白皮书，如《腾讯云安全白皮书》、《腾讯云数据安全白皮书》、《隐私白皮书》等，本白皮书也包括在内。详细信息请参考官网链接：
  https://cloud.tencent.com/act/event/compliance#mod5
  https://www.tencentcloud.com/zh/services/compliance
- 三方合作伙伴：合规认证方面的合作机构如下：
  https://cloud.tencent.com/act/event/compliance#mod6
  此外可以在腾讯云云市场或者通过腾讯云商务部门联系到可以提供合规咨询服务的咨询公司或律所。腾讯云长期和此领域全球知名的公司保持合作，可以帮客户快速链接到相应的资源。

5.1.3 角色：合规责任共担模型

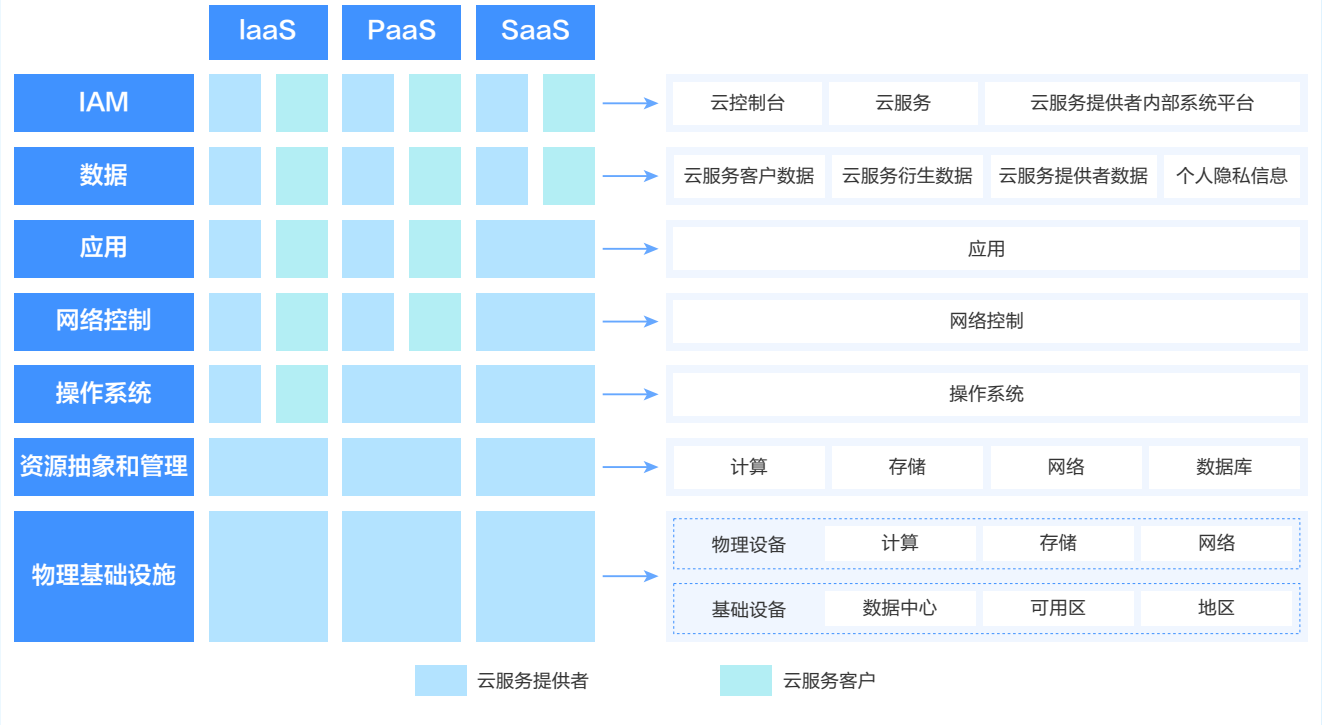
对于腾讯云来说，数据合规的责任共担模型是指腾讯云和客户之间共同承担数据合规责任的模式。

腾讯云的责任：

- **提供安全的基础设施和服务：**腾讯云负责提供安全可靠的云基础设施和服务，包括数据中心的安全、网络安全、数据加密等。
- **遵守相关法律法规：**腾讯云需要遵守相关的数据保护法律法规，例如 GDPR、 CCPA 等。
- **提供合规性工具和资源：**腾讯云通常会提供一些工具和资源来帮助客户满足合规性要求，例如数据加密工具、访问控制工具、审计日志等。
- **合规性咨询服务：**腾讯云并不直接提供合规性咨询服务，但可以在客户长期的合规能力建设过程中随时提供相关问题的解答或解读，同时腾讯云也会帮助客户引荐相关的专业合作伙伴，以帮助客户理解相关法律法规并制定合规策略。

客户的责任：

- **选择合适的云服务：**客户需要选择符合自身数据合规要求的云服务，并了解云厂商提供的安全保障措施。腾讯云完全满足各行各业以及全球各地业务的合规要求。
- **配置安全设置：**客户需要根据自身数据敏感程度配置相应的安全设置，例如访问控制、数据加密等。
- **管理数据访问权限：**客户需要管理数据访问权限，确保只有授权人员才能访问数据。
- **定期进行安全评估：**客户需要定期进行安全评估，确保数据安全措施有效。
- **及时响应安全事件：**客户需要及时响应安全事件，并采取必要的措施来保护数据安全。



责任共担模型的优势与目标：

- **提高数据安全水平：**通过责任共担，腾讯云和客户可以共同努力，提高数据安全水平。
- **降低合规成本：**腾讯云提供的工具和资源可以帮助客户降低合规成本。
- **提高效率：**责任共担模型可以帮助客户更有效地管理数据安全。

基于上述目标和上述合规责任共担模型，腾讯云将与客户进一步在更细粒度、更高层面上展开合作，共同应对企业出海过程中面临的各类问题与挑战。

腾讯云平台数据合规保障 5.2

本章节主要介绍，经过对全球各国数据合规要求的细致研究与遵守，腾讯云在数据合规领域提供的合规性能力保障。（本章节并不从场景化解决方案的视角来介绍产品，而只是展示腾讯云所具备的各项必要的合规能力，这些能力经过排列组合，可以支撑客户实现在绝大多数国家绝大多数场景下的数据合规技术方案。）

5.2.1 国际站账号

《腾讯云有两套账号系统，分别对应中国站和国际站，它们各自有不同的作用。中国站和国际站的账号系统是独立的，不能互相登录。

中国站账号系统

- **服务范围**：主要面向中国大陆地区的用户，提供腾讯云在中国大陆地区的云服务。
- **法律法规**：遵守中国大陆地区的法律法规，包括数据存储、数据安全等方面的规定。
- **支付方式**：支持人民币支付。
- **语言**：主要使用中文界面。

国际站账号系统

- **服务范围**：主要面向全球用户，提供腾讯云在全球各地的云服务。
- **法律法规**：遵守不同国家和地区的法律法规，例如 GDPR、 CCPA等。
- **支付方式**：支持多种货币支付，例如美元、欧元等。
- **语言**： 支持多种语言界面，例如英语、日语、韩语等。

对于企业来说，如果在中国大陆地区使用腾讯云服务，并且需要遵守中国大陆地区的法律法规，那么需要使用中国站账号系统。

如果是在其他国家和地区使用腾讯云服务，或者需要遵守其他国家和地区的法律法规，那么需要使用国际站账号系统。

5.2.2 云平台数据保护能力

腾讯云从以下三个方面确保云平台的数据保护能力。

物理安全

作为云计算服务提供商，腾讯云着力为每一个客户提供安全、稳定、持续、可靠的物理设施基础。腾讯云依据数据中心相关的国际标准和监管要求，遵循策划–执行–检查–改进（PDCA)的安全管理体系通用流程模型，建立了一套全方位的安全管理体系，从制度策略，到流程管理，并配合严格的监察审计，通过持续改进来保证云计算数据中心的物理和环境安全。



首先，腾讯云在全球的各数据中心均按照相关国际标准和当地安全要求进行选址、建设或租赁。

- 各数据中心电力系统和空调系统均采用高稳定性全冗余系统，任意单点故障，均不会影响数据中心的电力和供冷持续性。
- 各数据中心均配备完整的消防系统，包括定点区域火灾侦测系统、自动灭火系统以及供紧急使用的手动灭火装置。
- 各数据中心内部全部安装防静电地板，机柜、线槽等均安装接地线，用以防御静电给设备带来的损害。
- 腾讯云还要求所有机房管理人员定期接受安全教育培训和业务连续性应急演练培训，以确保数据中心基础设施的安全保障得到有效落实。

其次，腾讯云对数据中心采取了分级访问控制制度。腾讯云对数据中心不同区域定义了四类安全级别：

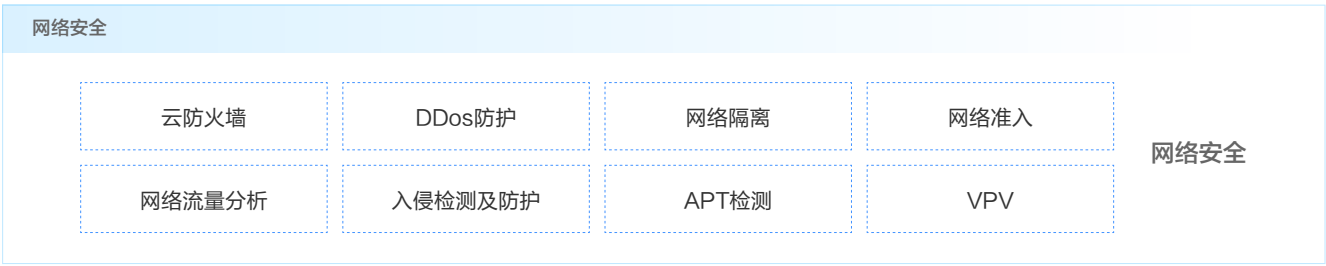
- 四级安全区域：不存放设备，不影响机房运营的公共区域，如园区等。
- 三级安全区域：存放业务信息的相关文件，涉及业务信息的办公区域，如办公区、运营中心等。
- 二级安全区域：存放非生产设备，不直接影响机房运营的区域，如库房等。
- 一级安全区域：存放运营设备，影响机房整体运营的区域，如客户专属机房、基础设施区等。

各数据中心根据不同级别的区域安全要求制订了严格的基础设施和环境访问控制。根据数据中心人员类别和访问权限，在门禁授权系统建立了完整的人员访问控制安全矩阵，实现对数据中心的各类人员的访问、操作等行为的有效管控。对于内部或外部员工，定期检查授权的准确性。员工辞职时，会及时清除所有权限并收门禁卡等访问控制物品。对于访客，必须提前提供有效身份证件号码、访问原因、访问时间、访问区域等信息申请授权。审批通过后，方可在约定的时间访问数据中心指定区域，且访问期间全程专人陪同

最后，腾讯云还提供了安全检查和审计制度。腾讯云各数据中心的安保人员每日均严格根据巡检清单和巡检计划对各机房和设备情况进行巡检，巡检频率不低于每2小时/次，巡检覆盖建筑物所有出入口、建筑物周边、楼宇内部等区域，并在每个检查点签名并记录检查时间，一旦发现安全违规事件，会立即启动数据中心机房管理紧急流程。各数据中心均已制订了物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。所有安全事件均会详细记录和分析，用于持续改进和提升现有安全管理规范和制度。

网络安全

腾讯云提供成熟的网络安全架构，包含防火墙、web应用防护等多重防护机制，以应对来自互联网的各种威胁。



其中主要包含四大类网络安全能力，分别是：网络通信安全、网络隔离、网络冗余与攻击防护。

- **在网络通信安全方面**，客户在腾讯云云产品控制台上的通信都受到了HTTPS安全协议的加密保护。客户也可以选择腾讯云提供的安全通道进行网络数据传输，如云计算平台内部实例之间的虚拟私有网络VPC，以及通过互联网连接云计算平台的专线网络与VPN。腾讯云的云产品所提供的云API接口具有HTTPS加密、签名校验、状态监测等安全能力，能为客户的业务提供端口级别的通信安全保障。

- **在网络隔离方面**，腾讯云制定了严格的内部网络隔离规则，通过物理和逻辑隔离方式实现内部的办公网络、开发网络、测试网络、生产网络等的访问控制和边界防护；腾讯云确保非授权人员禁止访问任何内部网络资源；以及，所有员工如需从公司网络前往生产网络开展日常运维时，都必须经过堡垒机登录生产系统。针对云端用户层面的网络访问隔离，腾讯云提供虚拟化控制层资源访问控制策略、云平台内部私有网络间隔离策略、Web控制台权限分配与身份验证、接口会话ID与访问密钥等安全机制，确保每位用户只能访问其已购买的云计算资源，有效实现多用户之间的访问隔离。

- **在网络冗余方面**，腾讯云基础网络采用N*N的冗余建设方式，配合路由层级的路径优先和路由可达性的流量工程调度，确保网络服务不会因为单点设备故障而中断。腾讯云的计算节点也是采用N*N的冗余建设方式，单一计算节点在故障发生时通过调度器实时自动剔除，有效保障用户业务的可用性。

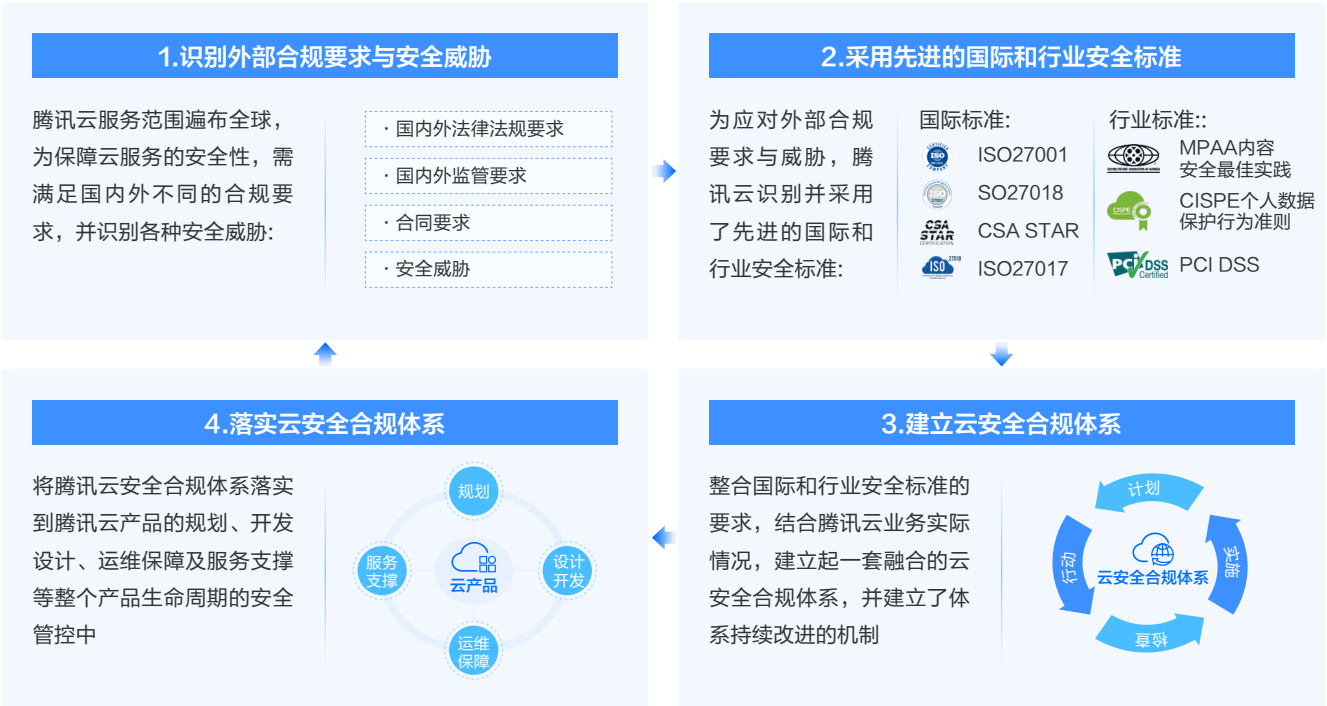
- **在攻击防护层面**，针对DDoS攻击，腾讯云为客户提供高效的防护能力。如DDoS防护（大禹），接入多线BGP线路，覆盖国内外主流及中小运营商，带来极速、稳定的访问体验，拥有xT防护带宽，可为社交文娱、游戏、跨境电商、智能制造等各类客户提供稳定的防护。

云产品确保客户数据安全

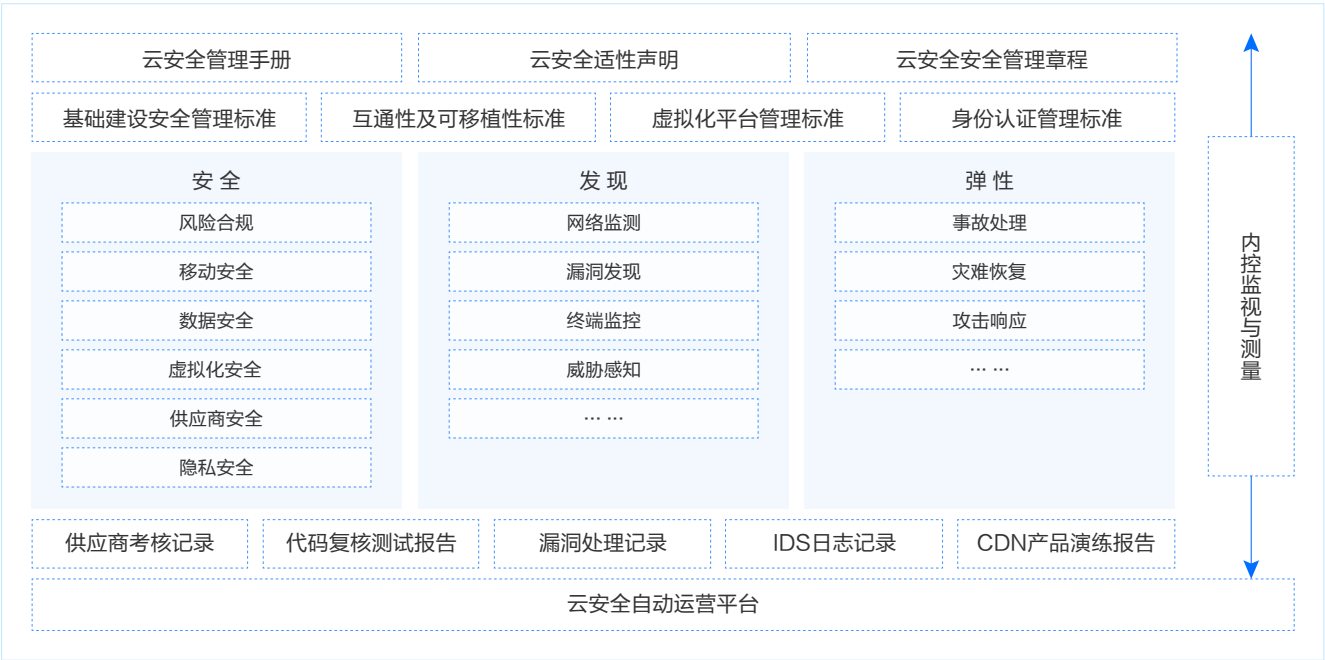
腾讯云提供各类云产品，以增强客户云上的数据保护能力。这些产品主要包括四类：安全类产品，计算与网络类产品，存储与CDN产品，以及数据库与大数据类产品。此节暂不展开，详细信息可参考5.3节

5.2.3 云平台数据安全治理体系

随着云计算、数字化技术的不断演变，各行业监管要求的日趋复杂，以及企业业务发展遇到越来越多的新问题（如出海在带来业务发展的同时，也会让腾讯云接触更多的风险面与监管面），安全合规性已然成为云服务提供商面临的一大挑战。“打铁还需自身硬”，腾讯云作为诸多出海中国企业的技术底座，一直致力于建立高效的安全合规体系与安全内控体系，紧随不同行业、领域、国家的合规要求，从制度流程及控制活动等方面完善自身的合规基础。

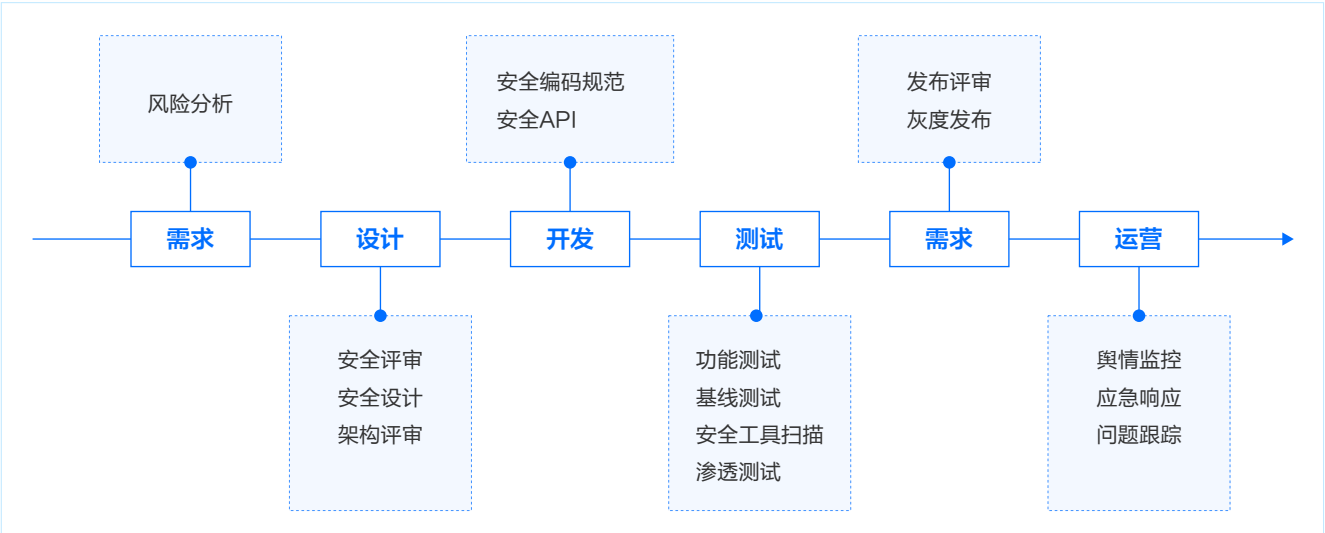


腾讯云也构建了统一的云安全内控体系，以云安全管理章程与云安全管理手册为指引，从基础建设安全管理、互通性及可移植性、虚拟化平台管理、身份认证管理等方面制定相应的合规标准，并细化到安全、发现与弹性三大方面的具体安全合规控制要求，通过内控监视与测量程序进行纵向管理，确保整个腾讯云安全内控体系的有效与高速运行。



5.2.4 云平台供应链合规

云平台供应链合规，是指提供给客户的云产品从设计、开发、生产、交付到使用全过程的合规性，确保整个供应链的安全可靠。在为客户提供的每一个云产品的背后，腾讯云着力将ISO/IEC 20000信息技术服务管理标准和ISO/IEC 9001质量管理体系标准融入到整个产品SDL安全开发流程中，关注需求、设计、研发、测试、交付、运维等不同环节，在产品开发各个阶段中消除信息安全和隐私问题，确保所有的云产品在其生命周期内均能获得足够的安全管控与评估。



为了保证最终的用户安全，腾讯云严格按照安全开发生命周期方法，开发云平台及云产品，目标是将信息安全融入到整个腾讯云的软件开发生命周期中。腾讯云的软件开发生命周期主要由以下几个部分组成：

- 安全培训(training)：针对开发人员推广安全编程意识，严格要求相关人员遵循安全编码的规范。
- 需求分析(requirements)： 针对业务内容、业务流程、技术框架进行沟通，寻找安全嵌入的最优方式。
- 系统设计(design)： 对系统设计进行威胁建模，对采用的架构进行安全技术评估。
- 实现(implementation)：开发过程中，提供腾讯自行设计的安全开发组件供研发人员使用；
- 验证(verification)： 通过渗透测试和代码审计发现漏洞。
- 发布(release)： 经过信息安全部门的最后检查确认后，系统才能发布到线上环境，以防止产品携带安全漏洞在生产环境运行。

通过上述流程和步骤，腾讯云可以确保提供的云产品符合合规要求：一是产品本身的组件和成分是合规的；二是客户使用腾讯云的产品也不会存在合规方面的问题。

5.2.5 云平台数据留存与删除管理

企业在腾讯云平台上留存的数据分为三类：

第一类：客户自身的用户信息，如公司名称，注册邮箱，账号，账号密钥等。

对于第一类数据，客户可自行在控制台进行查阅、更正、补充、复制、删除等操作。当客户或腾讯云协助您客户删除相关信息后，因为适用的法律和安全技术限制，腾讯云可能无法立即从备份系统中删除相应的信息。为此，腾讯云将安全地存储客户的个人信息并限制对其的任何进一步的处理，直到备份可以清除或实现匿名化。在客户主动注销账户之后，腾讯云将停止为客户提供产品或服务，并删除客户的个人信息（自身的用户数据），或对其进行匿名化处理，但法律法规或行业监管规则另有规定的除外。总而言之，腾讯云用户可以顺畅地在腾讯云平台上实现其数据主体权利。

第二类：客户的业务数据，如客户app的用户数据，客户广告系统的打点日志等。

对于第二类数据，腾讯云不会触碰或知悉客户在云环境中的客户内容，客户内容被腾讯云内部定义为绝密级别，没有客户授权任何人无权访问。对于云上的业务数据的管理和保护，腾讯云建议每个客户根据自身适用的安全标准（如ISO/IEC 27001： 2013、ISO/IEC 27017： 2015、等级保护要求等）以及各自企业既定的安全保护机制，来定义和实施云上业务数据的保护。

第三类：云平台的运维数据。

腾讯云负责分析和处理公有云产品底层产生的非用户层面日志信息，包括物理环境设施、网络设备、服务器硬件、数据库管理系统等。作为腾讯云公有云产品的使用者，企业仍需要关注基于公有云计算平台的业务运营活动中所产生的各类日志信息（访问记录、操作日志、系统状态信息、告警信息、错误提醒等），以实现更好的安全管控和风险处置。

数据的删除很难通过应用代码层进行真正的删除，因为应用层的删除大都是指“逻辑删除”，用户的数据实际上还是存在于云平台的各类存储介质上。所以想要进行符合数据合规的“真正删除”，必须要云平台的产品层面的能力。客户可以通过云平台提供的产品和工具对第二类和第三类数据进行留存或删除。客户在其账号注销后腾讯云将不会继续为客户提供云产品或云服务，与此同时，留在云产品或云平台内的客户的业务数据和运维数据也将删除。

5.2.6 云平台数据合规问题应对体系

腾讯云拥有多地域互备的客户服务中心，能够7*24不间断处理来自客户的建议与咨询。在标准服务的基础上，针对大型客户或特殊客户我们能够确保提供一对一的专家服务，帮助您更好地应用腾讯云提供的云产品。

腾讯云十分关注客户体验 ，为了更好地了解和满足您的需求，腾讯云主动通过多个渠道来获取反馈信息：

- **来自监管机构：**通过与各地通管局、网监局的共同协作，及时获取与腾讯云自身或您的业务活动相关的安全通告。
- **来自内部反馈：**腾讯云已建立的舆情监控系统能够获得内部人员的实时安全问题反馈。
- **来自互联网：**腾讯云客户服务中心对诸如V2EX、微博等互联网信息渠道进行监控。

腾讯云客户服务中心为客户提供业界领先的服务响应时效和处理质量。客户的满意是腾讯云不懈的追求，运营管理团队同客户服务中心通力协作，全年能够累积达到99%的客户满意度。

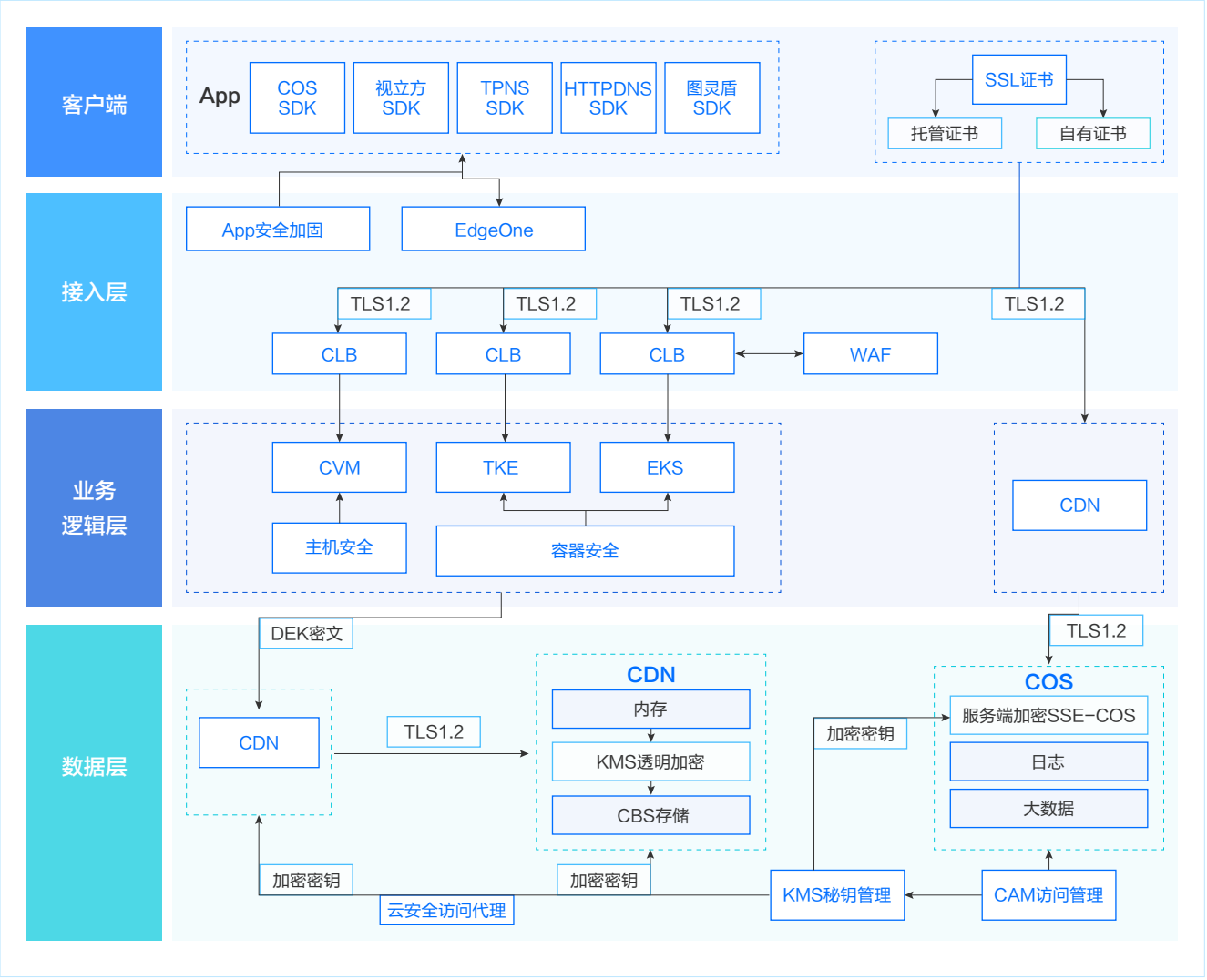
5.2.7 云平台的透明性与可审计性

腾讯云通过大数据处理和可视化分析，实现对所有内部运营活动的全面自动化监控。监控的对象包括所有的后端系统组件（如网络设备、物理服务器、数据库及管理系统等），并可根据系统组件的不同功能和使用情况设置告警阈值，一旦出现监控告警则迅速通知相关人员进行评估与处置。

腾讯云生产环境已全面部署堡垒机，通过堡垒机将腾讯云后端系统组件的管理员账号权限进行集中管控。运营管理团队人员仅能使用堡垒机新赋予的账号并通过二次身份校验（如动态验证口令）进行登录，自动获得适当的系统操作权限。所有后台运维操作记录均由日志平台集中加密存储，由腾讯云内部审计团队定期对记录信息进行审核。

5.3.1 数据安全

在数据合规领域，从技术层面上来说，确保网络安全与数据保护的方案需要综合考虑客户端、接入层、业务层和数据层的实现。以下是腾讯云与之相关的产品方案大图。



密钥管理

云上的密钥管理与数据加密是确保云数据安全的重要组成部分。它涉及到密钥的生成、存储、使用、销毁等各个环节，需要一个安全可靠的管理体系来保障。腾讯云主要依托KMS产品（也叫T-Sec密钥管理系统）来进行密钥管理。其包含如下能力:

- **密钥生成**

  密钥生成器： 云平台提供密钥生成器，用于生成随机、强壮的加密密钥。

  密钥长度： 密钥长度应足够长，以确保安全性，例如128位、256位等。

  密钥类型： 密钥类型包括对称密钥和非对称密钥，根据不同的加密场景选择合适的密钥类型。

- **密钥存储**

  硬件安全模块（HSM）： HSM 是专门用于存储和管理密钥的硬件设备，具有更高的安全性。

  云密钥管理服务（KMS）： 云平台提供 KMS 服务，用于存储、管理和使用密钥。

  密钥版本控制： KMS 提供密钥版本控制功能，可以管理不同版本的密钥，方便进行密钥轮换和更新。

- **密钥使用**

  密钥访问控制： KMS 提供密钥访问控制功能，可以限制对密钥的访问权限，确保只有授权人员才能使用密钥。

  密钥轮换： 定期轮换密钥，降低密钥泄露的风险。

  密钥审计： 跟踪密钥的使用情况，记录密钥的使用日志，方便进行审计。

- **密钥销毁**

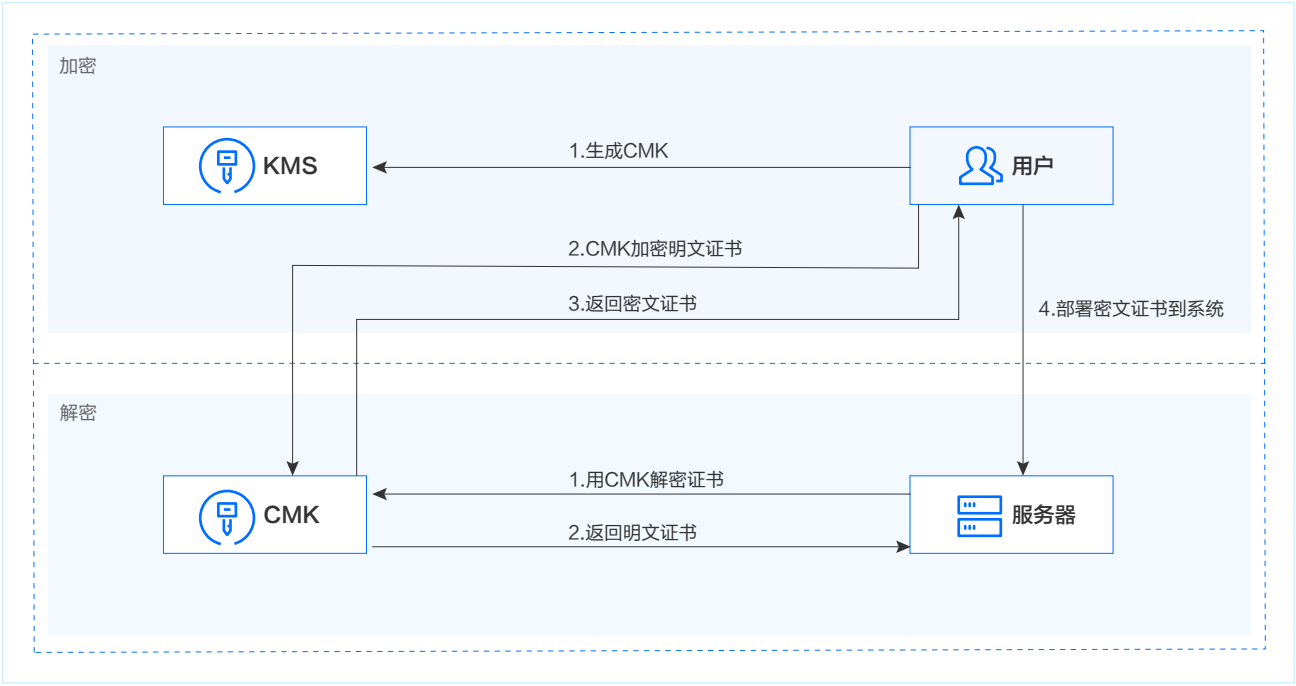
  密钥销毁机制： KMS 提供密钥销毁机制，可以安全地销毁密钥，防止密钥泄露。

  密钥销毁记录： 记录密钥销毁的日志，方便进行追溯。

以下是使用密钥管理进行数据安全防护的典型场景与腾讯云解决方案：

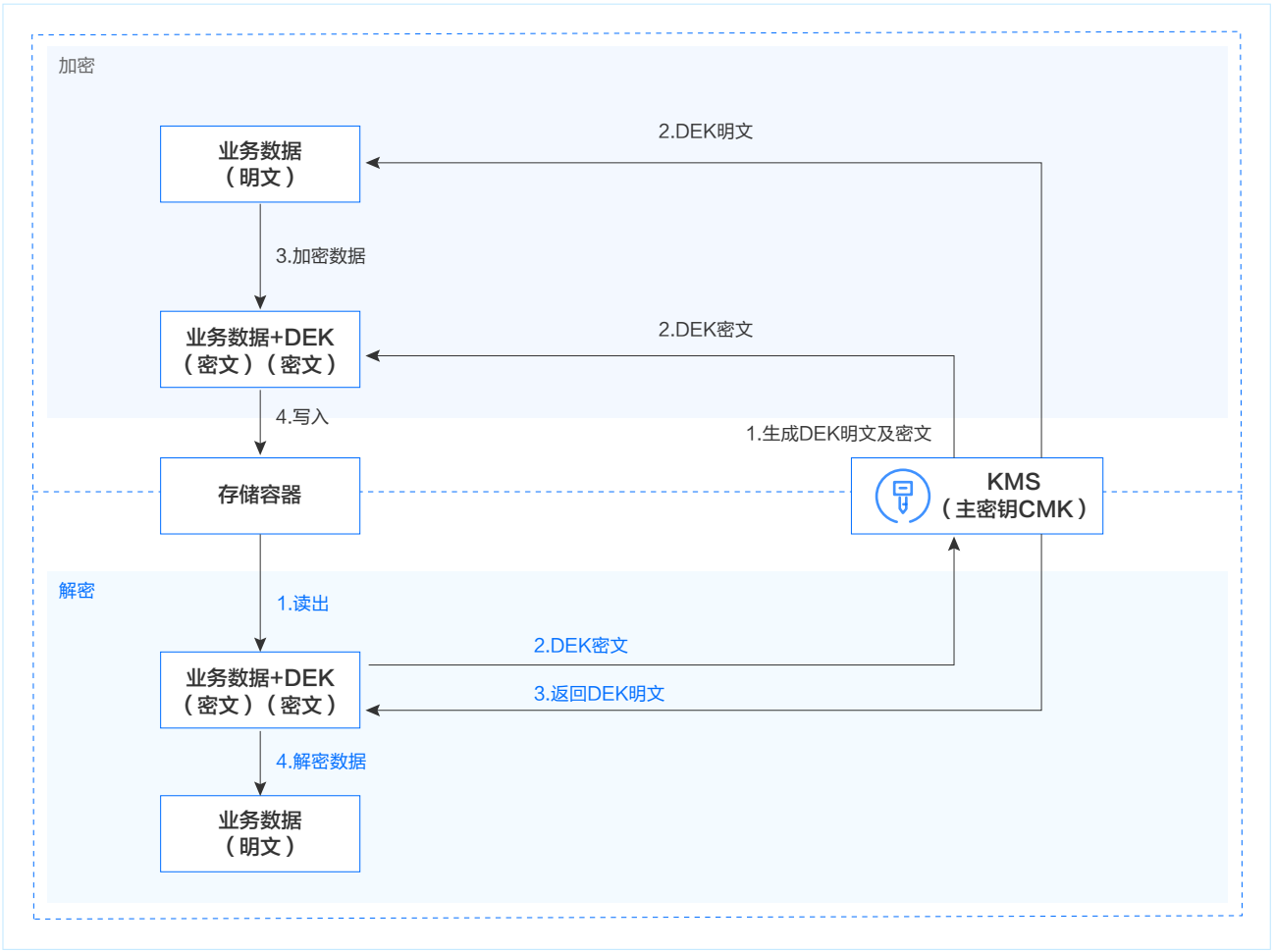
- **敏感数据加密**

  敏感信息加密是密钥管理系统核心的能力，实际应用中主要用来保护服务器硬盘上敏感数据的安全（小于4KB），如密钥、证书、配置文件等。企业主要面临的挑战是机密信息泄露、加密通道安全问题、签名被伪造。客户可以通过密钥管理系统的 API 或在线工具对密钥加解密，加密后本地保存密钥的密文文件，使用时解密且不保存本地，使得攻击者难以获取，从而保证网页和应用的安全性。



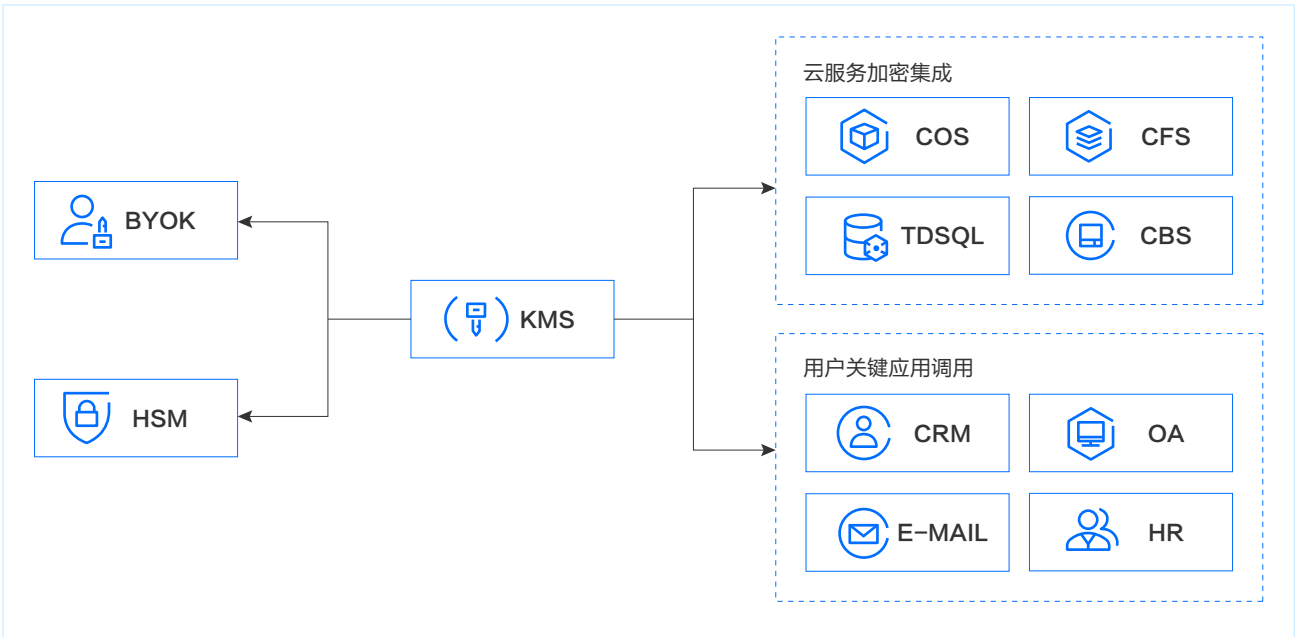
- **信封加密**

  信封加密（Envelope Encryption）是一种应对海量数据的高性能加解密方案。在密钥管理系统的信封加密场景中，只需要传输数据加密密钥 DEK 到密钥管理服务端（通过 CMK 进行加解密），所有的业务数据都是采用高效的本地对称加密处理，对业务的访问体验影响很小。企业可将所有核心数据通过数据密钥加密，保存在对应的存储容器内，数据密钥再经过密钥管理服务加密，为核心数据提供双重保护。同时，缺乏有效权限的人员，即使拿到密文的数据密钥和数据，也无法得到其中内容，保障核心数据不会泄漏。



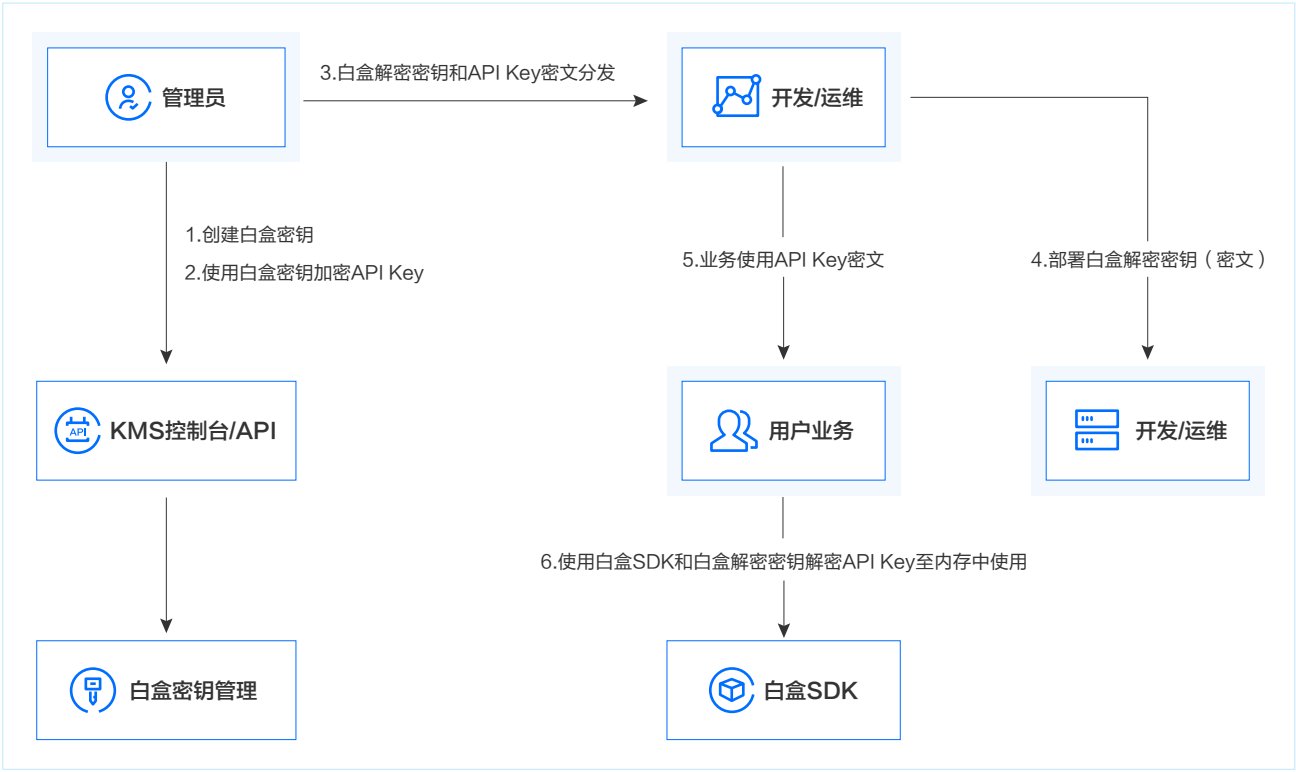
- **密钥导入**

在腾讯云上实施 BYOK（Bring Your Own Key）方案，允许客户在腾讯云架构上使用客户自有的密钥材料进行敏感数据加解密服务。可通过 KMS 服务生成一个密钥材料为空的 CMK，并将自己的密钥材料导入到该用户主密钥中，形成一个外部密钥 CMK（EXTERNAL CMK），再由 KMS 服务进行该外部密钥的分发管理。



- **白盒密钥管理**

白盒密钥用于保护端上的敏感根密钥信息，例如 API SecretKey，用户内部系统使用的鉴权密钥或 token，其它本地敏感根密钥信息等。使用白盒密钥管理工具加密 API SecretKey，实现 SecretKey 的保密性，即使密钥丢失，也不容易造成信息的泄露。



数据加密

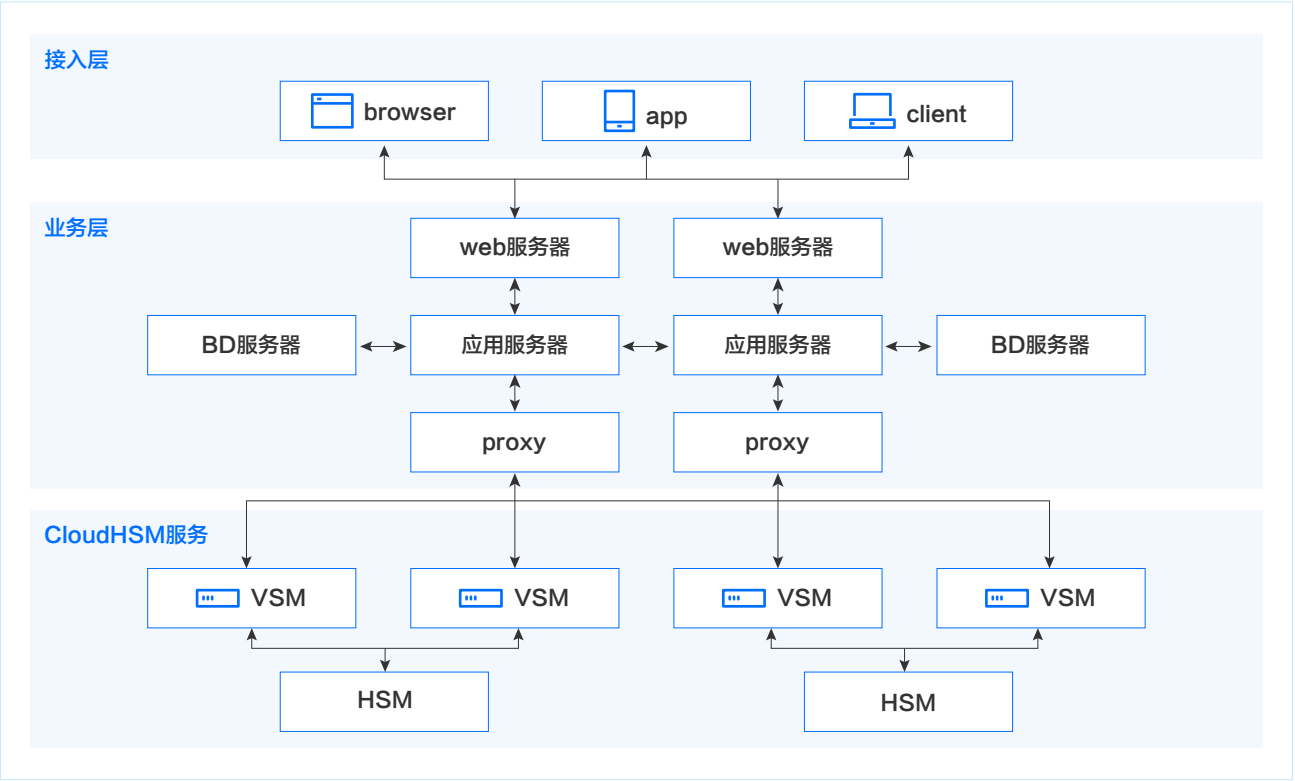
数据加密分为对称加密（使用相同的密钥进行加密和解密，例如 AES 算法）与非对称加密（使用不同的密钥进行加密和解密，例如 RSA 算法）。从加密方式来说分三个阶段：

- **数据在传输过程中的加密：**使用 TLS/SSL 等协议对数据进行加密传输。
- **数据在存储过程中的加密：**使用加密算法对数据进行加密存储。
- **数据在使用过程中的加密：**使用加密算法对数据进行加密使用，例如对数据库中的敏感数据进行加密。

腾讯云主要通过云加密机（Cloud Hardware Security Module，CloudHSM）产品提供数据加密服务。CloudHSM利用虚拟化技术，提供弹性、高可用、高性能的数据加解密、密钥管理等云上数据安全服务；符合合规要求，满足金融、互联网等行业加密需求，保障客户的业务数据隐私安全。其典型应用场景如下：

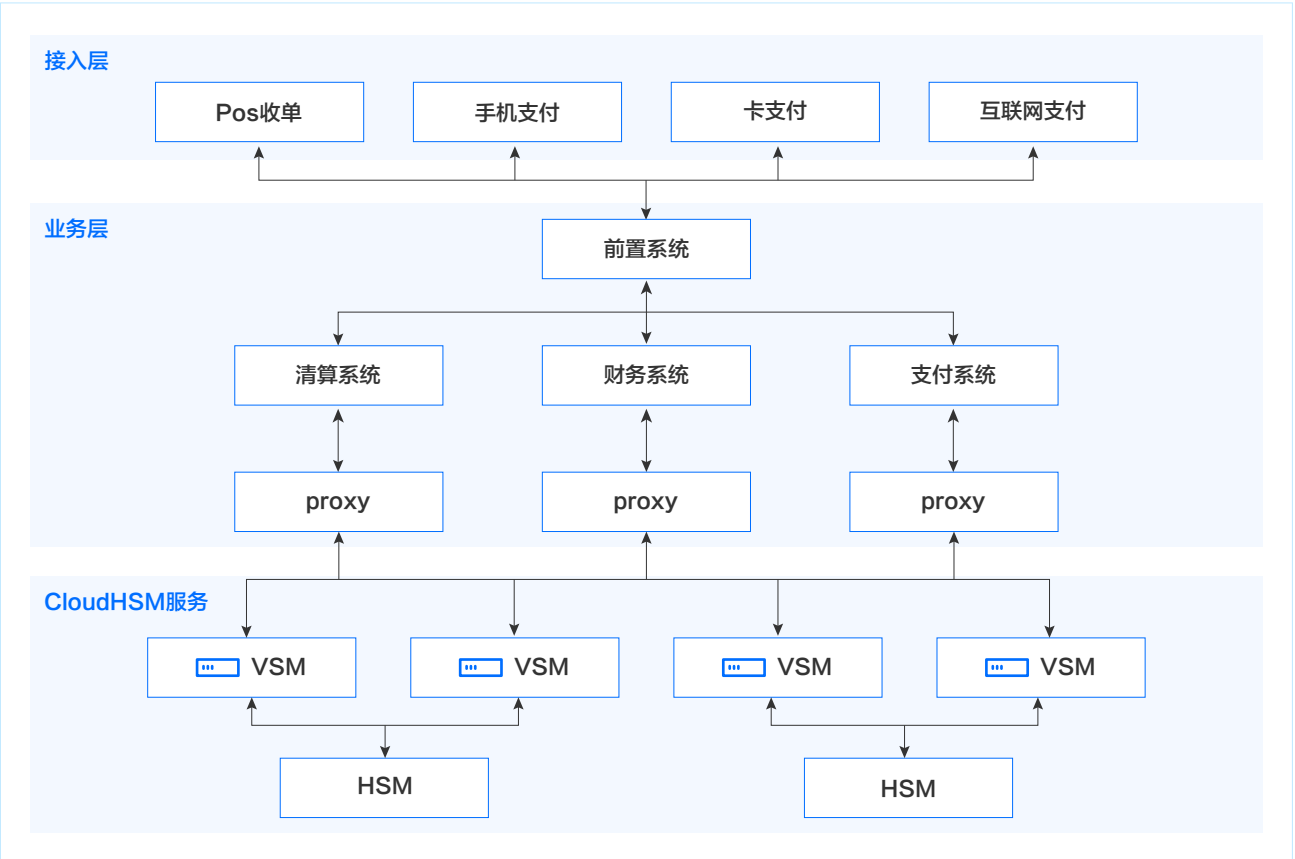
- **敏感数据加密**

应用于电商、门户、Web站点等需要对数据加密保护的系统应用。杜绝了明文数据被泄露和篡改的风险，提升系统的健壮性和客户价值。



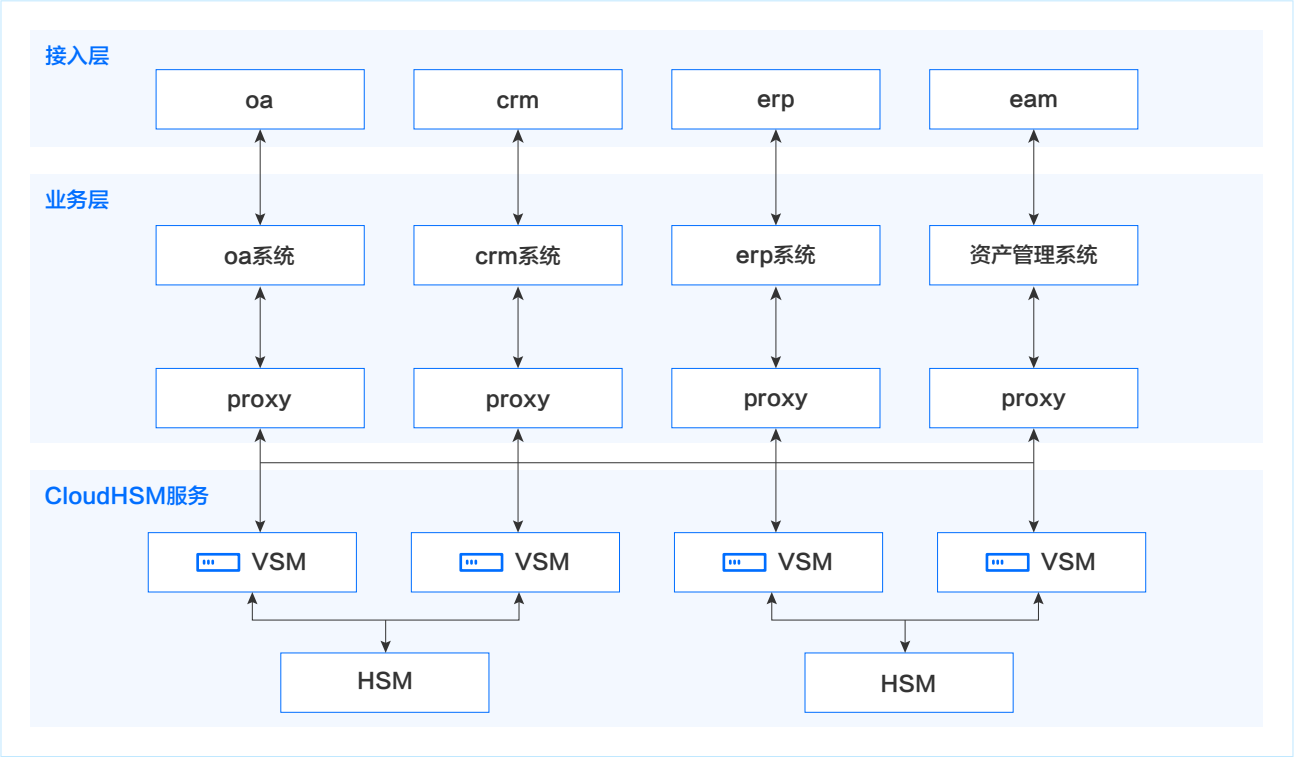
- **金融支付**

  应用于 POS 收单、互联网支付、预付费卡支付等各类第三方支付应用中，保证支付数据在传输、存储过程中完整性、保密性，并满足行业合规要求。



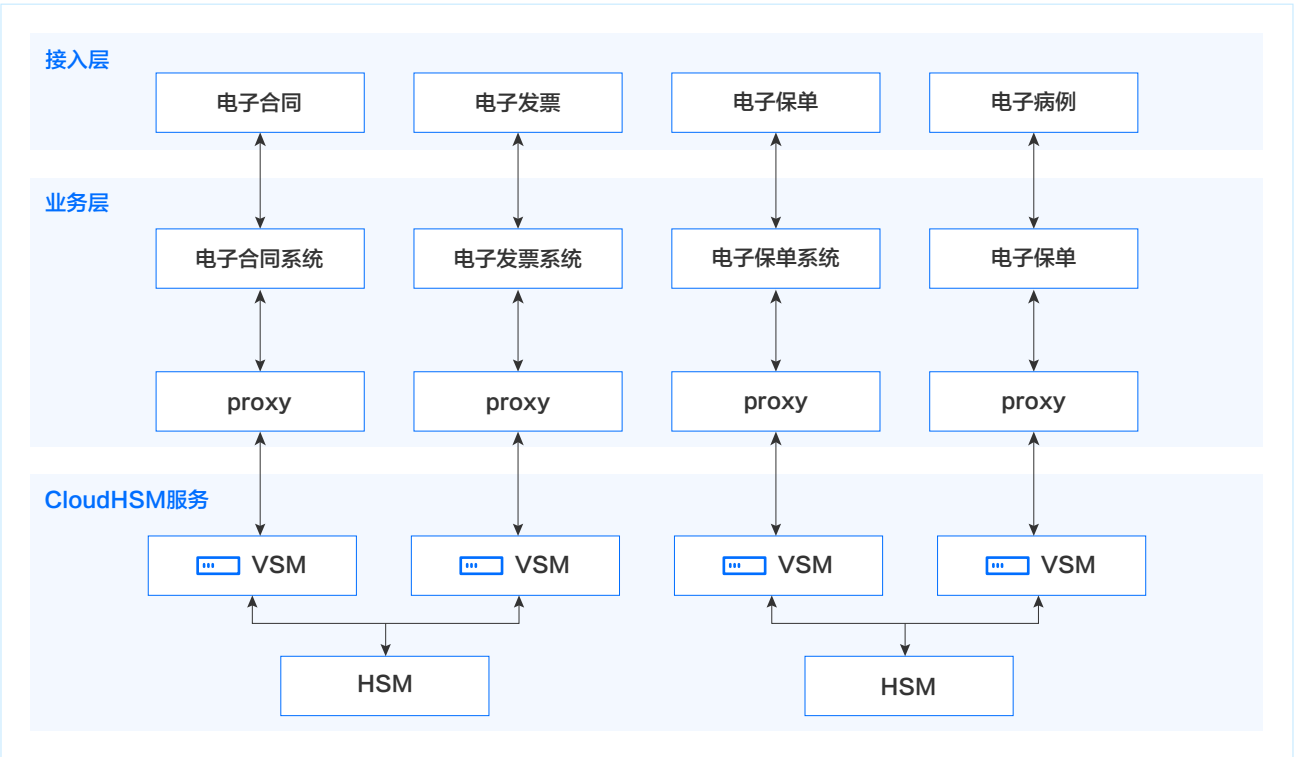
- **企业信息系统**

应用于大型企业的敏感数据保护，如企业资产、财务报表等加密保护及认证服务，保障企业资产安全性，防止无授权用户的访问。



- **电子票据**

应用于电子病例、电子发票、电子合同、电子保单等各类应用，确保电子票据类的应用用户身份的真实性，票据数据的生产、传输、存储过程中的完整性和安全性，符合监管合规要求，保障了电子化安全性，促进电子化业务发展。

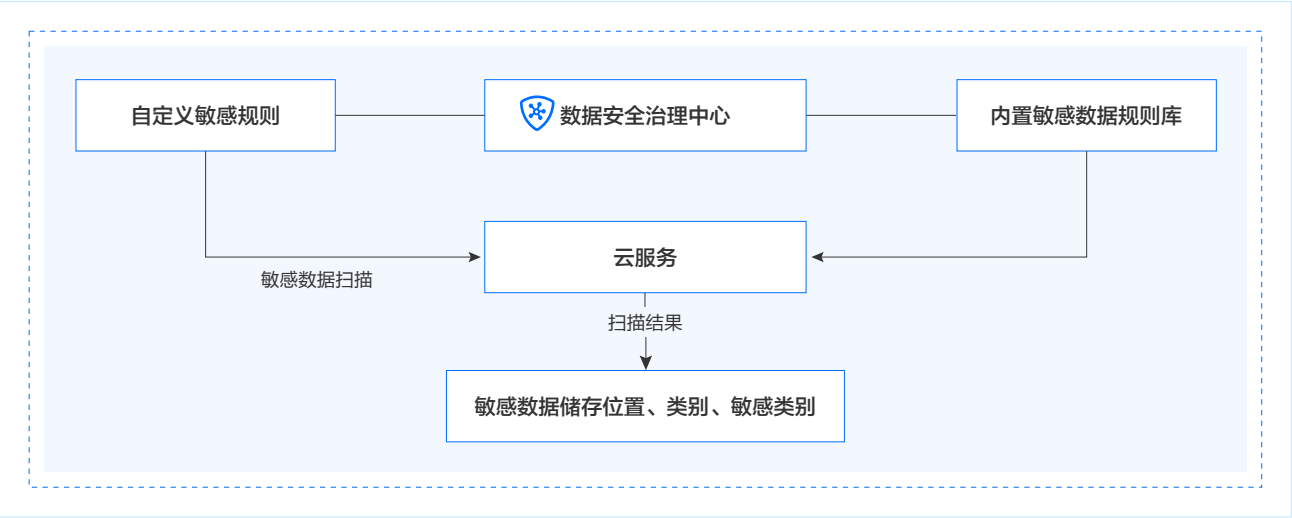


数据安全治理

腾讯云主要基于数据安全治理中心（Data Security Governance Center，DSGC）这款产品提供数据安全治理服务。DSGC从企业数据安全治理、数据安全合规出发，提供云原生数据资产管理、数据分类分级、风险评估等能力，帮助企业解决合规应对、敏感数据排查、数据安全风险检测等多方面的数据安全问题，降低数据安全治理TCO，提高数据安全保障能力。它主要提供四方面能力：

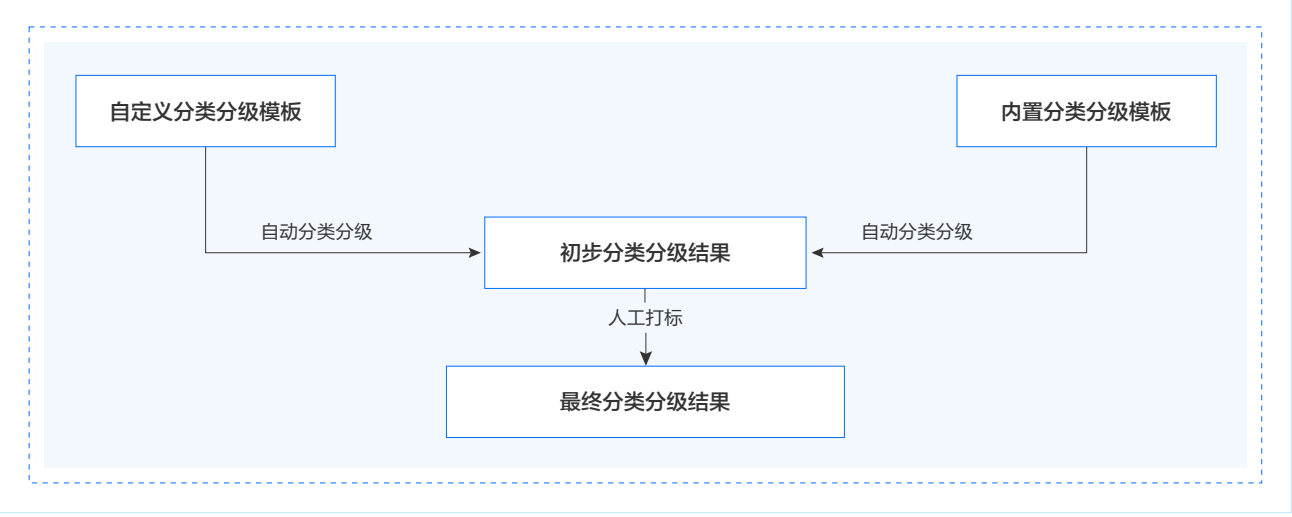
敏感数据梳理

对企业云上数据资产进行梳理，明确敏感数据的分布，并按照识别规则进行分类和分级，从而帮助企业更为有效地整理数据资产，为合规要求的建设和数据安全的实施部署提供有价值的参考。



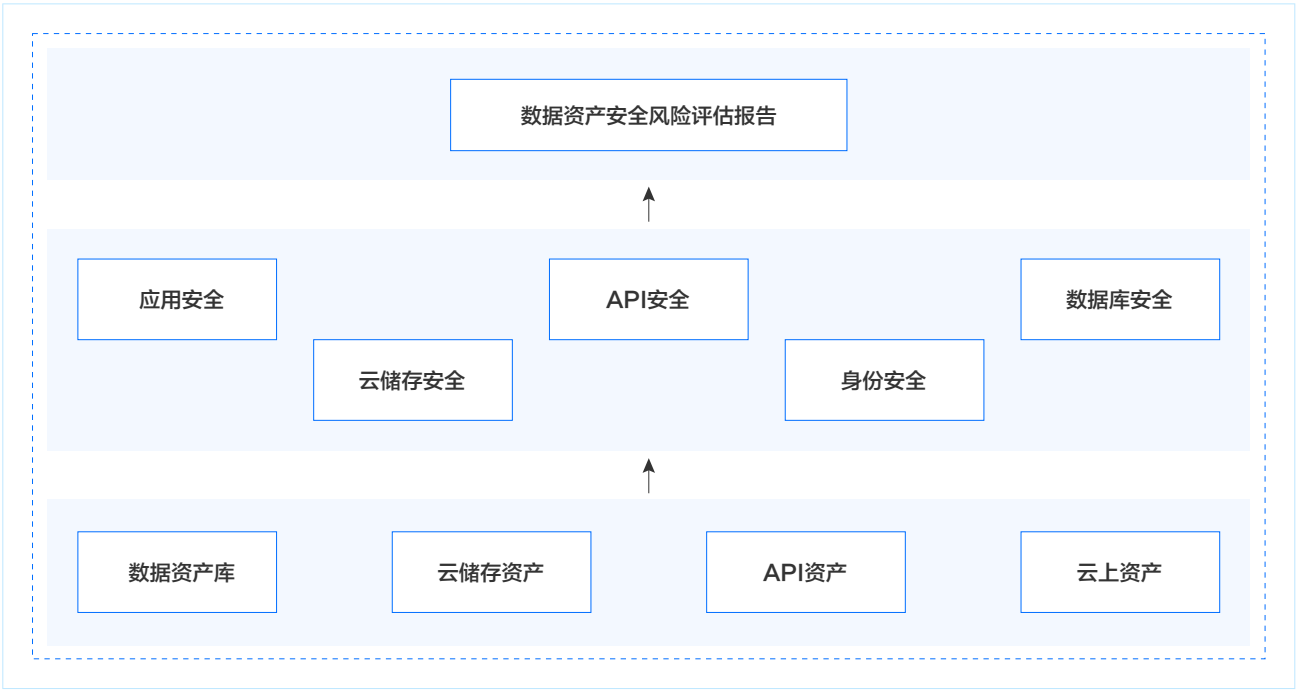
数据分级分类

根据国家、行业或企业自身的分类分级指南，对云上数据资产进行自动分类分级及人工打标，按照《数据安全法》要求，为数据进行分类分级保护建立基础。



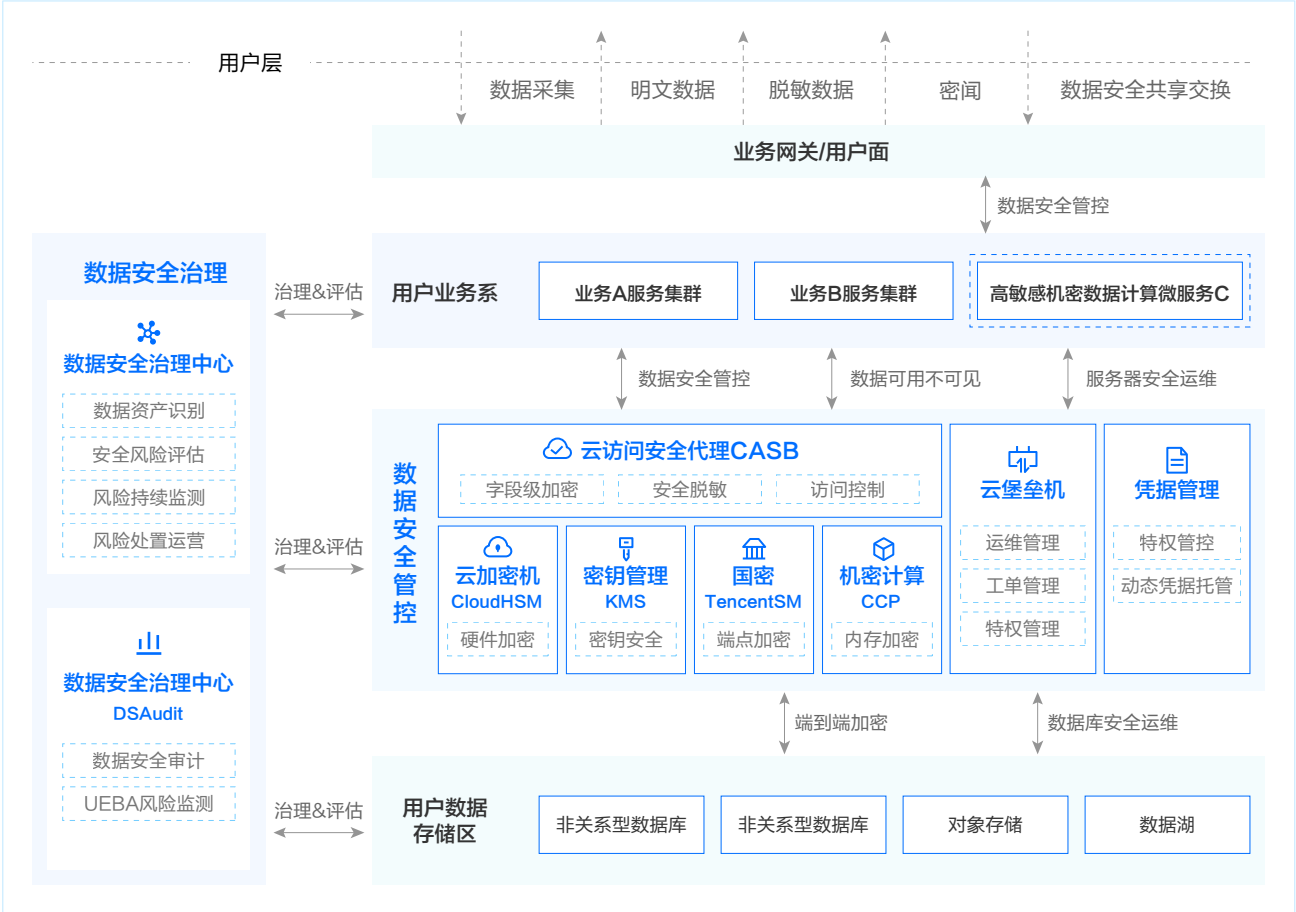
数据安全风险评估

数据安全风险是评估涵盖应用安全、数据库安全、身份安全、云存储安全、API安全等多方面综合性风险评估。通过系统地检测、识别、分析云环境中的潜在风险，帮助企业了解当前的数据安全基线状况，并制定相应的安全策略和措施，以确保业务的安全运行。



- **安全能力协同**

数据安全治理中心协同腾讯云上各类数据安全能力，帮助企业确保数据安全法律及行业合规标准的管理要求得到有效落实，为企业提供体系化的数据安全服务。

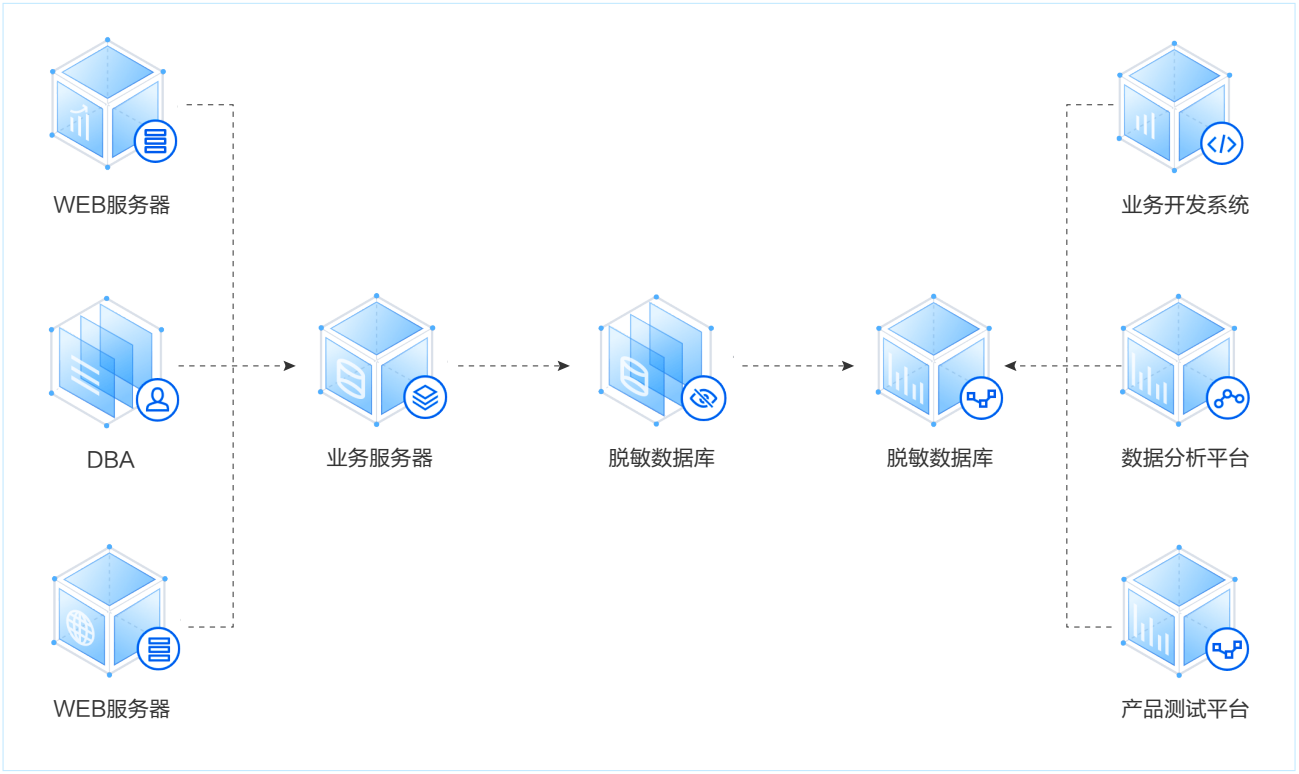


数据脱敏

腾讯云数据脱敏（Data Masking，DMask）是一款敏感数据脱敏与水印标记工具，可对数据系统中的敏感信息进行脱敏处理并在泄漏时提供追溯依据，为企业数据共享、迁移、分发提供安全保护措施。在内部数据迁移的场景和外部数据共享场景中，数据脱敏是一项非常重要的能力。

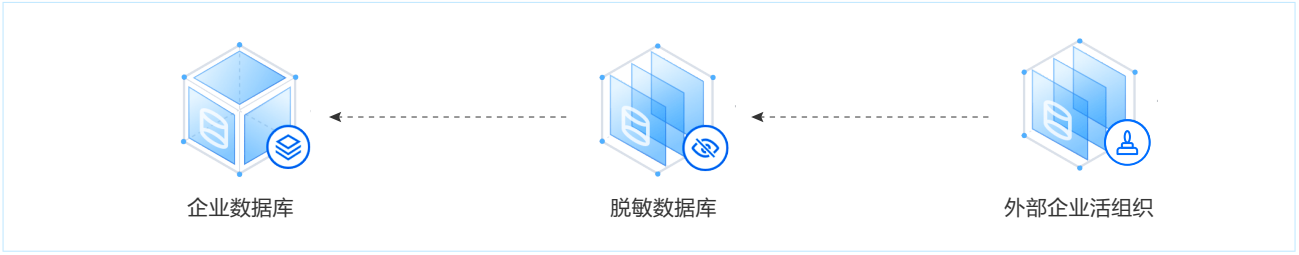
内部数据迁移

研发、测试、数据分析环境中，内部人员并不需要使用完全真实的数据，仅需要数据格式与生产环境一致即可。此时，如果数据不经处理，会产生数据泄漏的风险。内部人员如果因为一己私利倒卖关键数据，将对企业造成不可估量的损失。数据脱敏帮助企业在数据中生产环境向研发、测试、数据分析环境等迁移过程中，对数据进行脱敏处理，杜绝内部泄密。内部数据迁移场景下数据脱敏方案如下：



外部数据共享

当企业出于科研、商业合作等目的，需要向外部的企业或组织共享数据时，基于保护企业产权或用户隐私的需求，往往要对数据进行一定的变换，数据脱敏帮助企业实现数据共享脱敏，既能达到合作目的，又不会造成核心数据泄漏。



5.3.2 数据权限管理

云上的精细化权限管理与数据合规紧密相关，它的目标是确保数据安全和符合法规要求。精细化权限管理确保只有授权用户才能访问敏感数据，从而减少数据泄露的风险。许多数据保护法规（如GDPR、HIPAA等）要求企业实施适当的技术和管理措施来保护个人数据。精细化权限管理是满足这些要求的关键措施之一。

此外，合规性通常要求遵循最小权限原则，即用户仅拥有完成其工作所必需的最小访问权限。这有助于减少数据滥用和泄露的风险。同时精细化权限管理允许企业更好地监控和审计用户对数据的访问和操作，这对于合规性证明和风险管理至关重要。最后，合规性要求企业根据数据的敏感性实施不同级别的保护措施。精细化权限管理可以根据数据分类来设置相应的访问控制。

从技术手段上来说，云上的精细化权限控制一是体现在人员与账号体系的搭建与治理上，二是对云产品与云资源的访问设置上，三是对数据的细粒度访问控制上。以下分别说明。

访问管理

访问管理（Cloud Access Management，CAM）可以帮助客户安全、便捷地管理对腾讯云服务和资源的访问。您可以使用CAM创建子用户、用户组和角色，并通过策略控制其访问范围。CAM支持用户和角色SSO能力，客户可以根据具体管理场景针对性设置企业内用户和腾讯云的互通能力。

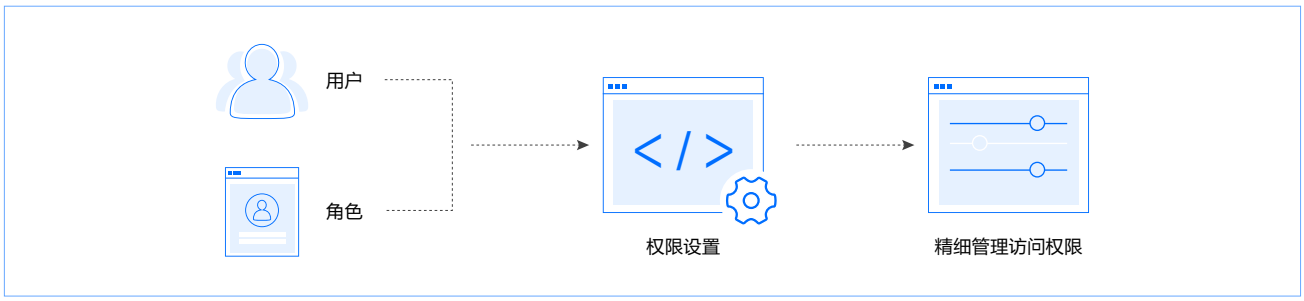
CAM是腾讯云进行权限管理的基石性组件，它具有如下场景化能力：

- **管理访问权限：**

  用户不必通过分享主账号相关的身份凭证，即可通过简单的授权给其他人员访问主账号资源。例如可以给主账号添加多个子账号给不同的员工使用，实现安全管理腾讯云账户下的资源。

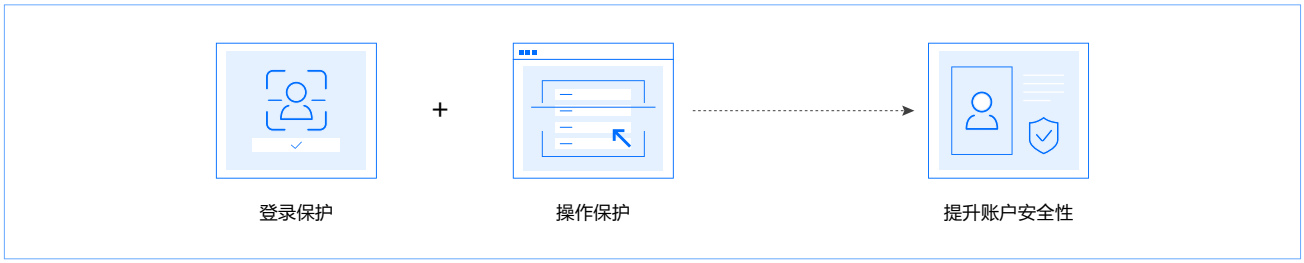
- **授予精细权限：**

  用户可以针对不同的资源给不同的人员授予特定的权限。例如可以允许某些子账号拥有某个 COS 存储桶的读权限，而另外一些子账号或者根账号可以拥有某个 COS 存储对象的写权限等。



- **二次身份校验：**

  可以为主账号和所属子账号开启二次身份校验以提升账号安全。借助二次身份校验，用户在进行登录或者敏感操作前，不仅必须提供使用账户所需的密码或访问密钥，还必须提供来自经过特殊配置的设备的代码。



- **联合身份校验：**

通过访问管理使用企业现有的身份验证系统（例如，在企业网络中或通过Internet身份提供商）获得密码的用户，获取对企业腾讯云账户的临时访问权限。



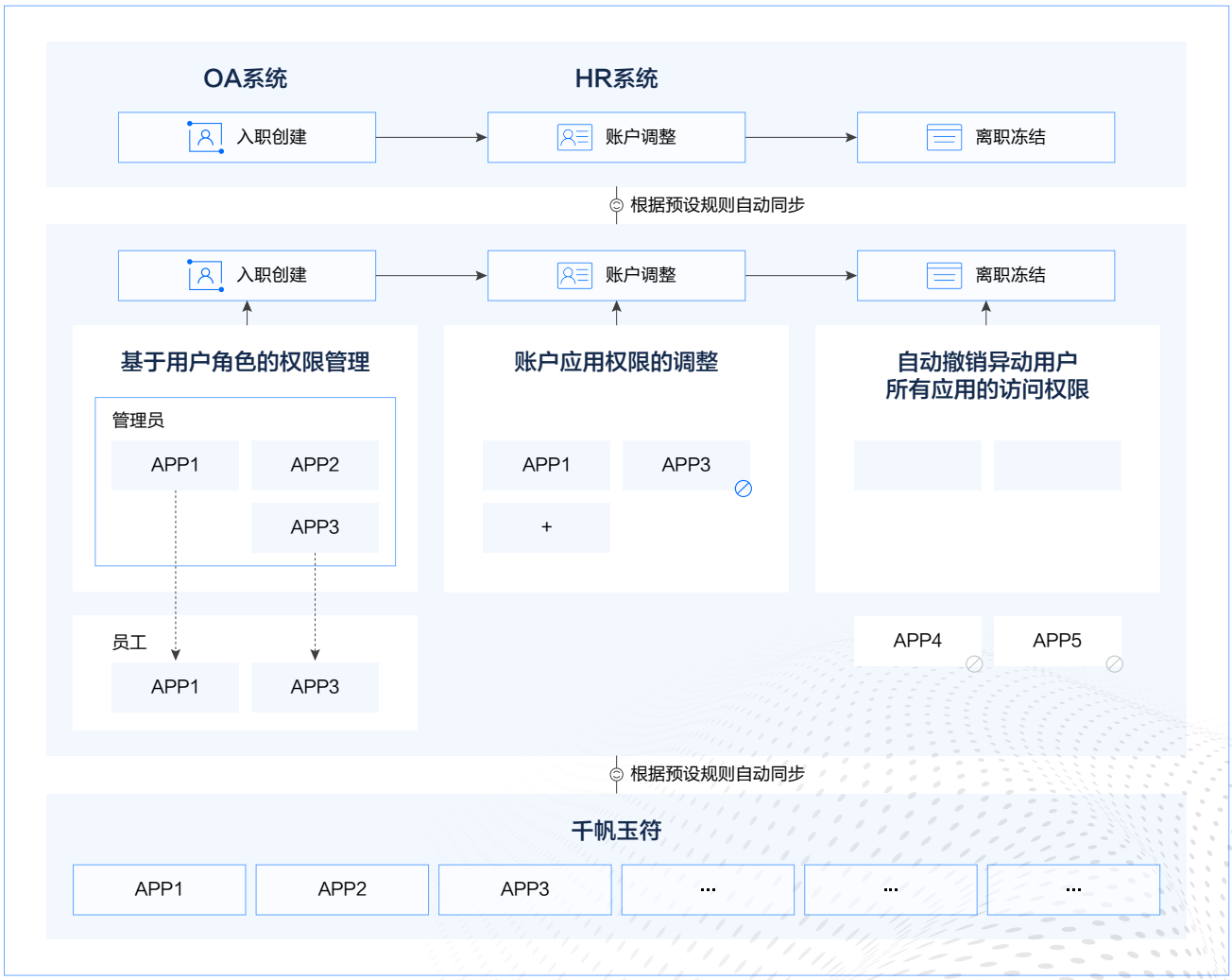
- **PCI DSS合规性：**

访问管理支持由商家或服务提供商处理、存储和传输信用卡数据，而且已经验证符合支付卡行业（PCI）数据安全标准（DSS）。是目前全球范围唯一且最为权威的支付卡产业数据安全标准。

账号与身份管理最佳实践

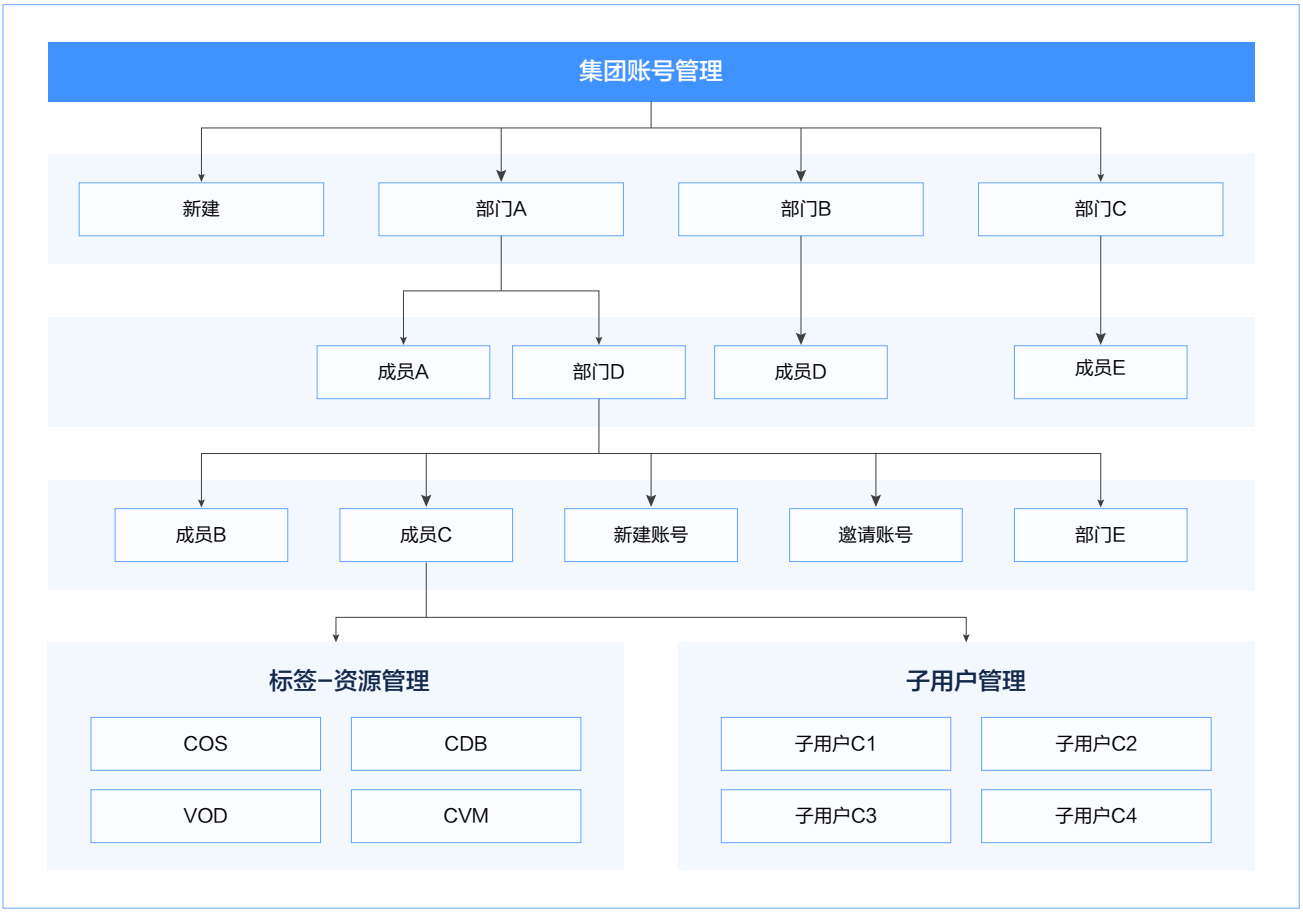
- **身份认证和数据管理服务**

腾讯云账号连接器（TencentCloud IDaaS）作为新一代企业身份连接平台，可针对多身份源进行数据清洗和数据聚合，适配复杂多样的企业既有应用和认证系统，实现企业应用身份的打通和连接。IDaaS可以同步各个系统中人员的身份信息，管理员可以通过预设规则，根据人员身份信息的不同，灵活的自动分配应用的使用权限范围。



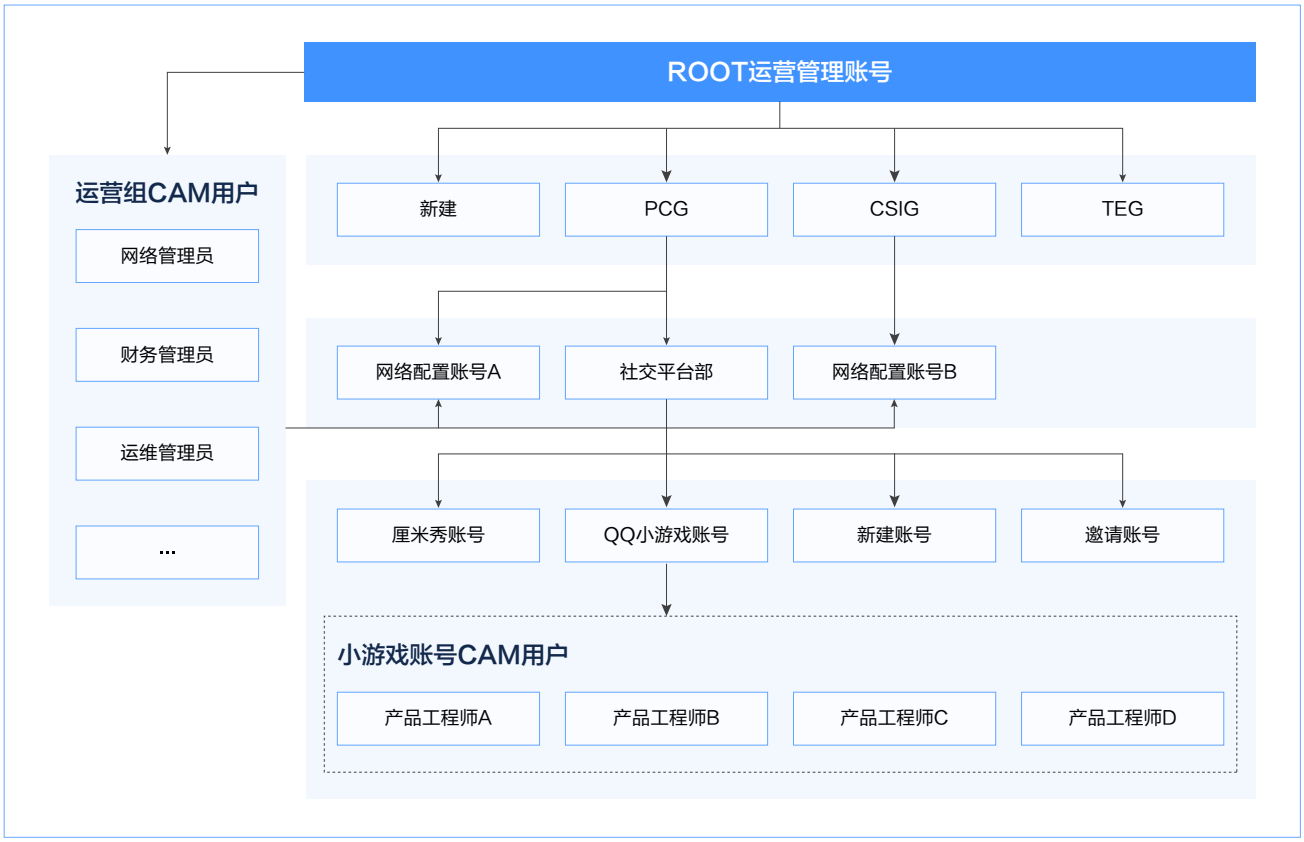
- **集团账号管理**

集团管理员可以在腾讯云上建立集团组织，并根据管理的需要创建最多五级的部门，通过邀请或创建的方式将集团的云账号统一加入部门中管理起来。并根据部门关系，实现对所有账号的财务管理、合规审计等。



- **访问控制与身份管理**

企业在云上按照产品或项目纬度对产品进行分类管理，并根据资源操作者的需求，授予相应操作权限，来实现资源的访问控制。通过访问管理产品，企业可以按照岗位职责创建用户组，并授予相应操作权限，如运维组、财务组等，并将相应子用户加入组中获取权限；同时企业也可以通过标签来分类和标识资源，并按照标签创建授权策略授予相应的子用户。



- **企业目录单点登录**

客户已具有腾讯云外部身份，并且需要访问腾讯云资源。可通过访问管理使用客户现有的身份验证体系向员工以及服务提供腾讯云服务和资源的访问权限。腾讯云支持基于 SAML 2.0（Security Assertion Markup Language 2.0）的联合身份验证来实现与企业内网账号的互通。



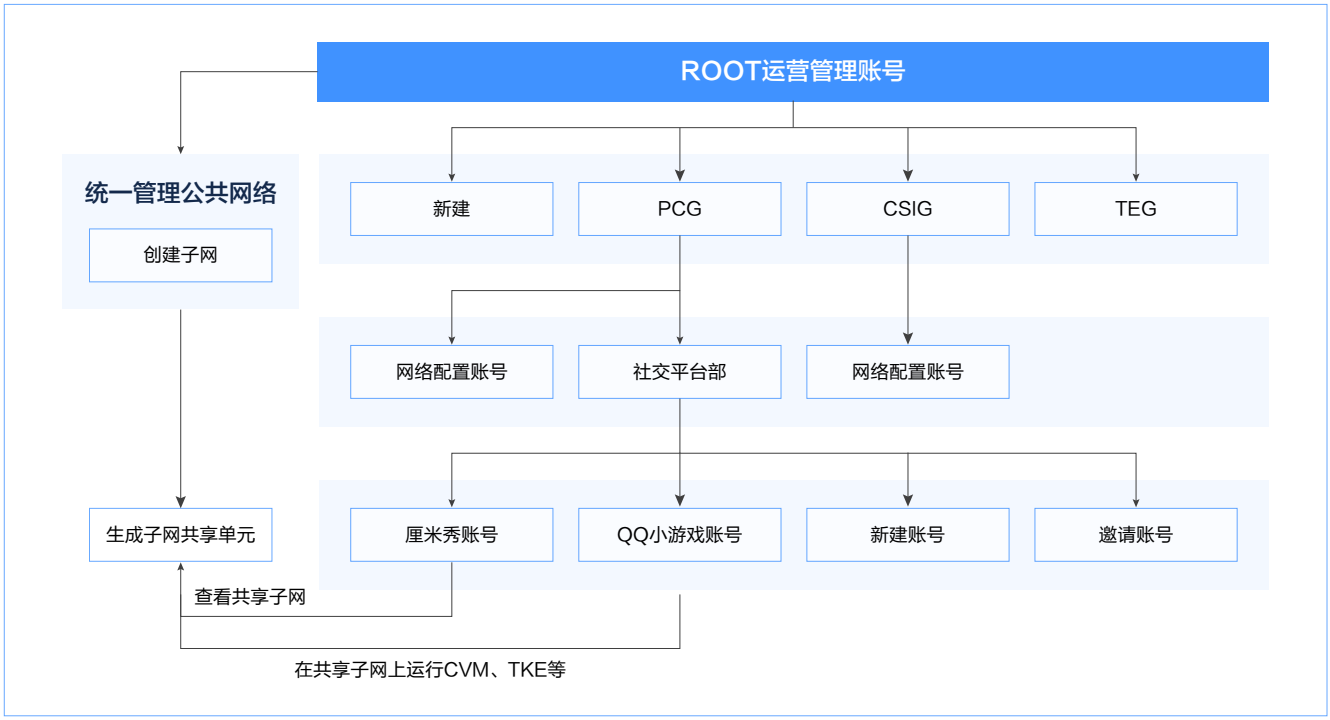
- **账号安全**

需要给子用户提供在用户名和密码之外再额外增加的一层保护。支持3种校验方式：微信扫码校验、MFA设备校验（分为硬件 MFA 设备校验和虚拟MFA设备校验）、手机验证码校验。根据设置状态，可能需要在登录和进行敏感操作前，进行微信扫码或者提供有效的六位安全码来证实身份和环境安全可靠。

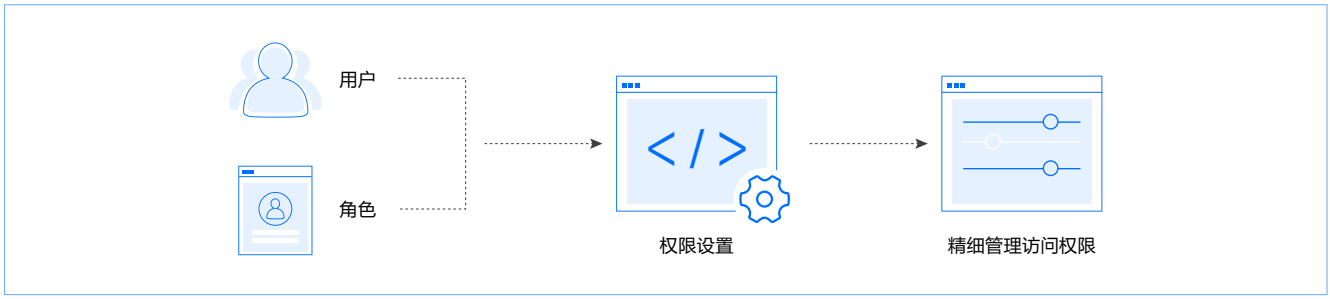


云资源访问管理最佳实践

集团统一管控公共资源，但是成员可以申请访问。集团管理员可以在集团账号管理中，创建资源共享单元，将子网等资源共享给指定成员使用。 成员在产品列表中可以查看和使用被共享的资源，如将 CVM 运行在被共享的子网中。



当集团账号和子用户的账号体系搭建完成后，需要给子用户分配资源管理权限。用户可以在访问管理中创建用户或角色，为其分配单独的安全证书（控制台登录密码、云API密钥等）或请求临时安全证书，供其访问腾讯云资源。用户可以管理权限，以控制用户和角色具体可以执行哪些操作和访问哪些资源。



数据的精细化授权管理

数据的精细化授权主要是指大数据平台与数据库系统中的精细化授权访问。大数据系统的精细化授权主要依靠WeData来实现，详情请参考5.3.6节“大数据与数据库”的内容。

至于数据库中的数据精细化授权管理，主流的数据库都有一套自己的账号与权限管理体系，借助这套账号权限管理体系，可以实现数据的精细化授权与管理。

- 在数据库中，可以通过各不同数据库的管理界面，创建、管理数据库的账号与权限，详情请参考：https://cloud.tencent.com/document/product/1003/62737
- 通过API接口可是比较方便地实现批量授权：https://cloud.tencent.com/document/product/1003/70113
- 数据的授权可以精细化到数据库的库、表级，通过API做如此设置请参考链接：TDSQL-C MySQL 版 修改账号库表权限-API 文档-文档中心-腾讯云

此外也可以使用DMC（Data Management Center）来统一对接所有的数据库系统进行数据的精细化授权，详情请参考5.3.5节“数据库”的内容。

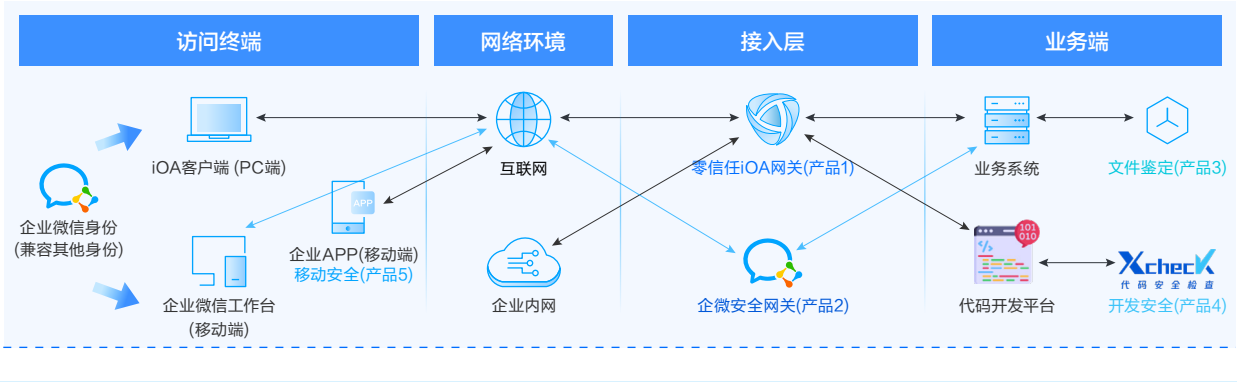
零信任方案

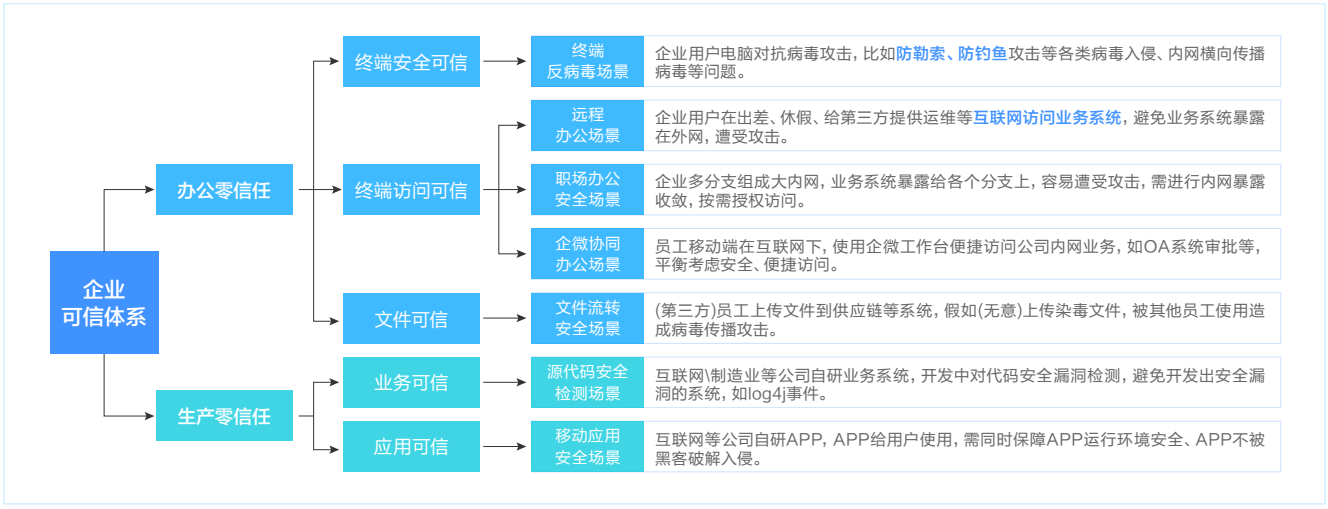
零信任（Zero Trust）是一种网络安全模型，它是对传统网络安全方法的一种新的思路和方法。它的核心思想是：

- **不信任任何实体：**零信任模型不再将内部网络视为"可信"区域，而是对所有实体(用户、设备、应用等)都采取"不信任"的态度。
- **持续验证和访问控制：**在每次访问时，都需要对用户、设备、应用等进行严格的身份认证和授权，而不是采取传统的基于网络位置的信任模型。
- **细粒度的访问控制：**零信任采用基于属性的动态访问控制，根据用户、设备、应用等多方面因素来灵活控制访问权限。
- **安全性贯穿全局：**零信任的安全防护不仅仅局限于网络边界，而是贯穿于整个IT架构的各个层面。
- **持续监控和响应：**零信任模型需要持续监控和分析各种安全事件，并根据实时情报采取相应的安全应对措施。

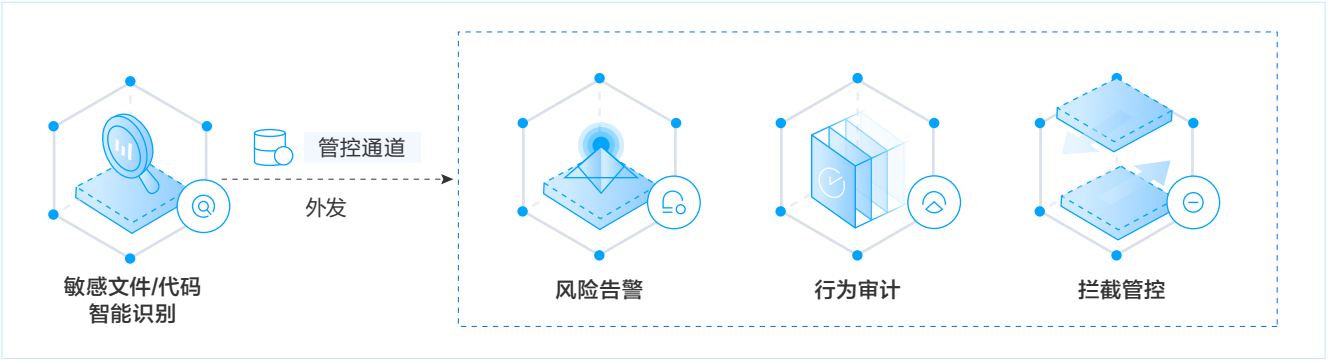
由此可以看出，零信任方案是通过数据访问的持续验证/授权，以及细粒度的访问权限控制，来保证数据访问的安全性和合规性的。它不仅能够加固外网访问的安全合规性，防止黑客用社会工程学等手段窃取用户数据；也能强化内网的安全合规性，防止类似删库跑路或内部人员监守自盗等行为。监管机构在检查企业数据合规的能力水平时，也越来越重视企业内网环境的数据安全与数据合规。

基于上述认知，腾讯云推出腾讯iOA零信任安全管理系统（Zero Trust Security Management）。它是根据腾讯自身无边界零信任企业网的最佳实践，所推出的新一代办公安全解决方案。基于可信终端、可信身份、可信应用、可信链路等核心能力，实现终端在任意网络环境中安全、稳定、高效地访问企业资源及数据。

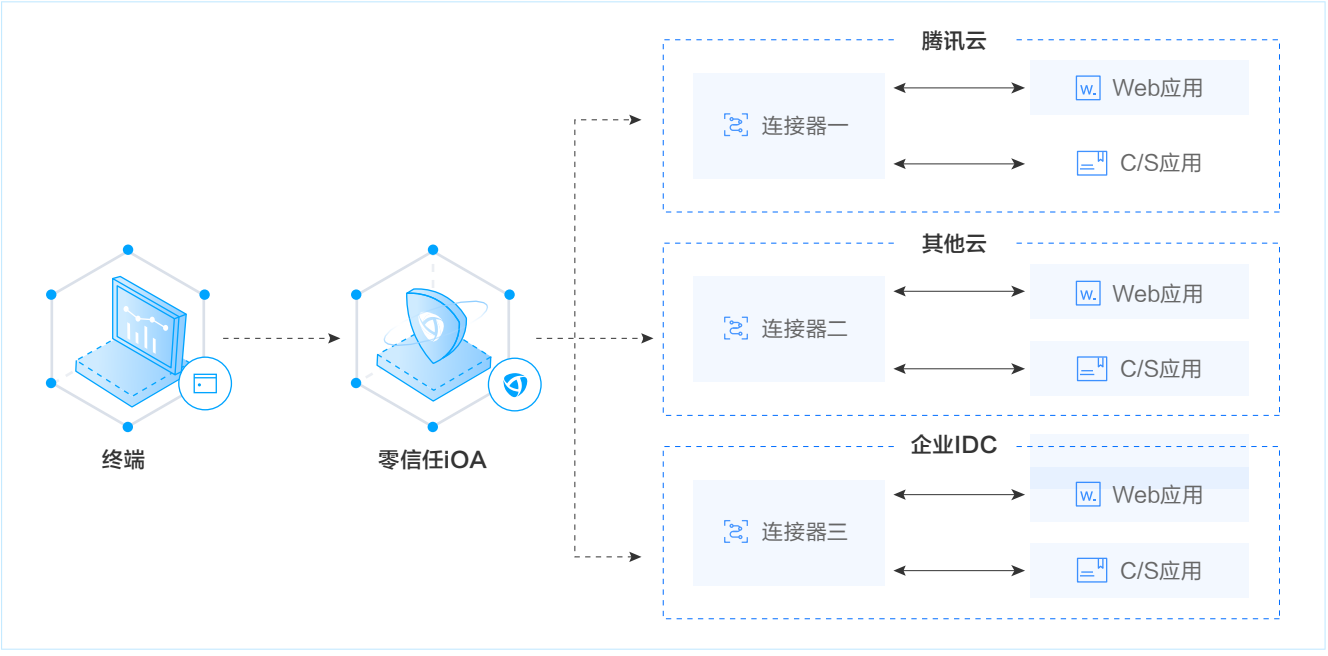




如上图所示，iOA可以对接企业身份（企微身份或其他），打造终端到业务端“泛办公安全”的零信任解决方案，塑造企业可信体系。举例来说，iOA内置企业常见敏感数据识别规则库，分级分类精细化管控，帮助企业建立数据资产地图，对IM、邮箱、网盘、远控、笔记、文件传输工具等文件外发行为进行审计和拦截，防止敏感数据泄漏。



另举一场景，如云上业务安全访问。公司业务上云或迁移之后需基于云服务的方式进行安全建设。面临IDC机房新增与裁撤等场景时，传统私有化交付方式缺乏灵活性，给企业IT管理造成了额外的成本和消耗。使用iOA可有效防护云资产入侵威胁，收敛云资源暴露面，提供在互联网传输过程中的数据安全防护。



5.3.3 数据合规审计

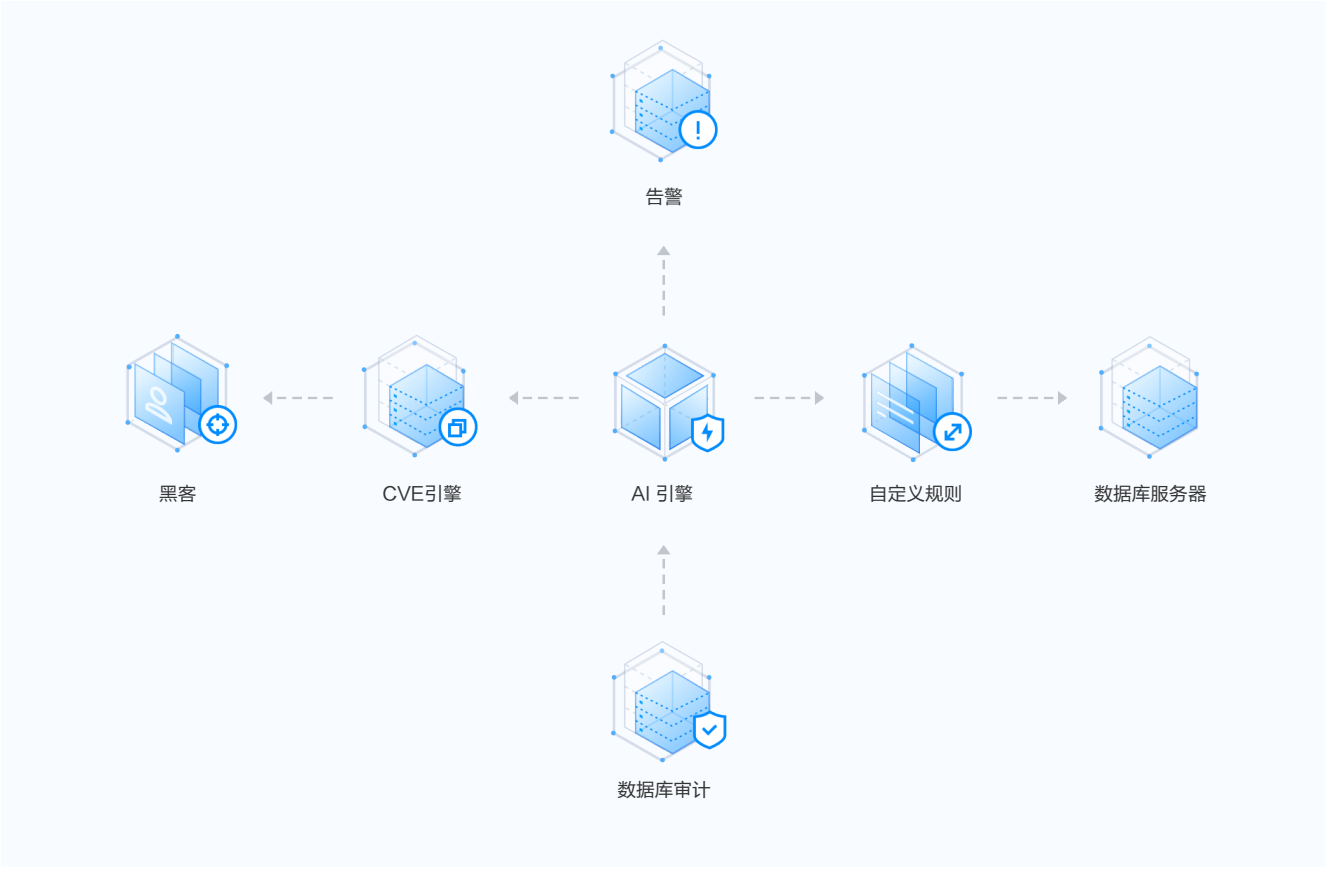
数据合规中的审计是一个关键环节，是一种监督性审计，它帮助确保企业数据处理活动遵守相关法律法规，包括定期自行审计和监管机构要求的强制审计两种形式 。企业进行数据合规审计有助于积极应对多头监管的局面，保证个人信息处理活动的合法性，并作为个人信息处理者无过错的有力证据，从而免除严苛的民事责任。

合规审计流程通常包含审计准备、审计实施、审计报告、问题整改、归档管理五个阶段。在数据合规审计领域，云厂商不仅要让客户能够对自己的业务数据进行追踪审计，也要支持客户自己在开发、运维、运营等日常经营中的过程数据的审计。这能够为客户提供充分的电子证据链，一是使客户在数据合规事件发生前能提前感知风险，发生时能及时止损，发生后能方便地找出根因；二是使客户能够自证清白，避免监管机构的处罚风险。企业可以使用腾讯云的数据安全审计、操作审计、日志审计、配置审计等产品、方案能力来快速高效地满足数据合规审计的要求。

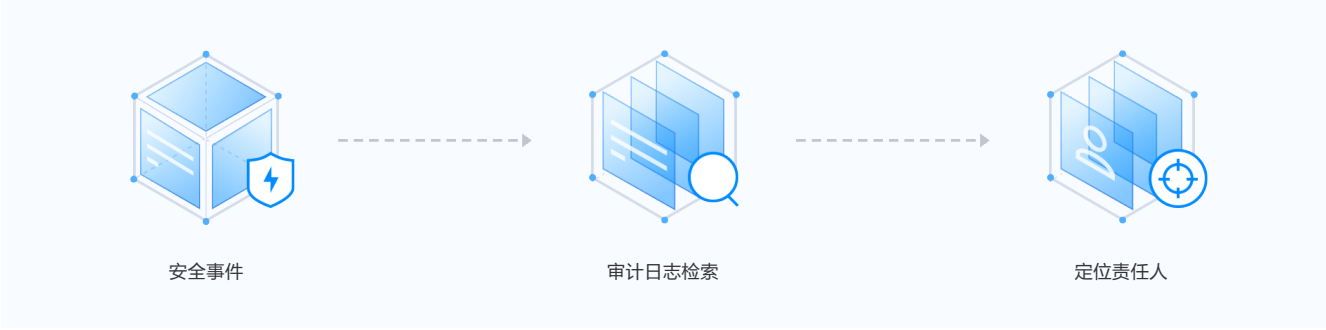
数据安全审计

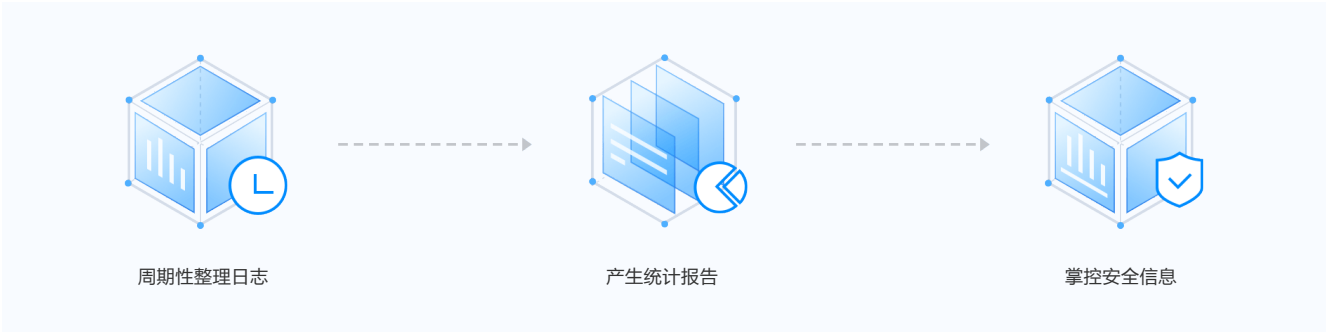
数据安全审计是指对一个组织的信息系统的管理、操作和控制进行系统性、独立的评估和验证，以确保信息系统的安全性、完整性、可靠性和合规性。对大部分企业来说，其信息系统的数据大都放在数据库中，因此对数据库进行安全审计就变得尤为重要。

腾讯云数据安全审计（Data Security Audit，DSAudit）是一款基于人工智能的数据库安全审计系统，可挖掘数据库运行过程中各类潜在风险和隐患，为数据库安全运行保驾护航。无论是自建数据库还是云数据库，都有可能面临来自内外网络的蓄意攻击，以及内部人员各类误操作导致的数据损失。当这些危险操作发生时，数据安全审计能够立刻检测出攻击源、攻击目标、攻击事件、操作的库表字段内容、所用语句等信息，并且及时产生告警，确保管理员第一时间能够掌控威胁信息，从容应对数据安全问题。同时，数据安全审计还能够将危险操作进行分类，按照影响范围、威胁程度分为高中低三级，让管理员在海量威胁告警中精准定位最紧急的事务，确保高威胁事件得到充分处理。



当出现数据被删除、信息被篡改、敏感信息泄漏等重大安全事件时，必须要进行全面的事件还原和严肃的追责处理。数据安全审计支持可扩充的SQL 语句存储，即便用户的数据库系统日常处于满负荷运转，也能存储指定时长的日志信息。通过对长时间跨度的历史信息进行深度检索，管理员能够清晰的将安全事件进行全貌还原，并对问题轻松溯源。此外当用户计划对全网安全信息进行周期性的统计时，数据安全审计能够提供强大的自定义报告功能，可对从全局概况到每个实例的具体信息进行自由定制，满足不同企业个性化的统计需求，提供详尽的分析依据。

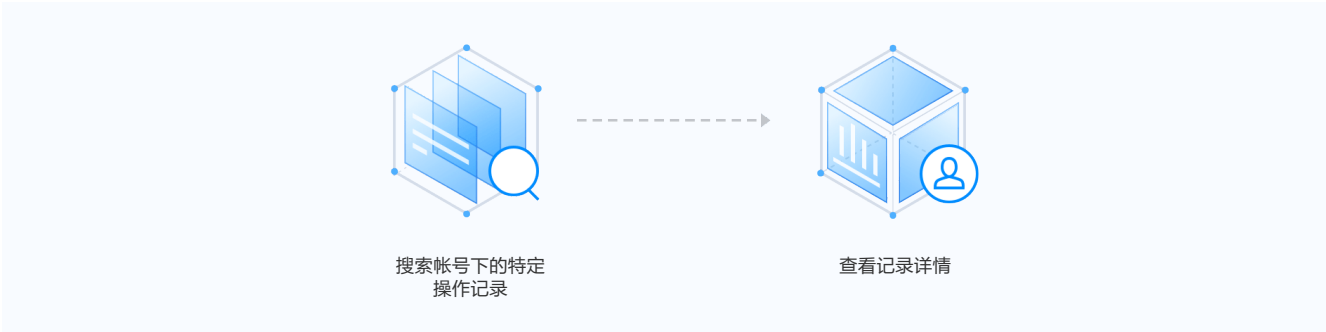




操作审计

操作审计也叫云审计，是指对云服务提供商的基础设施、平台、应用程序和服务进行的系统性审查和记录，以确保云服务的使用符合相关的政策、法规、标准和最佳实践。

CloudAudit是腾讯云操作审计的主要产品，它支持对客户腾讯云账号进行监管、合规性检查、操作审核和风险审核的服务。借助CloudAudit，用户可以记录日志、持续监控并保留与整个腾讯云基础设施中操作相关的账号活动。CloudAudit提供腾讯云账号活动的事件历史记录，这些活动包括通过腾讯云管理控制台、API服务、命令行工具和其他腾讯云服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。操作审计Cloud　Audit记录最近30天的腾讯云账号下的API或腾讯云控制台上的所有操作记录列表。用户可以搜索具体的操作记录详情，查看记录详情，包括访问密钥、区域、错误码、事件ID、事件名称、事件源、事件时间、请求ID、源IP地址、用户名。





借助跟踪集功能，用户可以将账号下发生的所有活动信息持久化存储到COS，从而简化日后可能进行的合规性审核。当然用户也可以将活动信息实时存储到日志服务，利用日志服务便利强大的功能做实时或准实时合规审计。

日志审计

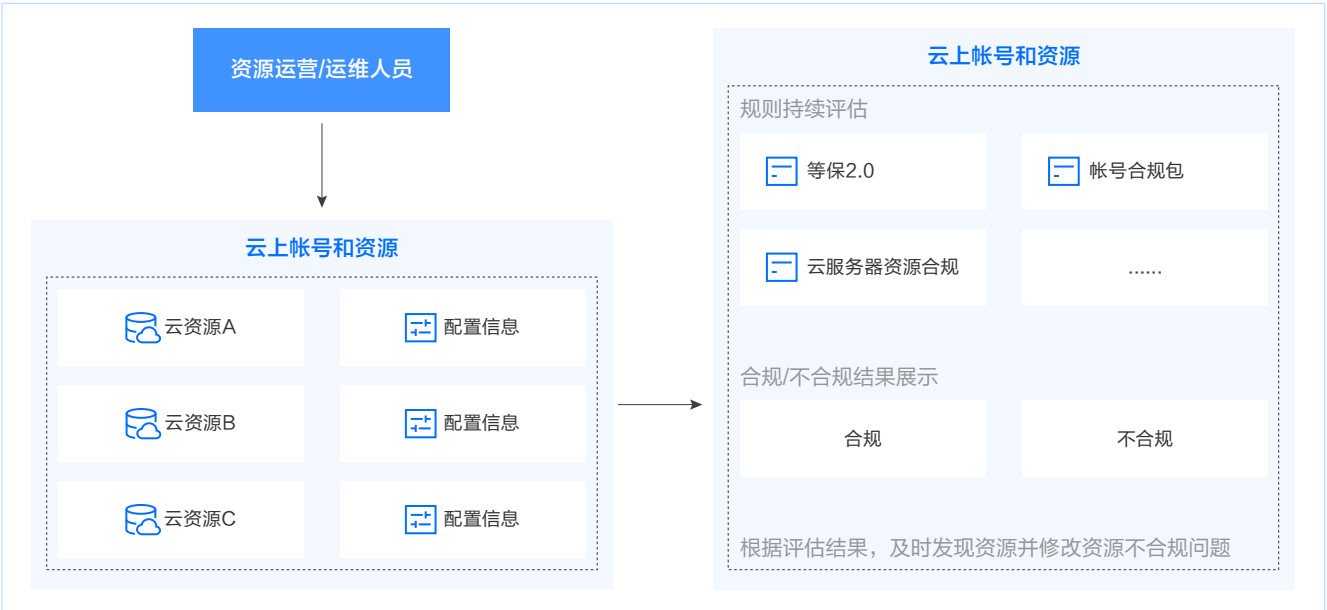
日志审计是指对信息系统、应用程序和网络设备的日志记录进行审查和分析的过程。这些日志记录了系统活动、用户行为、事件和配置更改等信息。由于日志信息在用途、性质和结构上与一般数据有显著的区别，因此最好的做法是使用专门的用于记录分析日志信息的产品来提供日志审计功能。我们可以使用腾讯云强大的日志服务产品来实现日志审计功能。

日志服务（Cloud Log Service，CLS）是腾讯云提供的一站式日志服务平台，提供了从日志采集、日志存储到日志检索、图表分析、监控告警、日志投递等多项服务，可以协助用户通过日志来解决业务日志审计的场景问题。通过日志服务的 Agent 收集日志到日志服务，通过日志查询能力，快速分析其访问行为，例如某个账号、某个对象的操作记录等，判断是否存在违规操作，通过日志投递对象存储 COS 还可以对日志数据进行长时间存储满足合规审计需求。



配置审计

配置审计（Config）帮助用户集中审计和治理云资源。它可持续记录和评估分散在用户账号下各地域、各类云资源的配置信息和变更操作，帮助用户高效实现资源自主监管和规范运维。在开启资源监控后，配置审计会自动发现云资源并记录配置信息，并在配置发生变化时记录变更后的配置快照。若用户同时启用了官方的托管规则，配置审计会根据规则持续评估对应的资源配置，帮助用户在运维过程中及时发现违规资源。企业云上 IT 管理存在各种各样的管理规范，配置审计提供基于腾讯云最佳实践的合规规则和合规包，对企业账号下的云资源配置自动执行持续的合规评估，帮助企业及时治理云资源，高效实现资源自主监管。



在上图的规则持续评估中，用户可以根据自己的业务场景自己创建规则模板，同时腾讯云也会不断丰富规则模板库，以供用户方便使用。

其他审计相关能力

除了上述经常用到的审计相关产品能力，腾讯云还提供了其他诸多合规审计产品能力，如：

- **堡垒机**：腾讯云堡垒机（Bastion Host，BH）可为您的 IT 资产提供代理访问以及智能操作审计服务，为客户构建一套完善的事前预防、事中监控、事后审计安全管理体系。
  https://www.tencentcloud.com/zh/products/bh
- **数据库管理（DMC）**：DMC 提供可视化的库管理、实例会话管理、SQL 窗口、SQL 安全审计、SQL 变更审批、实时监控、操作审计等数据库管理能力，集成诊断优化和数据可视化分析能力，从而简化和规范数据库管理操作、降低数据库运维门槛。
  https://www.tencentcloud.com/zh/products/dmc
- **容器服务审计**：容器服务 TKE 为用户提供了开箱即用的审计仪表盘。在集群开启集群审计功能后，TKE 将自动为该集群配置审计总览、节点操作总览、K8S 对象操作概览、聚合检索仪表盘。还支持用户自定义配置过滤项，同时内置 CLS 的全局检索，方便用户观测和检索各类集群操作，以便于及时发现和定位问题。
  https://www.tencentcloud.com/zh/document/product/457/38890?lang=zh

5.3.4 可信计算

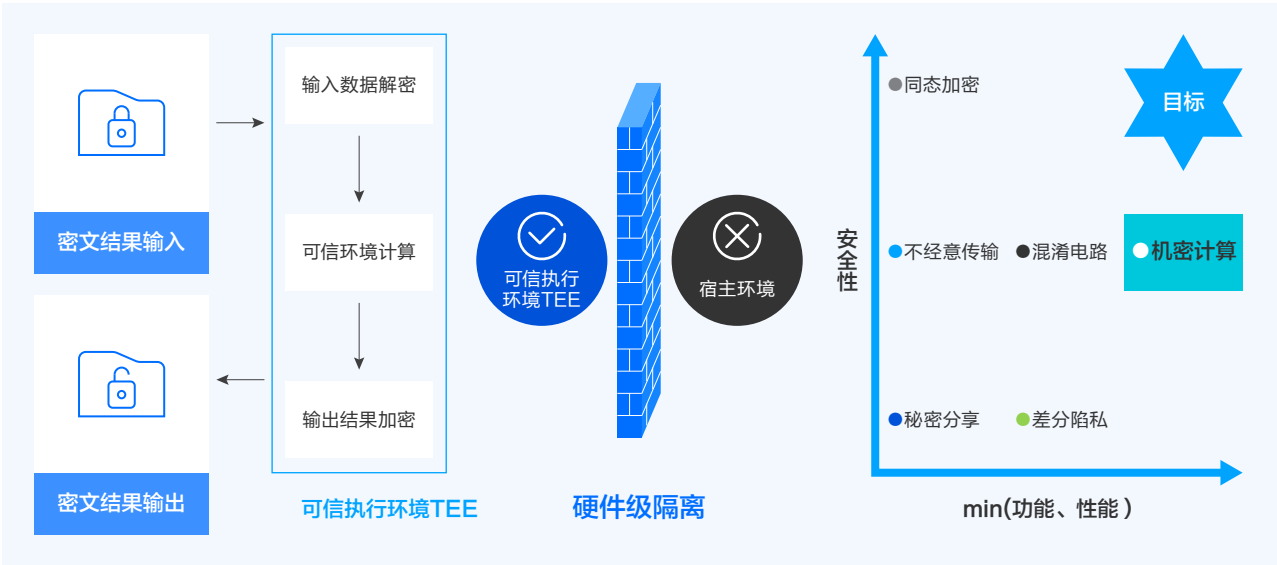
可信计算（Trusted Computing）是一种安全概念，旨在创建一个安全的计算环境，确保计算机系统、设备和网络的安全性和可靠性。它通常包括硬件安全、软件安全、系统完整性、身份验证和授权、数据保护、安全审计和监控等维度。在数据合规中，可信计算可以用来增强数据安全性，通过加密和安全存储，保护个人数据不被未授权访问和泄露，帮助组织遵守数据保护法规，如GDPR、CCPA等。这些法规要求采取适当的技术和管理措施来保护个人数据。此外，它也能使企业支持数据主体权利，帮助组织响应数据主体的查询、更正、删除等权利请求，符合数据保护法规的要求。

总之，可信计算为数据合规提供了一个坚实的基础，帮助组织建立安全、可靠和符合法规要求的数据处理环境。

腾讯云的可信计算有两个概念，一是指某些云主机规格由于符合国际的某些安全可信标准、提供了内核与代码层的加解密能力、具备较强的权限管控级别而成为“可信计算环境；二是指依靠区块链技术实现的可信计算服务。

可信计算环境

可信计算环境也叫可信执行环境，可信执行环境技术（ TEE ）提供了可行的技术支持，其核心思想是以可信硬件为载体，提供硬件级强安全隔离和通用计算环境，数据仅在隔离的安全区“飞地”（ Enclave ）内才进行解密并计算，数据在离开“飞地”（ Enclave ）之前会被自动加密，离开“飞地”（ Enclave ）后无法接触数据明文内容。



在可信计算环境中数据都是加密进行处理的，目前提供 TLS 协议加密及数据库表应用层加密两种方式。 TLS 协议加密是在可信计算节点与数据库服务间建立 TLS 安全信道，数据不会再进行应用层加密，数据源提供方和计算结果使用方无需额外操作，但要求数据库在数据源提供方和计算结果使用方中维护。数据库表应用层加密是数据源和计算结果数据本身会在TEE集群里进行解密和加密，在网络上传输的是密文数据，拥有更高的安全性，也支持数据源提供方、计算结果使用方使用第三方维护的数据库。

可信计算服务

腾讯云区块链可信计算服务将区块链技术与可信执行环境（TEE）相结合，提供用户数据权属确认、数据安全计算及数据可信共享服务，实现用户数据端到端的机密性和完整性，促进数据价值安全流转，实现跨地域、跨机构、跨应用间的数据可信融合与协同，满足用户多场景数据安全应用诉求。可信计算服务有以下典型应用场景。

- **政府数据协同共治**

  在充分保障数据隐私安全的前提下，实现在不同政府委办局之间数据可信安全共享，区块链可信计算服务应用于身份信息管理领域，确保原始信息安全可信；应用于政务信息管理领域，促进信息开放共享；应用于政府统计调查领域，确保数据可信、可追溯；应用于业务监查领域，协助政务数据溯源监查，满足多主体参与、多个流程和环节的共同治理过程，为构建政府数据协同共治提供技术支撑，帮助政府业务高效协同。
- **金融联合风控**

  随着数字经济发展，金融业务不断丰富，面临客户留存数据无法满足金融风控的问题，需引入外部数据进行补充。为满足数据安全保护要求，各机构间数据融合壁垒高，交互难度大。区块链可信计算服务可在多方不共享原始数据的前提下，融合多方特征确认共有的交集用户，对共有样本数据进行安全计算，解决单个金融机构数据量有限的问题。在信息核验时，通过黑名单数据共享，对其作恶行为进行匿踪查询，提升信息查询的安全可信度，在满足数据隐私保护的基础上实现金融联合风控。
- **医疗风险评估**

  在医疗领域，数据重要性高、隐私性强且分散在各个机构，数据使用和管理难度大。区块链可信计算服务可通过构建多方协同的可信环境，将数据所有者、数据提供方、数据使用者以及系统维护者等各方联合起来，实现数据的高效流通和安全共享，保险机构可联合多方进行合理的数据共享，有效地发现和排除保险欺诈，提高风险评估效率及准确性。
- **数据价值流通**

  当前，各行各业的信息化系统中，普遍存在着应用“烟囱”和数据孤岛现象，各类企业对数据流通顾虑重重，造成数据的重复采集、冗余开发和信息不完整等问题。数据即资产，既要保证数据的高安全可信，又要通过数据流通创造要素价值。区块链可信计算服务构建可信数据价值链接器，各方可把自己的数据在自己的信任域中进行可信计算，再将结果加密汇聚起来进行整合计算，实现“数据可用不可见，数据不动价值移动”。

5.3.5 数据库

数据库是企业核心数据资产的主要载体，能够提供数据的存储、管理和访问能力。作为企业核心数据资产的存储和管理平台，其合规性直接关系到企业数据合规性。只有确保数据库本身的合规性，才能保证企业数据使用的合规。数据库对数据合规的作用体现在这样几个方面：

- **访问控制与权限管理**：中国政府的政策推动是中国企业走向海外市场的重要动力。中国实施的“双循环”战略需要加强对外循环，促进更多中国企业在海外市场扎根发展。政府推出了一系列支持企业海外投资的政策和措施，为企业拓展全球业务提供了支持和便利。

- **数据脱敏和加密**：数据库支持对敏感数据进行脱敏和加密处理，可以在数据存储和传输过程中保护数据安全。这有助于满足数据合规中对敏感数据的保护要求。

- **数据生命周期管理**：数据库可以提供数据备份、归档、删除等功能，支持对数据进行完整的生命周期管理。这可以满足数据合规中的数据保留、销毁等要求。

- **审计和监控**：数据库提供了丰富的审计日志记录功能，可以记录对数据的各种操作行为。这为数据合规中的审计和监控工作提供了重要的数据支撑。

数据库管理中心DMC

腾讯云主要依靠数据库管理（Database Management Center，DMC）来实现数据库中合规场景。DMC是一个高效，安全，可靠的数据库一站式管理平台。DMC能够纳管腾讯云平台上多款NoSQL或关系型数据库产品。



此外DMC还提供可视化的库管理、实例会话管理、SQL窗口、SQL安全审计、SQL 变更审批、实时监控、操作审计等数据库管理能力，集成诊断优化和数据可视化分析能力，从而简化和规范数据库管理操作、降低数据库运维门槛、提升运维效率。



数据库智能管家DBbrain

数据库智能管家（TencentDB for DBbrain，DBbrain）是腾讯云推出的一款为用户提供数据库性能、安全、管理等功能的数据库自治云服务。DBbrain利用机器学习、大数据手段、专家经验引擎快速复制资深数据库管理员的成熟经验，将大量传统人工的数据库运维工作智能化，服务于云上和云下企业，有效保障数据库服务的安全、稳定及高效运行。在数据合规场景下，DBbrain可以结合数据资产信息、敏感数据发现信息，对严重偏离模型或合规模式的用户、行为、数据进行告警和安全等级评估，帮助管理员发现恶意操作等问题，为用户数据库提供更为精准的安全威胁分析和合规治理建议，从而保障数据的安全性与合规性。



数据生命周期管理

一般数据库相对缺少在大数据平台中常见的数据生命周期管理的工具化功能。但是数据库中的数据生命周期管理也是必不可少的一环，可以依靠某些数据库的功能来组合实现数据生命周期管理。下面以MySQL为例来阐述。

TTL（Time to Live）是指数据在存储系统中的存活时间。在MySQL中，我们可以通过设TTL来控制数据的存活时间，当数据过期后，系统会自动删除该数据。这对于一些需要定期清理过期数据的应用场景非常有用，比如用户的登录状态、验证码、临时缓存、用户要求或根据合规要求需要删除的数据等。可以使用如下四种方式：

- **使用 EXPIRE_INFO 函数设置TTL**

```
CREATE TABLE my_table (
    id INT PRIMARY KEY,
    data VARCHAR(50),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

ALTER TABLE my_table
    ADD COLUMN expired_at TIMESTAMP DEFAULT (DATE_ADD(created_at, INTERVAL 1 DAY));

SELECT EXPIRE_INFO('my_table', 'expired_at');
```

这里我们创建了一个名为 my_table 的表，并添加了一个 expired_at 列用于存储数据的过期时间。之后使用 EXPIRE_INFO 函数来设置 TTL。

- **使用 ALTER TABLE 语句设置TTL**

```
ALTER TABLE my_table
    ADD COLUMN expired_at TIMESTAMP DEFAULT (DATE_ADD(created_at, INTERVAL 1 DAY)),
    ALGORITHM=INPLACE, LOCK=NONE;
```

这种方式也是添加一个 expired_at 列来存储过期时间，不过是直接在 ALTER TABLE 语句中完成。

- **使用 CREATE TABLE 语句设置TTL**

```
CREATE TABLE my_table (
    id INT PRIMARY KEY,
    data VARCHAR(50),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    expired_at TIMESTAMP DEFAULT (DATE_ADD(created_at, INTERVAL 1 DAY))
);
```

在创建表的时候就直接添加 expired_at 列来存储过期时间。

- **使用 MySQL 8.0 新增的 GENERATED COLUMN设置TTL**

```
CREATE TABLE my_table (
    id INT PRIMARY KEY,
    data VARCHAR(50),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    expired_at TIMESTAMP AS (DATE_ADD(created_at, INTERVAL 1 DAY)) STORED
);
```

这种方式使用 MySQL 8.0 新增的 GENERATED COLUMN 特性，将 expired_at 列定义为一个计算列，自动根据 created_at 列计算过期时间。

无论采取哪种方式，设置 TTL 的关键是添加一个用于存储数据过期时间的列。之后可以通过定期扫描这个列，删除已经过期的数据。

- **数据过期/到期判断**

通过比较当前时间和数据的创建时间加上有效期来判断数据是否过期。

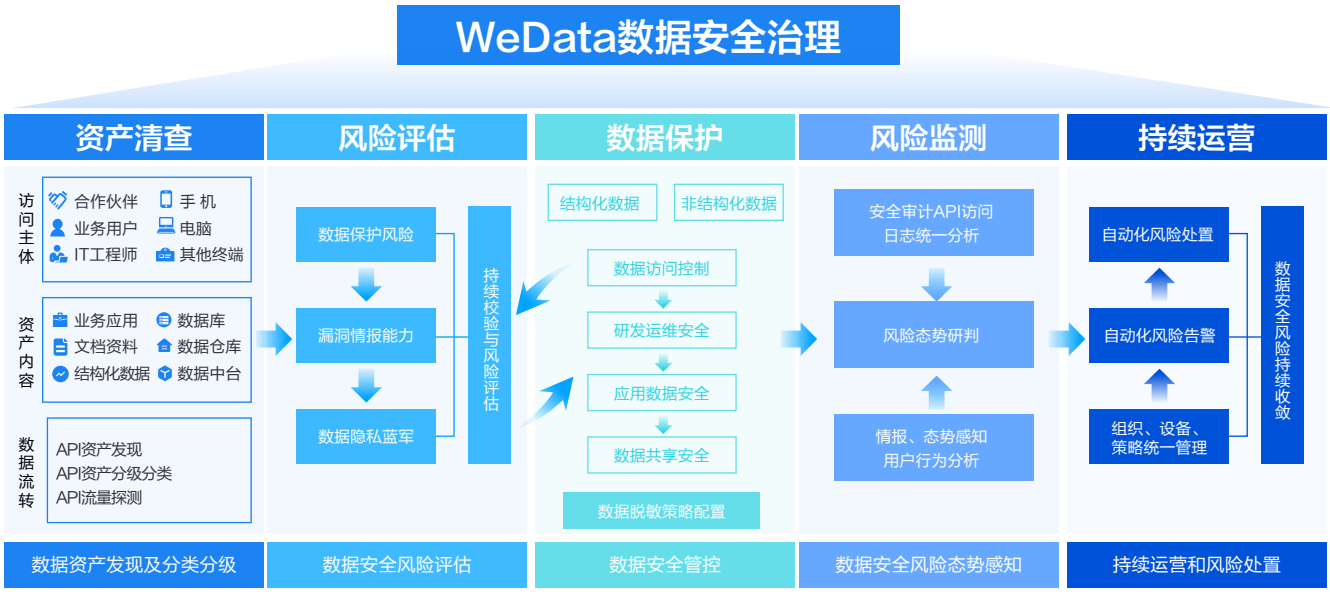
- **清理过期/到期数据**

定期清理过期数据（很多场景下也是规定存储时间到期的数据，必须要删除）是很重要的一步，清理存储空间降低成本是次要的，主要是可以降低合规风险。我们可以通过定时任务或者触发器来实现：

```
EVENT `clean_expired_data`
ON SCHEDULE EVERY 1 HOUR
DO
    DELETE FROM `my_table` WHERE `expire_time` < NOW();
```

5.3.6 大数据与数据湖

在大数据场景中，主要依靠腾讯云的WeData（数据开发治理平台　）产品来进行数据合规治理。WeData是位于云端的一站式数据开发治理平台，融合了包含数据集成、数据开发、任务运维的全链路DataOps数据开发能力，以及数据地图、数据质量、数据安全等一系列数据治理和运营能力，帮助企业在数据构建和应用的过程中实现降本增效，数据价值最大化。在数据合规领域，WeData可以提供一系列能力：



腾讯云WeData不仅支持传统的开源、托管以及腾讯云自研的大数据产品，也支持数据仓库与数据湖产品的数据合规治理。腾讯云数据湖计算DLC（Data Lake Compute）是基于Spark、Presto、Iceberg构建的云原生Serverless湖仓分析服务，具备存算分离、资源弹性、开箱即用、托管运维、自研内核增强等优势特性，灵活覆盖离线/近实时分析、交互式查询、跨源联邦分析、数据科学等大数据场景，助力企业敏捷构建一站式的数据分析平台。DLC先进的Lakehouse架构，全面覆盖湖场景（大模型数据预处理、数据科学）和仓场景（离线/近实时分析、交互式分析），满足企业大数据各类分析需求。

WeData在数据湖产品体系中的作用和位置如下图所示：



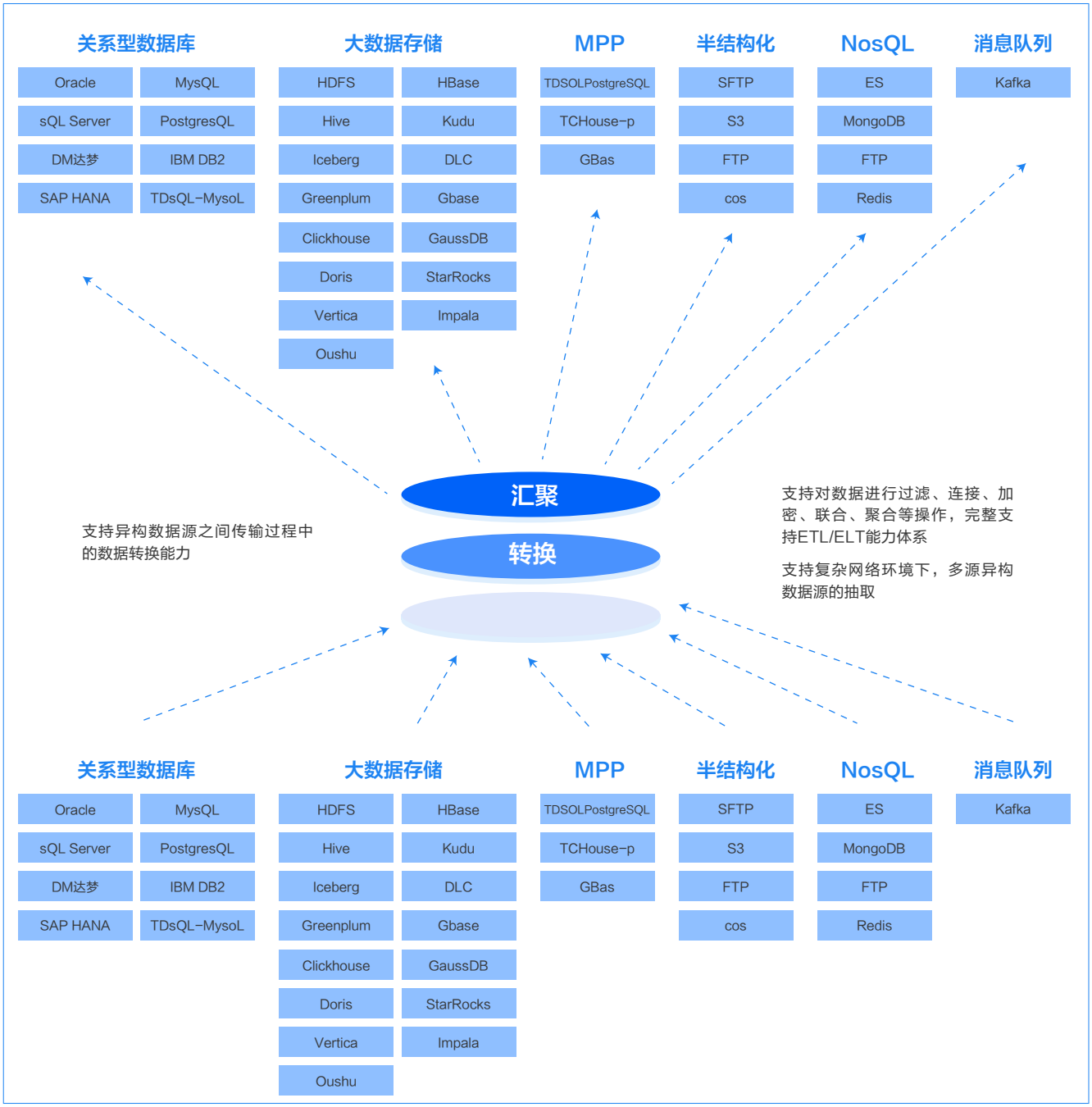
以下分别介绍WeData在数据合规中具体的应用场景。

资产管理与分级分类

WeData提供数据目录功能，可以对用户的数据资产进行统一管理，包括数据源、表结构、字段定义、数据质量等信息，方便用户了解数据资产的整体情况。它可以追踪数据的流向，从数据源到最终的应用，帮助用户了解数据的来源和去向，方便您进行数据溯源和合规性分析，即所谓的数据血缘能力。此外，WeData支持对数据进行分类分级，例如根据敏感度、重要性等进行划分，方便用户制定不同的数据安全策略。

数据本身的合规性与否，在多数场景下要看此数据与彼数据之间的关系，很多不敏感、合规的数据与其他数据汇聚之后，很可能就具备更高的敏感度与隐私性，其合规性要求就会变高。因此企业能够建立一张全面的资产地图，是否对自己的数据资产有全局的掌控就至关重要。否则企业外部互联网、监管机构将企业当成一个汇聚主体来看，会发现企业自己未曾发现的数据合规风险点，从而加大违规风险。

如下图所示，WeData能够接入多源异构数据，帮助企业建立更全面的数据视角与数据资产地图。

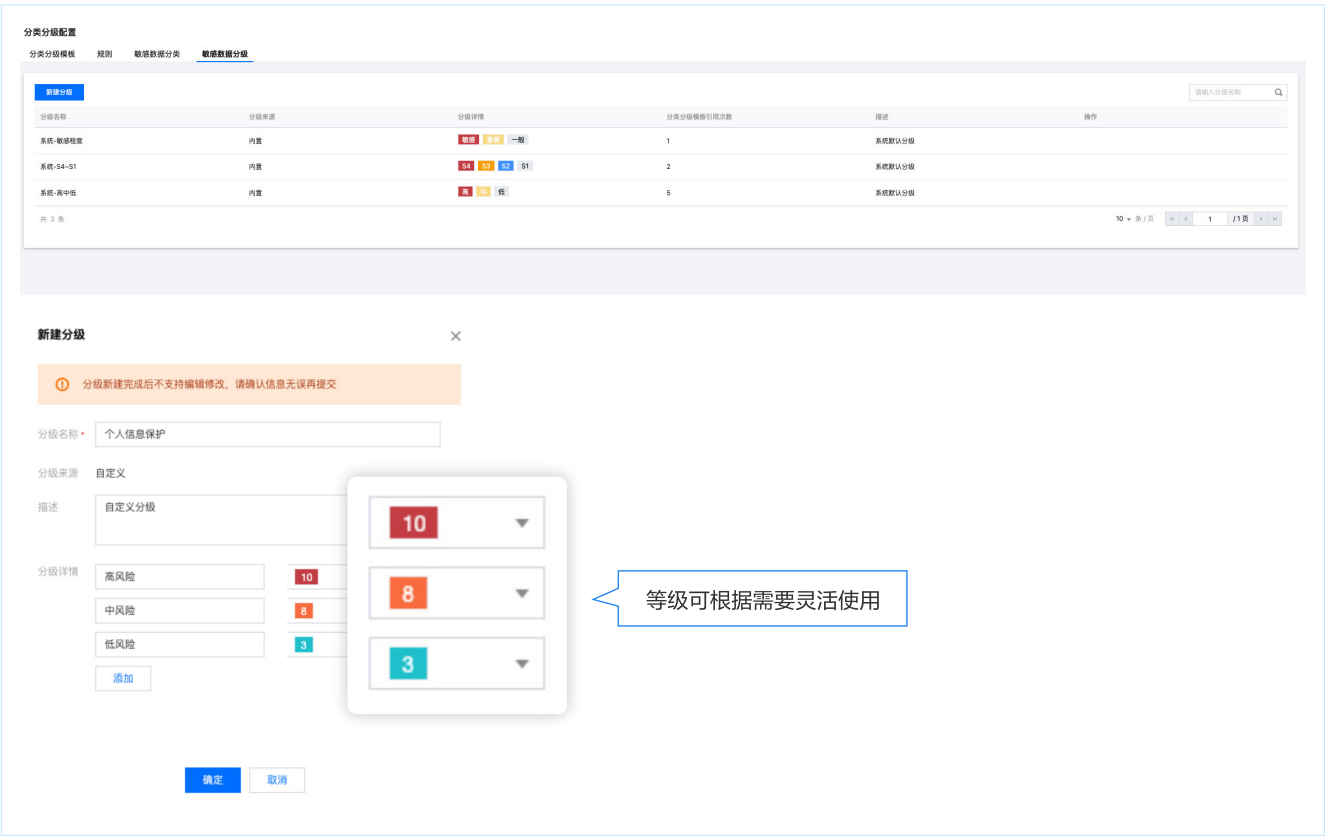


在接入众多异构数据源之后，接下来的一步就是数据分类分级。它是通过对数据全盘梳理，通过对数据分类分级&敏感数据采用不同的管控策略，实现精细化管控。将数据安全等级与敏感数据识别规则进行结合，以敏感数据识别任务的形式对数据进行周期性检查并输出相应的数据敏感度分类分级，同样支持人工对敏感数据进行打标。

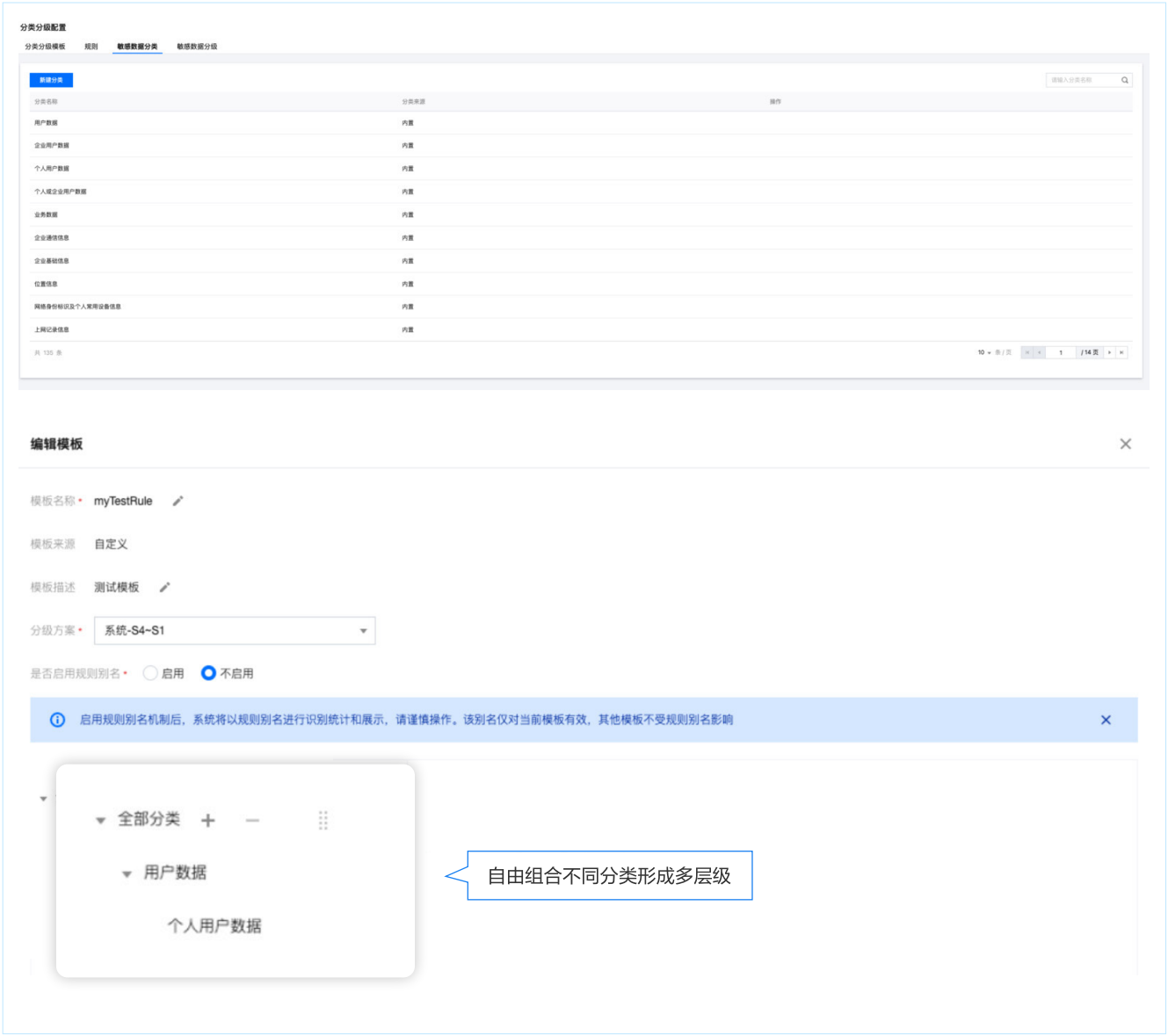
- 敏感数据识别



- 敏感数据分级

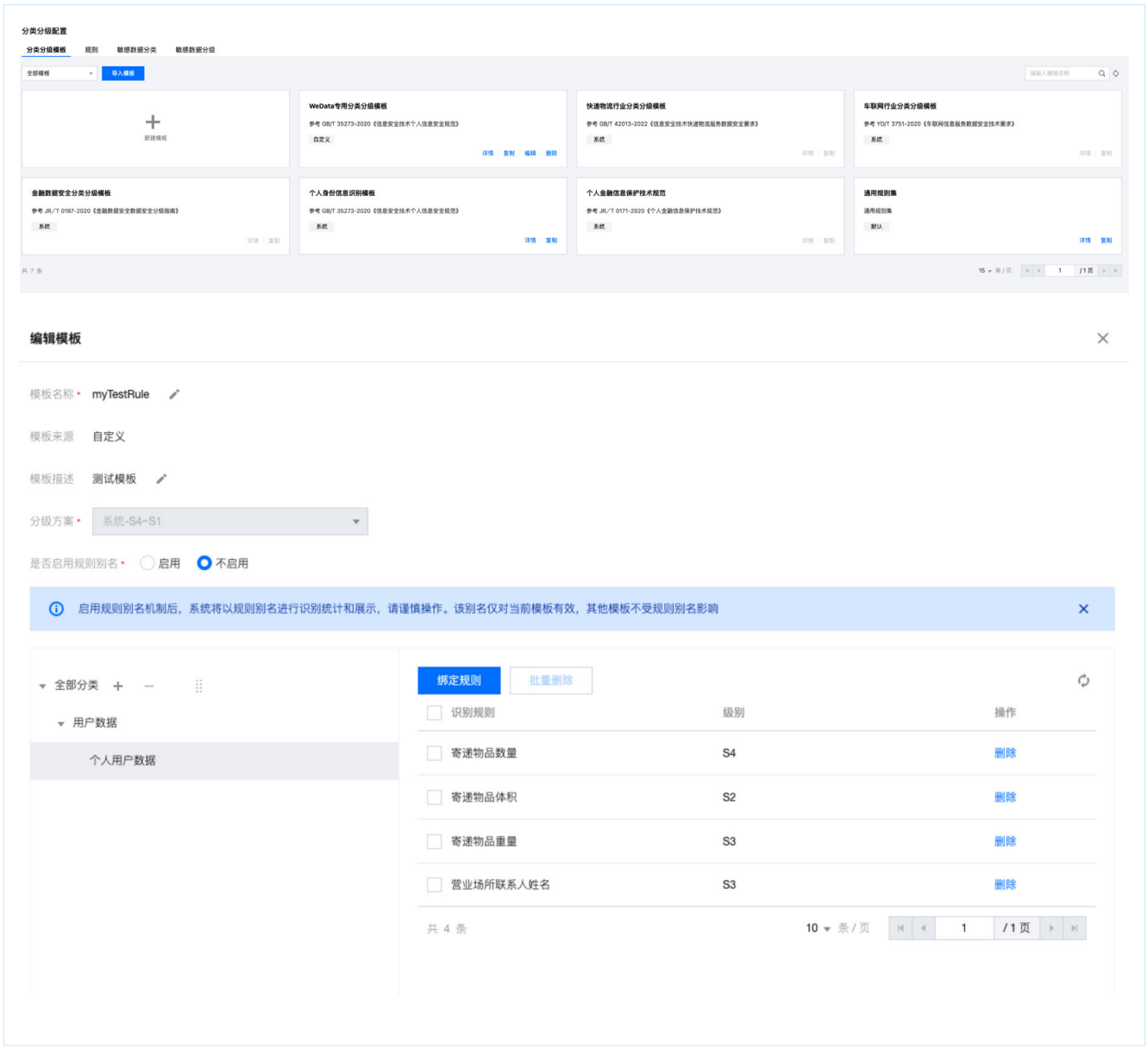


- 敏感数据分类


分类分级配置
分类分级模板
规则
敏感数据分类
敏感数据分级
新建分类
分类名称
分类来源
操作
用户数据
内置
企业用户数据
内置
个人用户数据
内置
个人或企业用户数据
内置
业务数据
内置
企业通信信息
内置
企业基础信息
内置
位置信息
内置
网络身份标识及个人常用设备信息
内置
上网记录信息
内置
共 135 条
10 条/页
1
/ 14 页
编辑模板
模板名称 * myTestRule
模板来源 自定义
模板描述 测试模板
分级方案 * 系统-S4~S1
是否启用规则别名 * 启用 不启用
启用规则别名机制后，系统将以规则别名进行识别统计和展示，请谨慎操作。该别名仅对当前模板有效，其他模板不受规则别名影响
全部分类
用户数据
个人用户数据
自由组合不同分类形成多层级

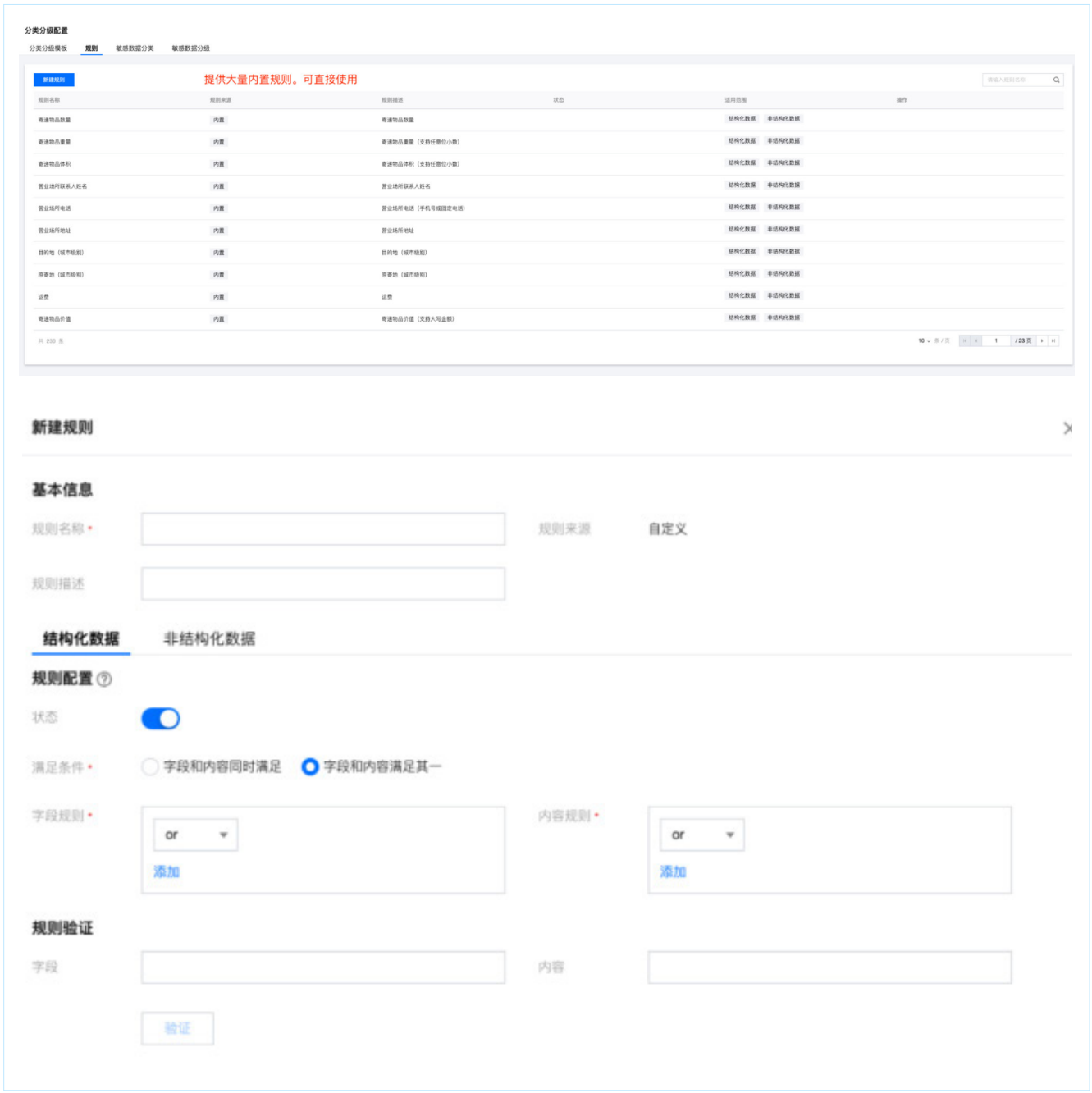
- **数据分级分类模板**

分类分级模板将分类、分级以及识别规则整合起来，实现某个业务场景下的敏感数据识别规则集。在 WeData 中，最终是按照分类分级模板粒度执行数据敏感识别的。为了方便快速使用，内置了5种分类分级模板，如：JR / T 0197−2020《金融数据安全数据安全分级指南》。同时用户也可以根据自己的业务场景自建模板（如GDPR隐私保护等）。



- **识别规则触发**

通过创建敏感数据识别规则的方式来针对数据表字段名称、字段描述、数据内容进行敏感数据识别，主要使用正则表达式来建立规则。利用数据安全分级与识别规则相结合，可以对识别到的敏感数据进行分类分级。

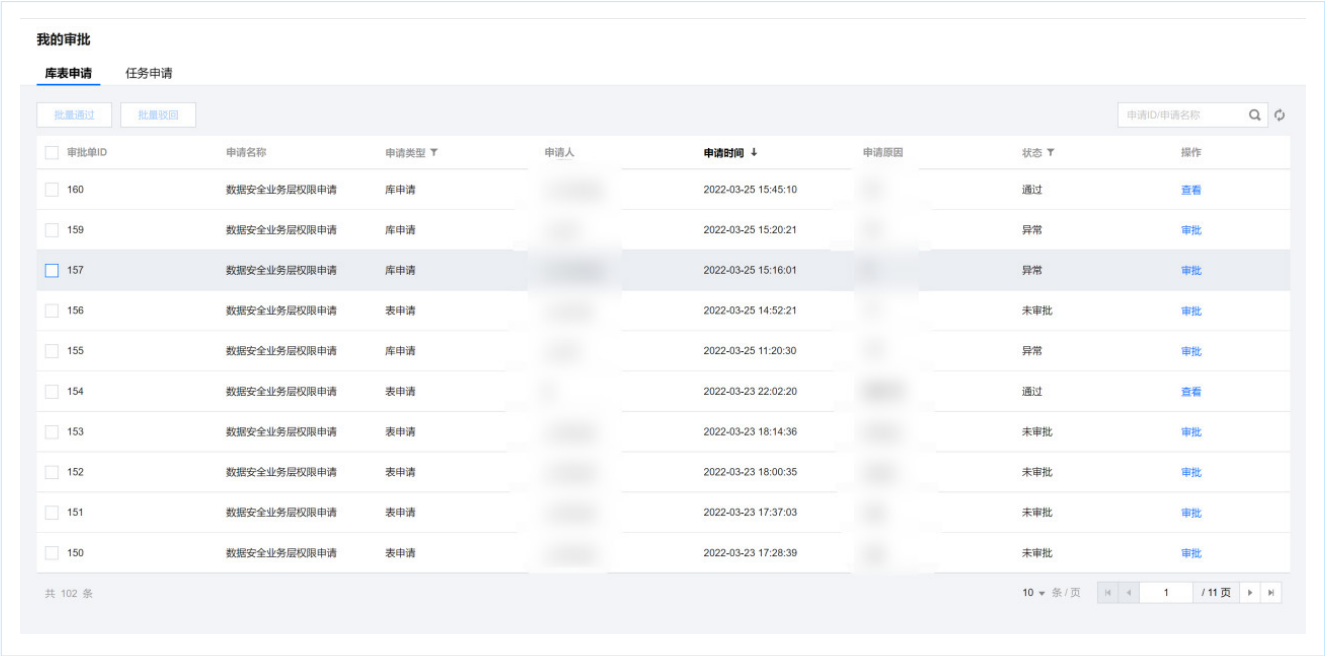


权限管控与风险控制

WeData提供细粒度的访问控制，可以根据用户角色和权限控制对数据的访问权限，防止敏感数据被非法访问。它的数据脱敏功能，可以对敏感数据进行脱敏处理，例如将姓名、身份证号等信息进行替换，保护用户隐私。WeData还支持数据加密，可以对数据进行加密存储和传输，防止数据被窃取。最后，WeData的数据审计能力，可以记录所有对数据的操作，方便用户进行数据审计和合规性检查，并在需要的时候提供给监管机构。

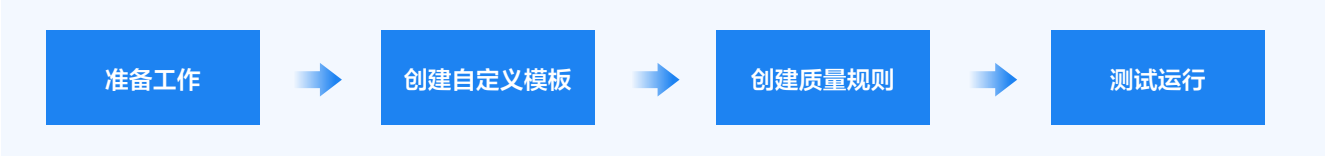
如在WeData控制台，管理员可以进行成员与角色管理。

用户可通过库表申请页面集中管理需要本账户审批的库表权限申请审批单。



合规检查与合规运营

WeData可以根据不同的数据安全法规和行业标准，对数据进行合规性检查，如 GDPR、CCPA 等（需要模板支持），并生成数据合规性报告，以方便用户进行合规性评估和汇报。



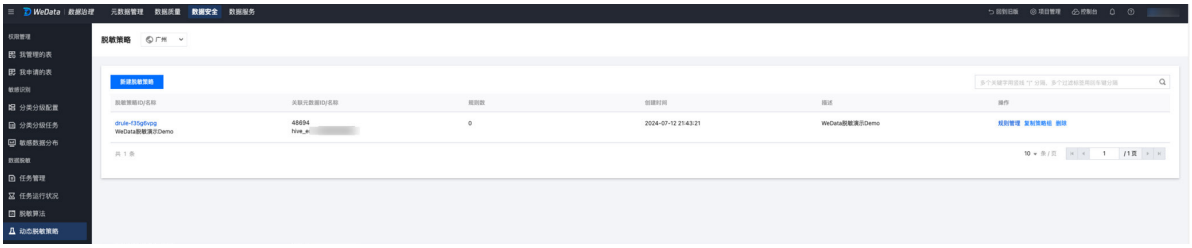
除此之外，WeData也可以帮助用户建立数据合规运营流程，例如数据风险态势研判、组织合规策略统一管理、数据合规风险自动化告警与处理等，能够大大方便数据合规的持久运营。

数据脱敏

数据脱敏包括动态脱敏与静态脱敏。

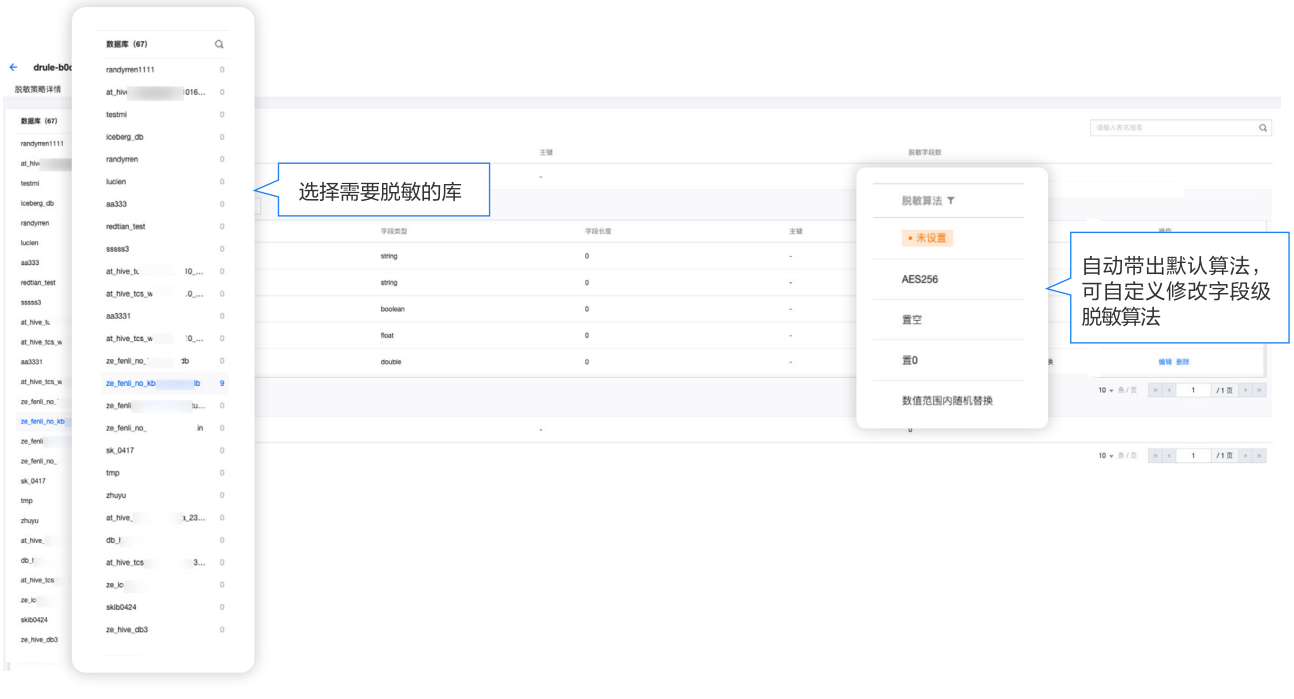
动态脱敏

数据动态脱敏是一种重要的数据安全技术，它能够在数据使用过程中，针对敏感数据进行实时的脱敏处理，以确保数据的隐私性和安全性。WeData支持用户级的数据动态脱敏策略配置，用户可以先开启动态脱敏并配置脱敏策略：





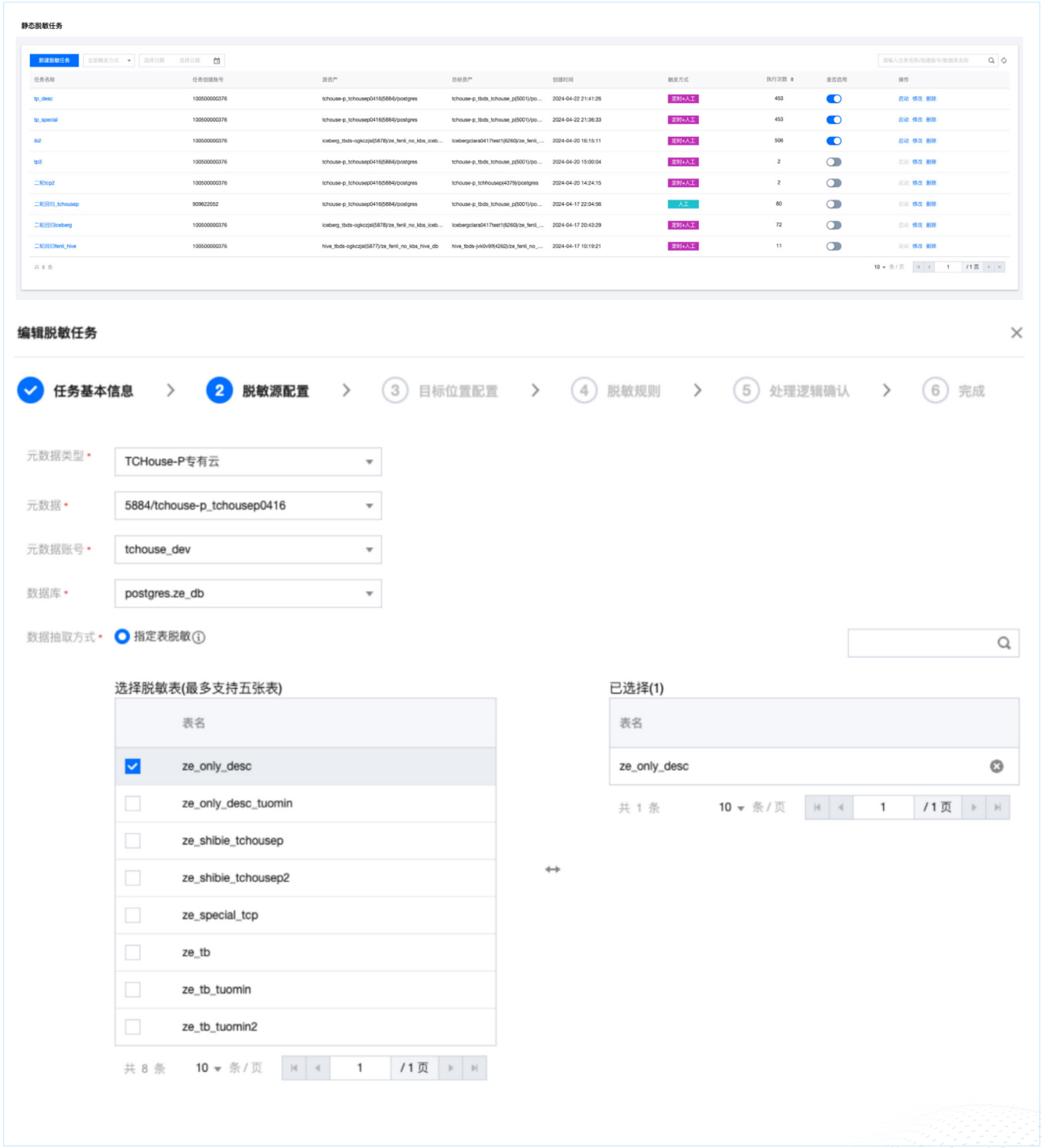
然后可以根据算法管理动态脱敏：



- 静态脱敏

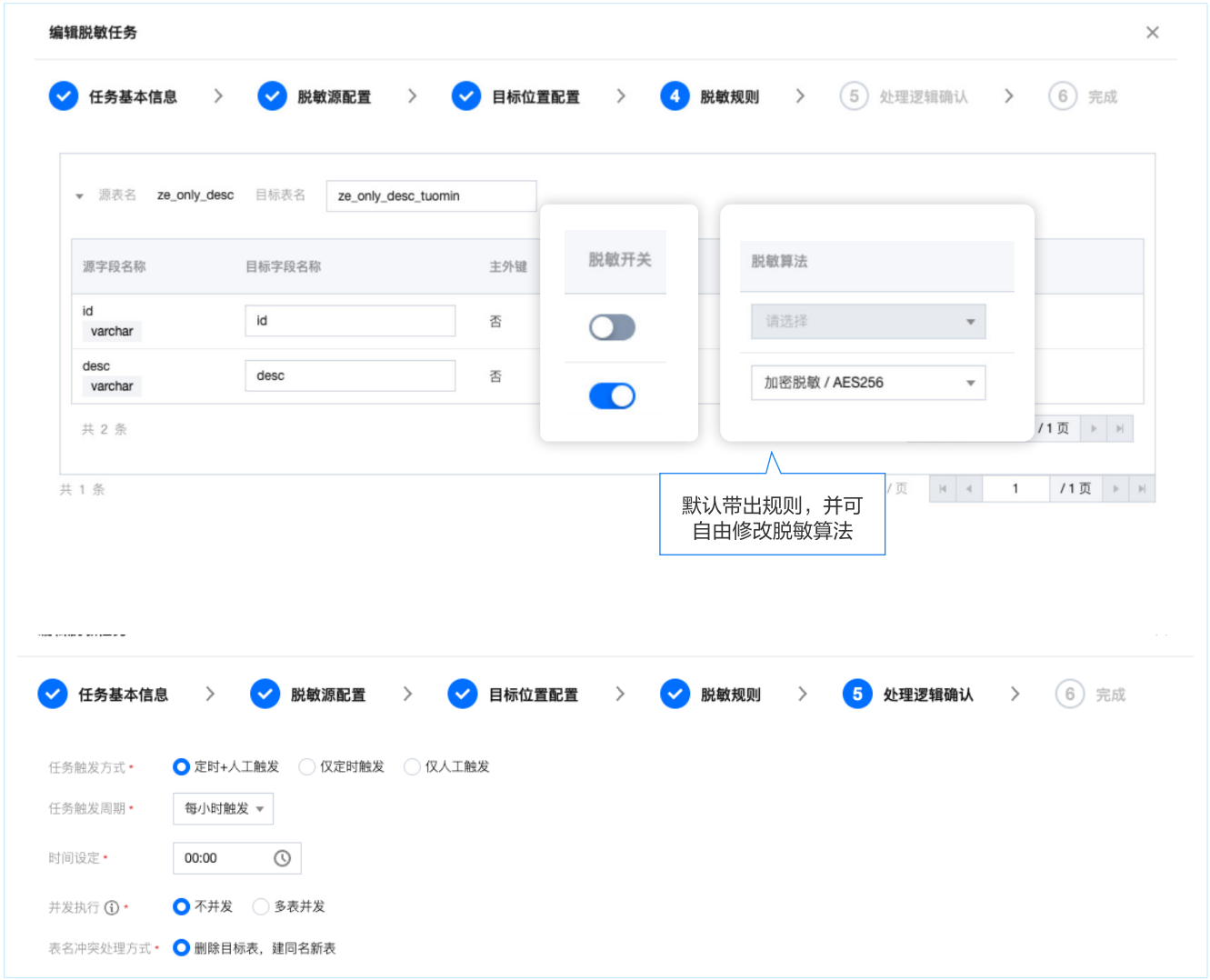
数据静态脱敏是一种常见的数据隐私保护技术，它指的是在数据存储或备份阶段，对数据中的敏感信息进行一次性的脱敏处理，使得数据不会泄露隐私。WeData静态数据脱敏通过离线任务方式，按照任务策略完成数据脱敏。

和动态脱敏相同，用户可以先新建静态脱敏任务：



- **脱敏规则触发**

接下来比较关键的是配置脱敏规则和脱敏触发规则：



腾讯云助力数据重要环节的安全合规 5.4

本章上述各小节的内容陈列了腾讯云在数据安全、数据合规各方面的能力，但是仅有这些能力仍然是一种静态的、被动的应对合规的态度，流动的数据才有价值，也只有将上述能力动态的应用到数据流动的各环节中，才能真正做好数据的安全合规。

这个动态的过程，从数据生命周期的视角来展开是业内通行的做法，也是一种比较合理的做法。因此本章各小节将从数据生命周期各阶段展开，以案例或最佳实践的形式，提供一份数据合规的落地样本。

5.4.1 数据生命周期视角合规实施框架

澳大利亚法规要求概述

简单来说，数据生命周期是指数据的采集、传输、存储、使用、共享、留存与销毁这六个环节。在实施过程中，有如下三个关键点需要注意：

- 在实际业务环境中，这六个环节并非是严格的顺序关系，而且也不是线性的单向流动关系，而是一个不断循环的关系。因此它是一个持续运营的过程，而不是一个一次性的项目或工程。
- 每一此循环务求解决阶段性问题并做一定的前瞻性建设即可，即无法也没必要一蹴而就将每个环节都建设到100分。
- 采取这些手段进行数据合规加固的核心是保障数据主体的权利。对企业来说，应对监管是末，保障数据主体权利是本。具体来说，就是保障数据主体对其数据的访问权、纠正权、擦除权、限制数据处理者或数据控制者处理数据的权力、个人数据的可移植权、反对处理其个人数据的权力、撤销之前授权给数据处理者/控制者处理数据的权力、否定自动化分析与决策的权力、个人数据泄漏被及时通知的权利、可以投诉数据处理者/控制者的权利。



5.4.2 数据采集收集

某在线教育公司为了提升用户学习体验，需要收集用户的学习习惯和学习效果数据。为了确保数据收集的合规性，该公司采取了以下措施：

- 制定数据收集政策：明确收集哪些用户信息，如学习时长、错题记录、学习效果等。
- 制定数据收集的目的和使用范围，如优化课程设计、改进教学方法等。
- 遵循数据最小化原则，仅收集与目的相关的必要信息。
- 获取用户明示同意：在用户注册或首次使用时，通过弹窗或勾选框的方式，明确告知用户数据收集的目的和用途，并获得用户的明示同意。同时提供拒绝授权的选择，尊重用户的隐私选择。
- 采取数据脱敏措施：对于一些敏感数据，如学习成绩、家庭情况等，在收集时即进行脱敏处理，如对名称进行随机替换等。确保即使数据泄露，也无法还原出用户的真实隐私信息。
  对于数据的脱敏技术方案，可以参考5.3.6.4章节和5.3.5章节。
- 制定数据保护政策：建立健全的数据安全管理措施，如访问控制、加密传输、备份恢复等，确保收集的数据得到妥善保护。
- 明确数据保留期限，到期后进行彻底删除或匿名化处理。在这个场景中，用户的个人数据主要会存储在MySQL数据库中以及腾讯云对象存储COS中。关于MySQL中的数据生命周期设置可以参考5.3.5.3小结。而对于COS中数据生命周期的设置，则可以参考腾讯云官网关于COS数据生命周期设置的内容：https://cloud.tencent.com/document/product/436/14605
- 定期合规性检查：建立数据合规性自查机制，定期检查数据收集、使用及保护措施的合规性。及时发现并修复合规隐患，确保数据合规性持续满足法规要求。

5.4.3 数据存储

某电商公司为了提升推荐效果，需要收集并存储用户的浏览、购买等行为数据。为了确保数据存储的合规性，可以采取以下措施：

- 制定数据分类管控策略：将收集的数据按照敏感程度进行分类，如个人身份信息、交易记录等属于高敏感数据。关于数据的分级分类存储，可以在应用代码层面对敏感字段进行设置，将收集的不同敏感级别的数据存储到不同的表或对象存储bucket中。也可以后续进行统一的敏感数据识别与自动分级分类，这部分内容可以参考5.3.6.1节。
- 对高敏感数据采取加密存储，低敏感数据采取脱敏处理。技术实现可以参考5.3.1.2节。
- 实施访问控制机制：建立基于角色的细粒度访问控制策略，确保只有经过授权的人员才能访问相应的数据。技术实现可以参考5.3.2节。
- 对数据库账号进行严格管控，定期审查权限，杜绝权限滥用。
- 部署数据安全防护：采用业界领先的数据库加密技术，如透明数据加密(TDE)等，确保数据在存储过程中的安全性。
- 建立完善的备份和恢复机制，确保数据在发生故障时能够快速恢复。
- 规范数据生命周期管理：制定数据保留政策，明确不同类型数据的保留期限和删除机制。
- 在到期后对数据进行彻底删除或匿名化处理，避免敏感信息泄露。
- 实施合规性审查：定期对数据存储环节的合规性进行内部审查，发现问题及时整改。
- 配合外部监管部门的合规性检查，确保数据存储完全符合法规要求。

5.4.4 数据共享

某金融科技公司为了提升风控能力，需要与其他金融机构之间共享客户信用信息数据。为了确保数据共享的合规性，该公司采取了以下措施：

- 制定数据共享政策：明确数据共享的目的，如信用评估、风险管理等。制定数据共享的范围和对象，如仅与持牌金融机构进行共享。约定数据共享的安全措施和使用规范。
- 签订数据共享协议：与数据共享对象签订明确的数据共享协议，约定双方的权利义务。协议中明确数据使用的目的、范围、期限以及违约责任等条款。约定数据接收方的安全管理措施，如数据加密传输、访问控制等。
- 实施数据脱敏处理：对于一些高敏感personal信息，如身份证号、银行账号等，在共享前进行脱敏处理。技术方案可以参考5.3.6.4小节。确保即使数据泄露，也无法还原出用户的真实隐私信息。
- 实施数据共享溯源：建立数据共享的日志记录机制，记录数据共享的时间、对象、内容等信息。定期检查数据共享情况，发现异常情况及时追查和处理。数据溯源的技术方案可以依靠WeData来实现。

此外，也可以使用腾讯云的可信计算服务方案来实现数据共享场景的安全与合规。详情请参考5.3.4节内容。金融联合风控本来就是可信计算服务重点针对的场景。

5.4.5 数据使用

某互联网公司为了提升用户画像精准度，需要对收集的用户行为数据进行深度分析和挖掘。为了确保数据使用的合规性，该公司采取了以下措施：

- 制定数据使用政策：明确数据使用的目的，如用户画像、个性化推荐等。规定数据使用的范围和对象，如仅用于内部业务，不对外共享。制定数据使用的安全措施和合规性审查流程。
- 建立数据匿名化处理：对用户的个人隐私信息进行脱敏处理，如将用户ID替换为匿名ID。确保即使进行复杂的数据分析，也无法还原出用户的真实身份信息。
- 实施数据使用审查机制：建立数据使用申请和审批流程，确保每次数据使用都经过合规性审查。审查数据使用的目的、范围、安全措施等是否符合既定的数据使用政策。
- 实施数据使用监控：建立数据使用的日志记录机制，记录数据使用的时间、地点、操作人员等信息。定期检查数据使用情况，发现异常情况及时追查和处理。
- 开展数据合规培训：定期对公司内部的数据使用人员进行合规培训，提高合规意识。培训内容包括数据使用政策、风险点识别、合规操作规范等。

上述各措施的技术方案都可以在5.3章节找到。通过上述措施，该互联网公司实现了数据使用的合法合规，既满足了业务需求，又有效保护了用户隐私，为后续的数据分析业务提供了安全可靠的数据基础。

5.4.6 数据传输

某医疗机构为了提升诊疗效率，需要与患者的家属进行医疗信息的远程共享。为了确保数据传输的合规性，该机构采取了以下措施：

- 制定数据传输政策：明确数据传输的目的，如病情沟通、病情随访等。规定数据传输的范围和对象，如仅与患者的直系亲属进行共享。制定数据传输的安全措施和合规性审查流程。
- 采用加密传输通道：使用符合行业标准的加密算法，如TLS/SSL协议，对传输中的数据进行端到端加密。确保即使数据在传输过程中被截获，也无法被窃取和解密。
- 采用加密传输通道：使用符合行业标准的加密算法，如TLS/SSL协议，对传输中的数据进行端到端加密。确保即使数据在传输过程中被截获，也无法被窃取和解密。
- 实施身份认证机制：要求传输双方进行身份验证，如通过数字证书或双因素认证。确保只有经过授权的人员才能接收和查看医疗信息数据。
- 建立传输日志记录：记录每次数据传输的时间、地点、参与者等关键信息。定期检查传输日志，发现异常情况及时处理。
- 开展数据合规培训：定期对参与数据传输的医务人员进行合规培训，提高合规意识。培训内容包括数据传输政策、安全操作规范、风险点识别等。

通过上述措施，该医疗机构实现了数据传输的合法合规，既满足了业务需求，又有效保护了患者隐私，为后续的远程医疗业务提供了安全可靠的数据基础。

5.4.7 数据删除与销毁

某电商公司为了优化仓储管理，需要定期清理无用的历史订单数据。为了确保数据销毁与删除的合规性，该公司采取了以下措施：

- 制定数据保留政策：明确不同类型数据的保留期限，如订单数据保留3年、客户信息保留5年等。规定数据到期后的销毁与删除流程，包括审批、执行、验证等步骤。
- 建立数据销毁机制：对于纸质文档，采用碎纸机进行物理销毁，确保无法还原。对于电子数据，采用专业的数据擦除工具进行彻底删除，确保不可恢复。针对不同介质的数据，采取相应的销毁方式，如硬盘物理粉碎、磁带加热熔毁等。
- 实施销毁记录管理：建立数据销毁的台账，记录销毁的时间、地点、方式、负责人等信息。定期检查销毁记录，确保数据销毁得当，无遗漏。
- 建立销毁审查机制：对数据销毁的申请和执行情况进行审查，确保符合既定的数据保留政策。审查数据销毁的目的、范围、方式等是否合法合规。
- 开展数据合规培训：定期对相关人员进行数据合规培训，提高数据销毁与删除的合规意识。培训内容包括数据保留政策、安全操作规范、风险点识别等

06

不同行业出海数据合规建议

跨境电商

社交文娱

游戏

汽车/出行

教育

金融服务

传统制造业

智能终端制造业

行业案例梳理

跨境电商 6.1

6.1.1 行业监管概要

欧盟

- **GPSR《通用产品安全法规》**

GPSR《通用产品安全法规》：GPSR（The General Product Safety Regulation）是欧洲委员会制定的新《通用产品安全法规》，是保障欧盟市场上产品安全的基本法律规范。将在2024年12月13日起取代现行的《通用产品安全指令》和《食品仿制产品指令》。GPSR适用线下及线上销售的所有非食品类产品。GPSR是对之前欧盟《通用产品安全指令》（GPSD）的进一步修正及完善，在产品合规负责人、产品标签、证明文件、沟通渠道等方面均做出了重要调整，增加了新的合规要求。GPSR要求，如果经营者进行网络远程销售，那么应当在其网站上清晰、显著地标明下列信息：

- 制造商名称、注册商号或商标以及邮政和电子地址
- 如果制造商没有欧盟地址，则提供欧盟责任人的姓名和联系方式
- 产品标识符（例如照片、类型、批次、描述、序列号）
- 警告或安全信息

因此，为了产品的合规销售，只要你的产品进入到欧盟市场，符合条件的卖家就必需注册欧盟责任人，并且确保产品带有可识别信息，具体内容如下：

- 注册欧盟责任人：GPSR 要求对于投放到欧盟市场的每件产品，必须有一个在欧盟设立的经济运营商，明确负责安全相关任务。该负责人应在产品或其包装上或随附文件中标明相关信息。确保可以根据要求向市场监督机构提供技术文件，欧盟境外制造商的产品在欧盟出现任何故障/事故/召回等问题，应由欧盟授权代理进行联络，通报，并与主管机关进行沟通联系。
- 确保产品带有可识别信息（批次号或序列号）：在可追溯性方面，制造商有一项新义务，即确保其产品带有可识别产品的信息（例如批次号或序列号），这些信息对消费者而言需要易于查看和辨认。GPSR要求经济运营商能够在供应后10年和6年内分别提供有关产品的信息，并识别其采购方或供应方，因此卖家需要收集和存储相关数据。

- **ICS2进口管理系统2**

Import Control System 2 (ICS2) 第 3 版是欧盟 (EU) 实施的新一代预到货安全和保护系统的第三阶段。该 IT 系统已升级，可在货物运抵前，收集所有运往欧盟的货件数据。ICS2 旨在通过新的海关安全和安保措施，更好地保护欧洲的每一座市场及其公民，并通过适用于全球业务模型的、数据驱动型海关安全流程，促进贸易自由流动。从事货物、快件或 邮递货物的装卸、海运 和运输的所有经营者，需要向 ICS2 提供安全和安保数据。即使最终的目的地不在欧盟，所有通过任何欧盟国家/地区转运的货件同样需要进入 ICS2 系统，例如货件从亚洲运往英国，途经任何欧盟国家中转的情况。

- **MSR《市场监管法规》**

《欧盟市场监管法规 2019/1020》(《The Market Surveillance Regulation》）于 2021 年 7 月 16 日生效。新法规要求带有 CE 标志的商品需要具有在欧盟的人员作为商品合规性联系人（下称“欧盟负责人”）。除医疗器械、民用爆炸物以及某些升降机和索道装置外，所有带有 CE 标志的商品均在该法规适用范围内。如果销售的商品带有CE标志并且是在欧盟境外制造的，那么需要确保:

- 此类商品具有在欧盟的负责人；
- 带有 CE 标志的商品贴有负责人的联系信息。此类标签可以贴在商品、商品包装、包裹或随附文件上。

在 2021 年 7 月 16 日之后，在欧盟销售带有 CE 标志的商品但没有欧盟负责人属于违法行为。

美国

CBP 海关和边境保护局

2003年，美国海关总署解散，新成立的海关和边境保护局（Bureau of Customs and Border Protection，下称“CBP”）承担了海关总署的大部分职能。CBP于2016年2月23日发布了“3D式”执法操作方案，显示了CBP如何通过对高风险商业活动的监测，打击商业欺诈以及阻止不合规行为，如增加保证金、加强对高风险进口产品的定位和检查，以及对指控进行迅速和彻底的审查，以确保公平竞争的贸易环境。这也为CBP对跨境电商的监管提供了总的指导路径。CBP通过与美国各行业、47个美国合作机构以及外国政府协调合作，检测全球供应链中的异常情况、趋势和违规行为，以锁定高风险货物并促进合规。通过与ICE合作，CBP能够打击非法利用美国贸易的犯罪组织，并在边境内外开展执法行动，以确保美国平等竞争的贸易环境。

加州消费者隐私法案 California Consumer Privacy Act (CCPA)

加州消费者隐私法 (CCPA) 是美国第一个全面的隐私法。 它为加州消费者提供了多种隐私权利。 受CCPA监管的企业将对这些消费者承担许多义务，包括披露、一般数据保护条例 (GDPR) 类似消费者数据主体权利 (DSR) 、某些数据传输的“选择退出”以及未成年人的“选择加入”要求。CCPA仅适用于在加州开展业务并满足以下一项或多项条件的公司：(1家)的年总收入超过2500万美元，或(2)年收入的50%以上来自销售加州消费者个人信息，或(3)购买， 每年出售或共享超过50,000名加州消费者的个人信息。CCPA于2020年1月1日生效。 加州总检察长(AG)于2020年7月1日开始执行。加州AG执行CCPA，并有权开具不合规罚款。CCPA还提供仅限于数据泄露的私有行动权。私人诉权规定，每位消费者在每个事件中受到的损失可能介于100美元到750美元之间。加州司法部长还可在整体上实施CCPA，可就每次违规征收不超过2,500美元的民事罚款，就每次故意违规征收7,500的民事罚款。

6.1.2 合规关注要点

数据隐私

电商企业必须遵守《通用数据保护条例》（GDPR），保护欧盟居民的个人数据，确保数据收集、使用和存储的透明性和合法性。

数据安全

跨境电商业务流程中面临多个环节的数据安全问题，如源自跨境电商企业内部的信息泄露、物流供应商的系统漏洞以及针对用户的钓鱼攻击、账号被盗和木马病毒侵入等，企业必须全面关注并解决这些来自不同环节的数据安全问题，采取合适的措施以保护用户和企业的数据安全。

海关监管

遵守包裹物流发出国，途径国及目的国的海关关于跨境电子商务零售进出口商品的监管规定，确保业务相关电子数据和电子信息的真实性和实时传输。

税务合规

遵循涉及相关国家的税收政策，确保税务合规。

同意管理

确保获取用户的合法有效授权同意是跨境电商企业应优先考虑的合规问题。基于同意作为数据处理合法性基础的前提，在收集用户数据前，是否以明示、清晰的方式获取了用户的同意是最易感知的、易引发用户关注及投诉的个人信息收集问题。通常情况下，以下数据收集情景，电商企业应特别留意：

第一，应设立隐私政策等明确的个人信息收集处理规则。

第二，应以醒目、显著、易于察觉的方式呈现隐私政策（例如使用弹窗、明显的选择框等），方便用户查阅或获得用户的清晰同意。

第三，隐私政策内容需要详实，真实明示产品和服务所涉及的收集和处理的数据类型、数据共享和数据跨境的情况。

此外，考虑到电商的多样性和便捷性，数据收集也可能隐藏在私域流量运营等典型情境中，例如在即时通讯应用的群组聊天或评论中。在平台提供的隐私政策之外，电商企业应结合平台特点，在实施具体数据收集处理活动之前，通过友好的提示或对用户友好的设计，引导用户仔细阅读个人信息收集处理规则，了解并同意规则内容，以确保数据收集场景的合法性。

定向营销

定向营销场景依赖于对个人数据的收集和分析，以精准地针对特定用户进行广告投放，需要确保决策过程的透明度和结果的公正性，以降低合规风险并保护消费者权益，应满足的合规要求如下：

第一，用户同意和知情权：收集用户数据前，必须以明确、透明的方式告知用户数据将如何使用，并获得他们的明示同意。用户应该清楚了解他们的数据是否将用于定向广告。

第二，退出和选择权：用户应具备随时退出定向广告或选择不接收个性化广告的权利，并且这些选项应该易于实现。当用户明确表示拒绝接收个性化推荐时，不得再继续向其发送商业性信息。对于采用自动化决策方式进行商业营销的情况，应同时提供不基于个人特征的选项。

第三，数据最小化原则：企业应仅收集为实现定向营销目标所必需的数据，而不是过度收集用户信息，以降低潜在的隐私风险。

第四，个人信息的匿名化和去标识化：在将个人数据用于定向广告时，最好使用匿名化和去标识化技术，以降低用户被识别的风险。

第三方数据共享

跨境电商企业在使用数据的过程中，可能涉及与物流供应商、支付服务提供商、第三方平台供应商等第三方进行数据共享，对其中涉及的大量隐私合规风险，应采取足够的组织和技术措施进行管控。应重点关注的领域包括：

第一，识别角色并明确义务：识别企业和第三方的数据处理角色，明确双方在数据保护方面的权利和义务。

第二，明确数据使用的目的：为避免数据被滥用，要确保合同中明确定义了共享数据的使用目的，并限制第三方只能按照这些明确的目的使用数据。

第三，授权和知情权：透明地向数据主体提供共享细节是合规的关键，要确保数据主体已明确同意数据共享，并清楚了解他们的数据将与哪些第三方共享。

第四，数据安全保护：确保第三方有足够的安全措施来保护共享的数据，包括数据传输和存储的加密、访问控制、漏洞修复等。

第五，监管和审计：建立监管机制，允许企业对第三方的数据使用情况及数据安全措施的有效性等进行定期审计以确保合规性。

知识产权保护

跨境电商领域涉及的知识产权主要是商标权、著作权、专利权等，大多以文字、图片、声音、视频等数据信息的形式呈现，纠纷类型有商标侵权、专利侵权、著作权侵权、不正当竞争等。

消费者权益保护

退货与售后服务：许多国家对跨境电商的售后服务有严格要求，包括退货政策、退款流程和售后服务的响应时间。电商平台需确保其售后服务符合目的国的法律要求，以维护消费者权益。

消费者投诉与争议解决：在跨境交易中，消费者投诉和争议时有发生。电商平台应建立有效的投诉处理机制，并熟悉目的国的争议解决程序。

支付合规

支付处理与反洗钱法规：跨境支付涉及多个国家的金融监管，如反洗钱法规（AML）和反恐融资法规（CFT）。电商平台需确保支付流程符合国际及当地的金融法规，避免因不合规导致资金被冻结或交易失败。

6.1.3 腾讯云合规技术建议

用户注册及登陆

跨境电商需要实名认证，腾讯云慧眼人脸核身（原金融级身份证认证升级版）是一组对用户身份信息真实性进行验证审核的服务套件，提供各类认证功能模块，包含证件 OCR 识别、活体检测、人脸1:1对比等能力，以解决对跨境电商用户身份信息核实的需求。

图像搜索–侵权审核

电商平台对品牌logo、版权图案、原创花纹等图像元素进行侵权审核，及时发现售卖盗版商品、抄袭原创设计、造假入驻商家资质等问题，帮助品牌方打击侵权盗版，提升正品和原创保护效率。

跨境交易反欺诈风险识别

国际信用卡组织对拒付率的监管要求严格，相关处罚严厉。海外黑灰产通过交易流程中的正当规则允许的“漏洞”，恶意拒付以实现牟利目的，给商户和平台带来巨大损失。腾讯云风控引擎RCE通过交易反欺诈风险评分模型，在不采集个人隐私数据的前提下，实现精准识别黑灰产的请求，从而帮助商户和平台降低拒付率并提升订单通过率。

社交文娱 6.2

6.2.1 行业监管概要

欧盟

欧盟对社交媒体行业的监管和立法是走在全球前列的，相对也比较完整，并对其他国家或地区有着借鉴意义。在欧盟，除了GDPR，还有如下几部在数据合规方面的立法需要出海的社交文娱行业企业重点关注：

Digital Services Act（DSA，数字服务法）：DSA适用于向欧盟用户提供数字服务的各类在线平台，包括社交媒体、在线市场等。根据平台规模和潜在风险，DSA将其分为微型、小型、大型和超大型平台。DSA要求所有在线平台都需要建立内容管理机制，及时删除违法和有害内容，大型和超大型平台需要更严格的内容审核和用户保护措施。平台必须公开其算法、广告投放机制和内容推荐系统的运作情况，用户也必须能够了解其个人数据如何被用于个性化推荐的。DSA还要求大型和超大型平台需要定期评估自身服务对社会和民主的潜在风险，并采取相应措施，如强化内容审核、限制广告投放等来缓解这些风险。

DSA规定大型和超大型平台须接受独立第三方的年度审计，评估其合规情况，审计报告需向监管机构和公众披露。需要注意的是，DSA赋予欧盟委员会跨境执法的权力，包括对违规平台处以高达全球营业额6%的罚款。对于屡次违规的平台，监管机构还可以要求其暂时或永久停止在欧盟的服务。

总的来说，DSA是欧盟为规范互联网平台行为、保护用户权益而出台的一部重要法规。它将对包括社交媒体在内的数字服务提供商产生广泛影响。

ePrivacy Directive（即“Cookie Law"，cookie法）：该指令适用于使用Cookie和其他类似跟踪技术的网站和电子通信服务。网站必须获得用户的明确同意，才能在用户设备上存储或访问Cookie。用户的同意必须是自愿的、具体的、知情的，并可随时撤回。此外网站或应用必须向用户提供关于Cookie用途和管理方式的明确、易懂的信息。

Cookie法由各成员国负责执法和监Cookie使用的合规情况，违反规定的企业可能面临罚款等处罚。

Audiovisual Media Services Directive（AVMSD，即视听媒体服务指令）：该指令适用于各类视听媒体服务，包括传统电视广播和点播视频服务，以及社交媒体平台等托管用户生成视频内容的在线服务。指令要求视听媒体服务提供商对内容进行分级，以保护未成年人免受不适当内容的影响，禁止含有煽动仇恨或歧视性的内容。指令要求视听媒体服务提供至少30%的欧洲作品内容，并给予适当的突出展示，这旨在推动欧洲文化作品在数字时代的传播。指令规定视听广告必须易于识别，不得误导受众或损害儿童利益。

该指令由各成员国负责建立独立的国家监管机构，监管视听媒体服务提供商的合规情况，违反规定的企业可能面临处罚。总的来说，AVMSD旨在规范欧洲视听媒体市场，保护受众利益，促进欧洲文化作品的传播。这对社交媒体等在线视频服务提出了新的合规要求。

Platform-to-Business（P2B）Regulation（平台对企业条例）：该条例适用于在线平台与其商业用户之间的关系，与电商行业相关性较强，但也包括社交媒体平台与其商业页面或广告客户。条例要求在线平台必须以清晰、易懂的方式公开其商业条款和条件，包括排名算法、广告投放和数据访问政策等关键信息。禁止平台采取任何不公平或不透明的做法，损害商业用户的利益，如突然终止合作关系、不当修改条款等。此外平台必须为商业用户提供内部申诉和纠正机制，便于商家就平台行为提出质疑和投诉，商家可以诉诸独立的调解或仲裁机构解决与平台的争议。

该条例由成员国指定主管部门负责监管和执法，违反条例的企业可能面临罚款等处罚。P2B条例旨在确保在线平台与其商业用户之间的关系更加公平透明，以促进数字市场的健康发展。这也影响到社交媒体平台与广告客户或商业页面运营者的互动。

Network and Information Security Directive（NIS2 指令）：详见3.1.4.2节内容

美国及其他国家地区

美国目前还没有像欧盟GDPR那样全面的联邦数据隐私法，涵盖社交媒体和互联网行业。但是，以下两项相关法律和规定适用于这个行业的数据和隐私保护：

The Federal Trade Commission Act（FTC act，联邦贸易委员会法）：FTC法案授权FTC禁止"不公平或具有误导性"的商业行为，这包括社交媒体公司的数据收集和使用。例如，FTC已针对Facebook、Twitter等平台的隐私保护不力、欺骗性的广告等进行过调查和处罚。FTC法案要求企业如实披露其数据收集和使用政策，不得隐瞒或误导用户，这促使社交媒体公司必须加强其隐私政策的透明度，让用户更好地了解自己的数据如何被使用。FTC执行的COPPA法规定，网站/应用如收集13岁以下儿童个人信息，必须获得父母同意，这对社交媒体行业构成约束，要求其加强对儿童用户个人信息的保护。

FTC持续监测社交媒体公司的隐私和数据安全实践，并有权进行调查和处罚。这增加了社交媒体企业合规的压力，促使其持续优化用户隐私保护措施。总的来说，FTC法案为保护消费者、用户隐私权提供了重要法律依据，对社交媒体行业的数据收集、使用和保护产生了深远影响。这有助于增强用户对社交媒体平台的信任，促进行业健康发展。

The Children's Online Privacy Protection Act（即COPPA，儿童在线隐私保护法）：COPPA是美国政府针对儿童个人信息保护而制定的一项重要法规，适用于面向儿童13岁以下的网站、在线服务和移动应用。包括社交媒体平台、游戏网站、教育技术等行业。COPPA要求如果网站/应用收集13岁以下儿童的个人信息，必须先获得家长的书面同意，家长可以选择允许收集、限制收集或拒绝收集儿童个人信息。COPPA还规定了网站/应用可收集的儿童个人信息类型，如姓名、地址、位置等，必须最小化收集范围，只收集实现功能所必需的信息。COPPA要求网站/应用必须制定易于理解的儿童隐私政策，阐述信息收集和使用的细节，并提供家长查看和管理儿童个人信息的渠道。

由FTC负责COPPA的执法，包括调查违规行为并处以罚款等。COPPA违规可能导致高达4250万美元的罚款。总的来说，COPPA为保护儿童上网隐私权提供了重要的法律保障，要求社交媒体等公司采取更加负责任的数据收集做法。这有助于营造更加安全的儿童网络环境。

其他国家，如加拿大、澳大利亚、韩国、日本、欧盟（儿童隐私保护蕴含在GDPR里）等也都有儿童隐私保护相关的立法。

其他国家或地区（如日韩、中东、东南亚等）在社交与互联网娱乐行业的监管基本上是欧盟监管范围的子集，对于出海企业来说，遵循欧盟的法规，再加上着重遵循上述美国的两部法规，就可以大大提升全球的数据合规与隐私保护水平，降低合规风险。

6.2.2 合规关注要点

数据采集

在数据采集方面，需要重点关注以下两个方面：

- **隐私协议声明：**需要在隐私协议声明中简明易懂地说明要求用户自己提供的信息、网站/应用自动收集的信息以及其他来源的信息。尤其是关于这三类信息的采集方式的使用目的。例如出于对ePrivacy Directive的遵守，企业需要在隐私协议声明中明确网站使用的Cookie和类似的跟踪技术，如使用Cookie来记住用户语言偏好，或确保用户不会多次观看同一视频等。同样处于非必需目的的用于营销的cookie、SDK等也需要详细列出并说明。建议企业可以学习参考行业头部企业的做法，详细了解其官网的隐私协议声明。
- **数据采集的正当性、合法性和必要性：**企业需要遵循最小必要原则来采集数据，非必要不采集，保证数据采集的正当性、合法性。尤其是针对敏感数据的收集，需要在数据采集环节建立明确、可操作的用户同意机制，获得用户对数据收集的明确授权。

数据存储

社交媒体行业企业需要关注数据安全保护，采取适当的技术和组织措施，确保个人数据的机密性、完整性和可用性，包括访问控制、加密、备份恢复等措施。

社交文娱行业企业往往会存储各式各样的个人数据和非个人数据，对这些数据的分级分类不仅是各国监管的重点关注领域，也是企业能够将数据合规方案进行落地的基础。企业需要对敏感/隐私数据采取更严格的安全措施。

企业需要制定合理的数据保存期限政策，避免无限期保留个人信息，在达到保存目的后及时删除或匿名化处理。此外更重要的是需要向用户说明数据的存储地点，这在跨境部署的场景中尤为重要。企业需要遵守业务所在国法律，以此来决定是否需要数据跨境或数据本地存储。企业最好能够在前述数据分级分类的基础上，详细说明各种不同的个人数据存储策略。如使用手机号码注册账号，如果用户需要一直访问服务，则企业会一直保存其手机号码（包括初始注册手机号码、绑定的手机号码等），以保证用户正常使用该服务。当用户注销后，平台则需要依法删除相应的信息。当企业的产品或服务发生停止运营的情形时，企业需要以推送通知、公告等形式通知用户，并在合理的期限内删除用户的个人信息或进行匿名化处理。

企业需要建立数据处理活动记录，记录数据的收集、使用、存储等全生命周期信息，以便于监管部门检查和用户查询。

信息安全

对于社交文娱行业而言，信息安全主要涉及以下三个子场景：

- **数据加密：**主要指数据在端侧、传输、存储和共享等环节的加密保护。企业需要明确在这些环节采用什么技术手段或管理手段来确保数据加密能力的落地。
- **管理制度：**企业需要建立专门的制度、操作规程和组织以保障信息的安全。例如，严格限制访问信息的人员范围，要求他们遵守保密义务，并进行审计等。此外，请外部成员组成的独立机构对企业的个人信息保护情况进行监督也是一种不错的手段。
- **应急与通知：**如果发生个人信息泄露等安全事件，企业的应急预案及补救措施需要提前准备，以阻止安全事件扩大，并依法履行相关的报告及通知用户的义务。

第三方数据共享与营销

一般社交文娱行业企业为了投放广告，评估、优化广告投放效果等目的，会向广告主及其代理商等第三方合作伙伴共享用户的部分数据。企业需要要求合作伙伴严格遵守关于数据隐私保护的措施与要求，包括但不限于根据数据保护协议、承诺书及相关数据处理政策进行处理，避免识别出个人身份，保障隐私安全。同时企业需要公布其《第三方信息共享清单》。

在上述场景中，企业在其网站或应用中会使用较多第三方的SDK，因此需要在《第三方信息共享清单》中明确列出这些SDK，并说明这些SDK收集数据的方式、范围和目的。

最后，企业不能向合作伙伴分享可用于识别用户个人身份的信息，除非你用户明确授权。对于已经授权的合作伙伴，要允许用户能够撤销授权，例如不允许平台上某个广告商获取用户的行为数据或不允许向其推送广告等。

数据主体行权

企业需要完善用户权利通道，建立便捷、高效的用户权利行使渠道，如在线查询、删除等，确保用户能够轻松行使查询、修改、删除等权利，及时、全面地响应用户行使权利的各种请求。无正当理由不得拒绝或拖延用户的合法诉求。

企业需要建立完善的用户身份验证机制，确保只有真实用户才能行使权利，防止未经授权的第三方滥用用户权利。在处理用户的数据请求时流程要透明，向用户明确说明处理用户请求的具体流程和时限，增强用户的信任感和体验。

原则上不得收取用户行使权利的任何费用，除非法规允许收取合理费用。

企业如果拒绝用户请求，应提供合法、正当的理由说明，确保拒绝行为合法合规。当用户要求删除个人信息时，企业需要及时彻底地删除或匿名化用户要求删除的个人信息，防止用户信息的泄露和滥用。

未成年人保护

企业需要特别关注未成年人的隐私保护，如果业务涉及的国家或地区有相关的未成年人隐私保护法规，建议企业单独起草一份《未成年人隐私保护声明》，和常见的《隐私协议声明》一样公诸官网。不同国家对未成年人的年龄规定有所差异，企业需要注意。

如某些社交互娱网站/应用是不允许未成年人访问使用的，有些则会限制未成年人的使用范围。大部分国家不允许对未成年人推送商业广告，也不允许对未成年人收集非必需的数据（这个场景中个性化推荐的能力就需要限制）。

更重要的是，在《未成年人隐私保护声明》中需要明确未成年人的家长/监护人所要履行的义务和责任，在网站/应用中为家长提供查看、管理未成年子女数据的便利通道，尊重家长对未成年人信息的监护权。

6.2.3 腾讯云合规技术建议

结合各国家地区的法规，以及合规主要关注点，社交文娱行业企业在数据合规的落地过程中，可以结合整体咨询方案，充分利用如下腾讯云提供的技术方案和产品进行落地。

内容安全方案

首先，可以利用腾讯云的强大计算能力，部署AI驱动的内容审核系统，快速识别并过滤违法违规、涉及未成年人的不当内容。确保内容发布前能够自动化地进行合规性检查。这属于应用层的合规检查。可以使用腾讯T-Sec天御的四大功能模块（文本内容安全，图片内容安全、音频内容安全、视频内容安全）来实践技术方案。关于腾讯T-Sec天御，可参考官网链接：https://cloud.tencent.com/product/ims

其次，内容存储与加密腾讯云存储服务，对用户生成的内容进行安全存储。采用加密等技术手段，保护敏感内容数据的机密性。技术方案可以参考5.3.1.2小节内容。

最后，腾讯云可以提供实时内容监控能力，利用腾讯云的大数据分析能力，实时监控平台上的内容动态。及时发现并处理违规内容，降低合规风险，为监管部门提供必要的内容审查和举报功能。可以参考5.3.6.1和5.3.6.3两节的内容搭建详细的技术方案。

数据分级分类方案

如各数据合规法规的要求，社交媒体行业在处理个人数据时，需要提供数据分级分类的能力。以下是社交文娱行业可以参考的一张数据分类分级参考表：

分级	类型	示例	管理措施
公开信息 (Public)	用户自愿公开的基本信息	– 头像 – 昵称 – 性别	– 无需特殊管控 – 可自由使用
一般个人信息 (General Personal Information)	– 注册账号信息 – 使用行为记录 – 内容互动记录	– 联系方式 – 兴趣爱好 – 浏览、点赞、评论记录 – 设备信息	– 制定收集、使用、存储政策 – 确保合法合规
敏感个人信息 (Sensitive Personal Information)	– 特殊身份属性信息 – 涉及特殊群体的信息 – 隐私性信息	– 种族、政治倾向、宗教信仰 – 未成年人、残障人士信息 – 健康状况、性取向	– 明确告知用户并获得同意 – 严格限制使用范围
重要个人信息 (Critical Personal Information)	– 财务信息 – 生物特征信息 – 位置轨迹、通讯记录	– 银行账号、支付密码 – 指纹、人脸信息 – 位置轨迹、通讯记录	– 采取加密、脱敏等技术手段 – 严格访问控制

可以参考上述分级分类表，结合5.3.6.1节的技术方案，在WeData中建立专属社交文娱行业的数据分级分类模板与规则。

敏感数据识别与脱敏方案

结合上一小节数据分级分类参考表中关于敏感个人信息和重要个人信息的字段定义，以及5.3.6.1节和5.3.6.4节内容执行社交文娱行业的敏感数据识别与脱敏方案。

游戏 6.3

6.3.1 行业监管概要

总体来说，在数据合规方面全球各国对游戏行业并没有太多比较具备行业特色的监管法规。对于游戏行业企业来说，建议重点关注以下法规：

- 个人信息保护法规：欧盟的GDPR(General Data Protection Regulation)
- 美国各州的隐私法，如加州消费者隐私法(CCPA)
- 中国的个人信息保护法及其他国家和地区的类似法规

此外，由于游戏的玩家很多都是未成年人，因此游戏企业还需要关注：

- 美国的COPPA(Children's Online Privacy Protection Act)
- 欧盟2022年发布的《儿童和年轻人数字权利指南》

这些法规要求游戏公司对收集和使用玩家个人信息进行合法合规管理，如获得玩家同意、限制数据使用范围、实施安全保护措施等。上述法规除了欧盟的《儿童和年轻人数字权利指南》之外，其他法规在上面章节已有相关介绍，此处不再赘述。

《儿童和年轻人数字权利指南》是欧盟在2022年发布的一份针对儿童和青少年数字权利的指引，其中对游戏行业提出了一些具体要求，主要包括：

- **年龄验证和账户管理的要求：**要求游戏公司实施有效的年龄验证机制，确保未成年人无法进入不适合自己年龄段的游戏内容。游戏公司需要为未成年人提供专门的账户管理功能，如设置时间限制、消费限额等。
- **内容适当性的要求：**游戏内容和设计应当与玩家的年龄段适当匹配，不应含有过多暴力、性等不适合的元素，要为不同年龄段的玩家提供相应的游戏内容选择。
- **商业行为规范：**禁止利用心理操纵手段诱导未成年人进行冲动性、过度消费。确保游戏内购买行为的价格和条款信息透明，获得玩家自愿同意。
- **隐私保护限制：**收集未成年人的个人信息，仅获取游戏运营所必需的最少信息。为未成年人提供简单易懂的隐私信息说明。
- **参与和表达：**为儿童和青少年提供合适的沟通渠道，倾听并重视他们的意见。要鼓励游戏公司与家长或监护人进行合作，共同保护未成年人权益。

6.3.2 合规关注要点

数据采集

游戏公司只能收集运营所需的最少个人信息，并获得用户的明确同意。对于儿童和未成年人，需要更加严格的个人信息保护措施，如获得家长同意。制定详细的隐私政策，向玩家充分披露个人信息的收集、使用、保护等情况。

数据存储

首先，需要确保游戏收集的个人数据存储在符合GDPR要求的服务器和存储系统上。采取加密、去标识化等技术措施，提高个人数据的安全性。同时制定数据保留和删除政策，明确不同类型数据的保留期限。为数据接触和使用制定严格的内部管控制度，限制访问权限。

再者，如需将欧盟境内的个人数据传输到第三国存储，需确保目的地国家或组织具有GDPR认可的足够数据保护水平。要采用GDPR认可的数据传输机制，如标准合同条款、绑定公司规则等。确保跨境传输过程中个人数据的安全性和完整性。

其次，游戏公司如使用第三方服务商(如云服务提供商)，需对其数据安全和合规措施进行尽调和评估。游戏公司需要与分包商签订数据处理协议，明确双方在个人数据保护方面的责任和义务，持续监督分包商的数据处理活动，确保其符合GDPR要求。

最后，游戏公司需要制定完善的个人数据泄露事故应急预案，明确各部门的职责和应对流程。定期开展安全漏洞扫描和渗透测试，及时修复存在的安全隐患。一旦发生数据泄露事故，需在72小时内向监管机构报告，并采取补救措施。

数据安全

部分关于数据安全的相关要求已经在上面“数据存储”小节做了介绍，此处再补充两点在数据安全层面的要求。

- **技术安全防护：**企业需要采取加密、匿名化、去标识化等技术手段，提高个人数据的安全性。实施访问控制、权限管理等机制，限制内部人员对个人数据的访问。部署网络防火墙、入侵检测/预防系统等，防范外部攻击。定期进行系统漏洞扫描和渗透测试，及时修复发现的安全隐患。
- **组织安全管理：**制定完善的个人数据安全管理制度和操作规程，明确各部门职责。指定专人负责数据安全工作，建立安全管理组织体系。对员工进行数据安全和隐私保护的培训和教育，提高安全意识。建立数据安全事故应急预案，确保发生问题时能够快速响应和处理。

数据使用

在游戏行业数据使用主要包括以下几个方面，需要游戏公司重点关注和完成以下工作：

- 游戏公司首先在数据采集环节只能出于特定合法目的收集和使用个人数据，不得超出目的范围。然后需要明确界定收集数据的具体用途，如游戏运营、用户分析、广告投放等，确保数据使用与披露给用户的信息一致，不得存在欺骗或误导。
- 数据最小化使用：游戏公司只能收集运营所需的最少个人数据，不得过度收集。对收集的数据进行必要的匿名化或去标识化处理，减少隐私风险。定期评估数据使用需求，及时删除不再需要的个人信息。数据合法性对于个人数据的收集和使用，需获得用户的明确、自愿的同意。对于特殊群体如儿童，需获得家长或监护人的同意。当用户撤回同意或行使删除权时，及时停止使用相关数据。
- 透明度和用户控制：通过隐私政策等方式，向用户充分披露数据使用的情况。确保用户能够了解自己的数据如何被使用，并能够行使相关权利。建立便捷的用户数据访问、修改和删除机制。
- 内部管控：制定明确的数据使用管理制度，规范内部员工的数据使用行为。建立数据使用审批流程，限制仅有必要权限的人员访问。定期评估数据使用情况，识别并纠正不当使用行为。

数据主体行权

同6.2.2.5小节内容。

未成年人保护

请参考6.3.1小节中关于《儿童和年轻人数字权利指南》的内容，以及6.2.2.6小节内容。

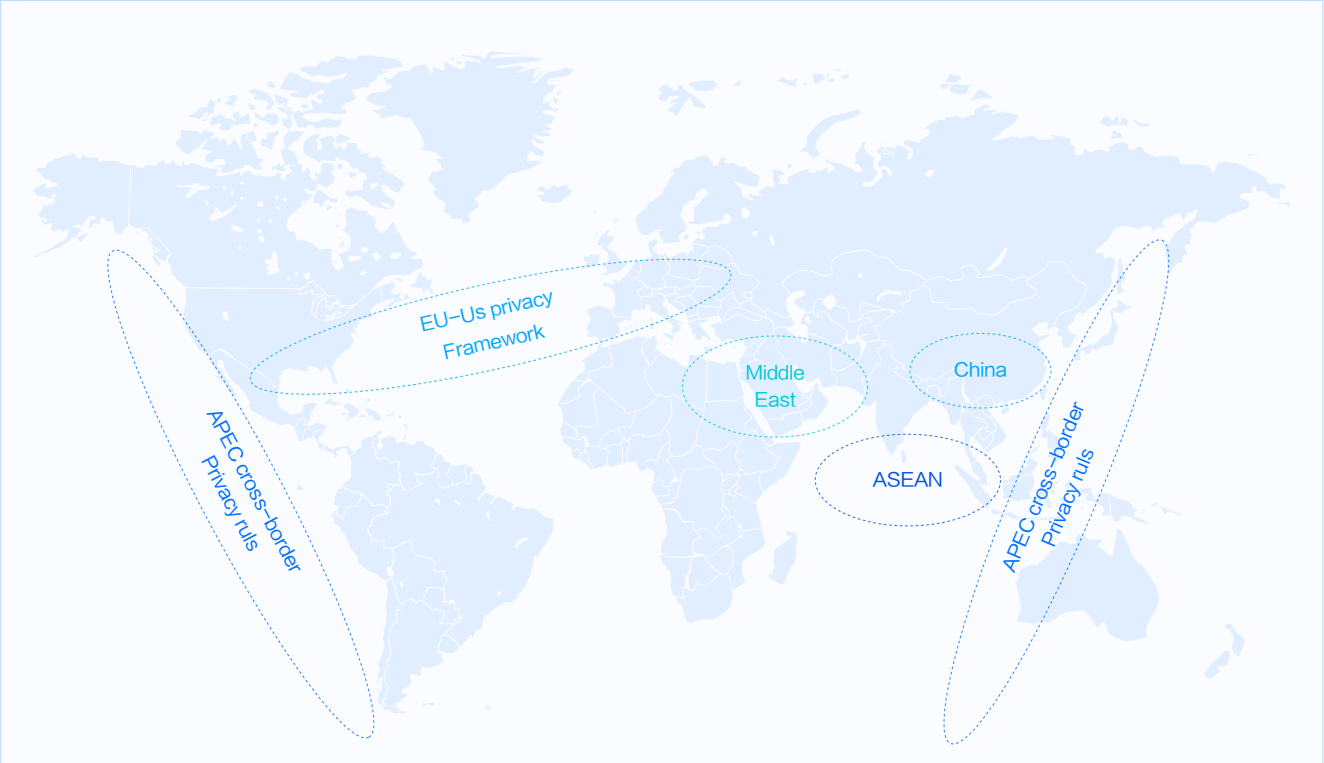
6.3.3 腾讯云合规技术建议

全球合规部署

游戏的IT系统一般会分为战斗/游戏服与平台服两个系统。

游戏服主要负责游戏逻辑的实现和玩家交互，包括游戏世界的渲染、玩家操作的处理等。通常由游戏公司自主研发或者通过第三方游戏引擎供应商提供。主要面向玩家，负责实时响应玩家的游戏操作，提供流畅的游戏体验。游戏服可能采用集群部署、分区部署等方式，以应对大量玩家同时在线的需求。一般游戏服为了较好的用户体验，会就近部署在游戏玩家所在国家/区域。同时，从上述业务类型也可以看出，游戏服中处理的用户敏感个人信息较少，因此在部署时的主要考虑因素就是地理位置决定的时延，数据跨境的约束因素相对较小。

平台服是提供游戏账号管理、支付结算、社交互动等功能的支撑系统。通常由游戏发行商或平台运营商提供，为多款游戏产品提供共享服务。平台服负责管理玩家账号信息、道具购买记录、好友关系等数据。同时，一般来说用于广告营销、用户分析及道具推荐等的大数据系统也属于平台服。从平台服提供的服务类型可以看出，平台服涉及较多的个人敏感数据，数据出镜的约束较多。但又因为平台服在数据一致、部署成本等方面的业务考量，也不太可能分成太多区域分别部署，因此平台服的全球部署架构需要平衡，设计时会复杂些。



如上图所示，根据各国之间签署的数据跨境相关的国际条约，可以按照合规的约束将全球几个主要的数据合规域，在同一个数据合规域中跨境传输个人数据的合规风险相对较低。

- EU-USprivacyframework：成员国有美国及欧盟诸国，此外英国也事实上在满足一定的可以和欧盟、美国互传个人数据；
- APECCBPR：成员国包括美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、中国台北、菲律宾；
- China
- 中东
- 东盟

这意味着，大体上来说，在这些数据合规域内部，可以只部署一个数据中心来支撑此合规域内所有国家的业务，也即意味着游戏的平台服可以在这些区域内只部署一套。而如果游戏客户对于精简架构有更进一步的追求，两个或数个合规域也可以只部署一个数据中心。如某全球知名的中国游戏企业，其全球有两套平台服：中国一套，用来服务大陆的游戏玩家；新加坡一套，用来服务欧盟、美国、东南亚的游戏玩家。

数据分级分类

数据的分级分类几乎是所有涉及大量个人数据的行业做数据合规的标准动作，游戏行业也不例外。以下是游戏行业的数据分级分类参考表：

分级	类型	示例	管理措施
公开信息 (Public)	用户自愿公开的游戏内基本信息	– 游戏昵称 – 游戏头像 – 游戏等级和成就	– 无需特殊管控 – 可自由使用
常规游戏信息 (Regular Game Data)	– 游戏账号信息 – 游戏行为数据 – 游戏内容互动	– 注册信息 – 游戏进度、虚拟资产 – 聊天记录、社交互动	– 制定数据收集、使用、存储政策 – 确保合法合规
敏感个人信息 (Sensitive Personal Information)	– 涉及未成年人的信息 – 涉及支付、交易的信息	– 未成年人账号信息 – 支付账号、充值记录	– 明确告知用户并获得同意 – 严格限制使用范围
重要个人信息 (Critical Personal Information)	– 生物特征信息 – 位置轨迹信息	– 人脸特征、语音生物特征 – 实时位置轨迹	– 采取加密、脱敏等技术手段 – 严格访问控制

制定好数据分级分类表之后，可以参考这样一张表来制定数据分级分类模板。技术方案同6.2.3.2节。

敏感数据识别与脱敏

方案同6.2.3.3节。

汽车 / 出行 6.4

6.4.1 行业监管概要

在欧盟，汽车/出行行业与数据合规密切相关的两个领域是车联网和自动驾驶。欧盟已经出台了一系列数据合规和数据安全相关的重要立法。相比欧盟的系统性法规，其他地区在自动驾驶数据合规方面的监管还比较分散和不完善。

2017 年美国众议院通过了《自动驾驶法案》（Self Drive Act）。该法案第五章要求自动驾驶厂商必须制定网络安全计划，包括如何应对网络攻击、未授权入侵以及虚假或者恶意控制指令等安全策略，用以保护关键的控制、系统和程序，并根据环境的变化对此类系统进行更新，制定内部人员的安全培训和管理制度。此外美国的《联邦隐私法案》等通用法规适用于自动驾驶企业的个人数据处理，部分州如加州、佛罗里达等颁布了自动驾驶测试和商业应用的数据报告要求。

在东南亚，新加坡、马来西亚等国家正在制定自动驾驶相关的数据合规法规，现有的《个人数据保护法》等通用法规适用于自动驾驶企业的数据管理，一些其他东南亚国家正在鼓励自动驾驶企业采用自愿性的行业标准和指南。所以本章节关于出行行业数据合规的解读仍以欧盟的法规体系展开。

欧盟在汽车/出行行业的数据合规相关立法主要包括以下几个：

一般数据保护条例(GDPR)

要求自动驾驶企业对收集的个人数据进行合法、透明的处理。用户拥有数据访问、删除等权利，企业需要做好用户授权和隐私通知。对于敏感个人数据的处理需要采取更加严格的保护措施。关于GDPR之前章节已有较详细的阐述，此处不再赘述。

但需要关注的是欧盟数据保护委员会（EDPB）在GDPR规范的个人数据保护框架下发布的《在联网车辆和出行相关应用环境下处理个人数据的指南》，一般简称《车联网个人数据保护指南》，其内容要点如下：

- **适用范围**：该指南适用于车载系统和相关服务中涉及个人数据的处理活动。
- **数据最小化**：车载系统及服务应只收集和处理与预定目的相关的必要个人数据。
- **透明度和信息提供**：需要向用户清晰透明地告知数据收集、处理的目的和方式。
- **数据访问和控制**：用户应能访问和控制自己的个人数据，如查阅、更正和删除。
- **安全性**：要采取适当的技术和组织措施保护个人数据免受未经授权的访问、披露等。
- **隐私by design**：在设计和开发车载系统时，就应融入数据保护和隐私保护的考量。
- **第三方共享**：对于向第三方共享个人数据的情况，需要征得用户同意并做好安全保护。

紧急救援呼叫系统(eCall)法案要求

欧盟的eCall（European Emergency Call）系统是一种车载紧急呼救系统，它是汽车行驶安全所必需的一套系统，属于车联网系统的一部分。

- **数据收集范围**：eCall系统仅可收集发生事故时所需的最小必要数据，包括车辆位置、时间、车速等。禁止收集车载系统中其他不相关的个人数据，如通话记录、浏览历史等。
- **数据存储和使用**：eCall系统必须确保收集的数据仅用于紧急呼救响应，不能用于其他目的。数据必须在紧急呼救结束后自动删除，最长保存时间不超过30秒。
- **数据隐私保护**：eCall系统必须采取加密等技术手段，确保数据在传输和存储过程中的安全性。只有在紧急情况下，才允许相关救援机构访问eCall系统收集的数据。
- **用户知情同意**：车载eCall系统必须向用户明确告知数据收集的目的和范围。用户可以选择是否激活eCall系统，以行使对个人数据的控制权。
- **第三方访问限制**：禁止车载系统制造商或其他第三方未经用户同意访问eCall系统的数据。只有在用户明确授权或紧急情况下，救援机构才能获取相关数据。

人工智能法案(AI Act)

欧盟人工智能法（AI Act）是全球首个以立法方式对人工智能（AI）进行监管的法律，旨在保障欧盟公民的基本权利并激励欧洲AI的投资与创新。在汽车/出行领域，它尤其适用于自动驾驶的场景，其内容要点如下：

- **数据收集和处理要求**：自动驾驶系统仅收集实现其功能所必需的个人数据，不得收集多余数据，数据处理必须符合GDPR等隐私法规，确保数据被安全和合法地使用。
- **数据共享和访问**：鼓励车联网参与方之间建立标准化的数据共享机制，促进跨系统间的数据互通，AI　Act明确规定政府监管部门可以在必要时获取相关数据，但需要遵守数据最小化原则。
- **数据安全和隐私保护**：要求车载人工智能系统必须采取加密、匿名化等技术手段，确保数据安全。同时制定用户知情同意、数据最少收集等数据隐私保护规范。
- **算法偏差和歧视防范**：规定训练自动驾驶算法时必须考虑多样性数据，避免算法产生性别、种族等偏差。要求定期评估算法的公平性表现，并采取纠正措施。
- **数据治理和责任**：认定要求车联网参与方建立健全的数据治理机制，明确数据责任和风险管控。对于数据滥用或未经授权访问等行为，规定相应的监管措施和罚则。

由此可见，AI Act对自动驾驶等“高风险"AI系统的数据管理提出了更高要求。需要进行算法审计，并确保系统的可解释性和公平性。

网络安全法案(NIS2)

NIS2要求自动驾驶企业建立健全的网络安全管理体系，实施数据备份、入侵检测、事故响应等安全防护措施。整体上这些要求与6.3.1.1部分NIS针对社交文娱行业的要求是类似的。但由于车联网和自动驾驶不仅包括云端的平台，也包括汽车座舱内的数据安全与数据合规。因此如何将这些要求落实到车舱本地环境中将会是具有一定行业属性的要求。

- **数据收集原则**：NIS2要求车载系统只能收集实现功能所需的最小必要数据，这对座舱内的各类传感器采集数据提出了限制，必须遵守数据最小化原则。
- **用户授权和知情**：座舱内数据的收集和使用必须得到用户的明确授权，同时要向用户透明地告知数据的具体用途和处理方式。
  数据加密和保护：NIS2规定车载系统中的所有敏感数据都必须采取加密保护，这适用于座舱内的语音、影像等个人隐私数据。
- **访问控制管理**：对座舱内数据的访问和操作要实行严格的权限管控，只有经过身份认证的正授权人员才能访问相关数据和功能。
  第三方数据共享：NIS2鼓励车企与第三方建立安全标准化的数据共享机制，但共享座舱内数据须得到用户授权，并确保数据安全。
- **事故响应和通报**：一旦座舱内数据发生泄露或安全事故，要在规定时间内向监管部门报告。同时还需要采取补救措施，并通知受影响的用户。
- **第三方管理**：涉及座舱内数据的外包服务商，也需要纳入NIS2合规评估。确保其安全能力和隐私保护水平符合监管要求。

6.4.2 合规关注要点

车联网和自动驾驶涉及的数据有着多样性、规模性、非结构性、敏感性等特点。

这两个场景涉及的数据类别不仅包括了汽车基础数据（车牌号、车辆品牌和型号、车辆识别码、车辆颜色、车身长度和宽度外观等相关数据），还包括了基础设施、交通数据、地图数据（红绿灯、道路硬件、道路行人、行驶方向、运动轨迹、街景、各类交通标志、建筑物外观等真实交通数据），以及车主的大量用户身份类数据（姓名、手机号码、驾照、证件号码、支付信息、家庭住址、声音、声纹、指纹、脸部信息等生物特征识别信息等）、用户状态数据（语音、手势、眼球位置变化等）、行为类数据（登录、浏览、搜索、交易等操作信息等）等数据。

此外车联网数据融合了来自汽车、道路、天气、用户、车载计算系统等多方面的海量数据（结构化数据+非结构化数据），涉及数据类型多，规模大，涉及众多数据处理主体，如智能网联汽车生产企业、车联网服务平台运营企业等，并且随着用户的增加，数据呈指数级增长态势，需要统计分析应用的数据总量大。

上述特点给数据合规造成了巨大的挑战。

数据采集、传输与存储

根据《车联网个人数据保护指南》的内容，可以将汽车采集数据分为车外数据、座舱数据、运行数据和位置轨迹数据。其中车外数据可能包含个人信息、敏感个人信息和重要数据；座舱数据可能包含敏感个人信息。

在数据传输方面，除符合例外情形或经个人信息主体单独同意，不得通过网络向外传输包含未匿名化处理个人信息的车外数据、座舱数据。汽车和设备制造商、服务提供商和其他数据控制者应当尽量使用不涉及个人数据或不涉及传输个人数据到车外的流程（例如，数据在内部进行处理）。

在数据出境方面，车外数据、座舱数据、位置轨迹数据不应出境，运行数据出境前应通过数据出境安全评估。

在数据存储方面，有着较为严格和特殊的要求，如：

- 除非符合例外情形，否则车外数据、位置轨迹数据在车外位置保存时间不应超过14天。
- 用户必须对存储在第三方平台上的数据有处置的权力，例如有权删除存储在汽车维修店或经销商系统中的其个人数据的能力。
- 应该在车辆内部安装用户配置文件管理系统，以便存储已知驾驶员的偏好并帮助他们随时轻松地更改其隐私设置。
- 生物识别模板/模型存储在车辆内，以加密的方式，使用最先进的密码算法和钥匙管理。
- 对构成生物识别模板和用于用户验证的原始数据进行实时处理，即使在本地也不对其进行存储。

合规左移与默认设计

"by design"的理念是指在系统或产品的设计和开发过程中，就将数据保护和隐私保护的要求纳入考虑，从根本上确保隐私和安全得到充分保障。这意味着安全与合规设计的左移。

在诸多其他行业，如教育、文娱、游戏等，by design是一项指导，并没有那么迫切的要求。但在车联网与自动驾驶的场景中，de design近乎是一项强制要求。这主要是因为涉及的数据的敏感性和私密性导致的，同时也因为诸多数据只能车内处理，不能出座舱，因此在云-端协同的过程中需要充分考虑数据在云端和车端的分别处理与协同。而又因为自动驾驶等场景涉及座舱内人员的生命安全，而自动驾驶与车联网的联网性质又不可避免面临远程攻击、内部设备入侵、数据窃取等威胁，因此无论是车端还是云端，对于数据安全、联网安全的能力要by design，从一开始开发系统的时候就要尽量考虑周全。举例如下：

- 当远程存储时，使用最先进的算法对数据进行加密。
- 默认保留汽车的访问日志至少6个月，以便于对攻击进行溯源和分析。
- 所有个人数据或敏感数据的存储应默认设定存储时间周期。
- 技术设计默认应以最小化个人数据的收集。
- 提供保护隐私的默认设置和确保数据主体得到充分告知，并且可以选择以简易的方式修改与其个人数据相关的配置为目的。
- 只有对于车辆运行所必需的数据才能被默认处理。
- 将瞬时速度有关的数据和地理位置数据默认分别存储在单独的数据库中（例如，使用具有不同密钥和批准机制的先进的加密机制）。
- 对于任一其他目的和控制者/处理者，数据主体都默认应可以激活或停用该数据处理， 并且可以删除有关数据。
- 使用基于个人数据处理或处理个人数据以完成任务的应用、服务和产品时，产品、服务和应用的制造商在开发和设计该类产品、服务和应用时需要默认把数据保护权利纳入考虑，并适当考虑先进技术，确保控制者和处理者能够履行其数据保护义务，保障数据安全。

数据脱敏要求

数据脱敏的要求至少在下述两个场景中是刚性的：

- **周围环境数据进入汽车**：自动驾驶车辆所收集的周围环境数据中涉及其他人的个人信息，如行人、其他车辆的车牌号等，在进入车载系统之前需要进行脱敏处理。
- **个人数据离开车辆**：车联网与自动驾驶相关的个人数据被要求尽量本地处理，此处的本地处理是指在车内处理。如果数据必须离开车辆，则应考虑在传输之前将其匿名化。GDPR不适用于匿名信息，即无法关联到已识别或可识别的自然人的信息， 或使数据主体无法被识别的匿名化的个人数据。

OTA场景

OTA全称“Over the Air"，指通过移动或无线网络提供空中接口，实现远程下载应用程序、服务和配置的能力。在软件定义汽车的大语境下，车联网、自动驾驶成为行业趋势，OTA在汽车行业尤其是新能源汽车中的渗透进一步加深。OTA场景的数据合规、数据安全就成为从业者需要重点关注的对象。重点以下几个OTA的功能场景中：

- **软件发布安全**

  提供OTA升级功能的汽车厂商需要建立OTA升级管理能力，能提供在线升级进行安全影响评估、测试验证、实施过程保障、信息记录等能力，确保车辆进行在线升级时处于安全状态，并向车辆用户告知在线升级的目的、内容、所需时长、注意事项、升级结果等信息。

- **内容推送**

  用OTA推送内容，如娱乐、导航、人车交互等功能的更新，以及涉及汽车的核心系统以及行驶功能的智能刹车、自动化驾驶等更新。后者是监管的重点。真正的自动驾驶功能（SAE 3 级以上）开发必须遵循迭代过程，在完全验证并获得必要的监管许可或批准之前，任何此类功能都不会向公众发布。未经验证或审批，不得通过在线等软件升级方式新增或更新汽车自动驾驶功能。

- **用户授权**

  通过OTA推送订阅功能并收取费用的车企，不得采用一次概括授权、默认授权、与其他授权捆绑、停止安装使用等方式，强迫或者变相强迫消费者同意收集、使用与经营活动无直接关系的信息。在自动展期、自动续费等日期前，应以显著方式提请消费者注意，由消费者进行选择。在服务期间内，应当为消费者提供显著、简便的随时取消或者变更的选项，且不得收取不合理费用。

- **电子商务与营销**

  “用户画像"与“精准推荐"是互联网营销中常见的策略。对于车企而言，遍布全车的各类传感器可以收集丰富的数据，这些数据在导入AI驱动的机器学习模型后，可以自动、批量对车主的使用习惯做出更加精准的画像，推送相应订阅解锁功能，从而提高商业转化率。个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇；通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

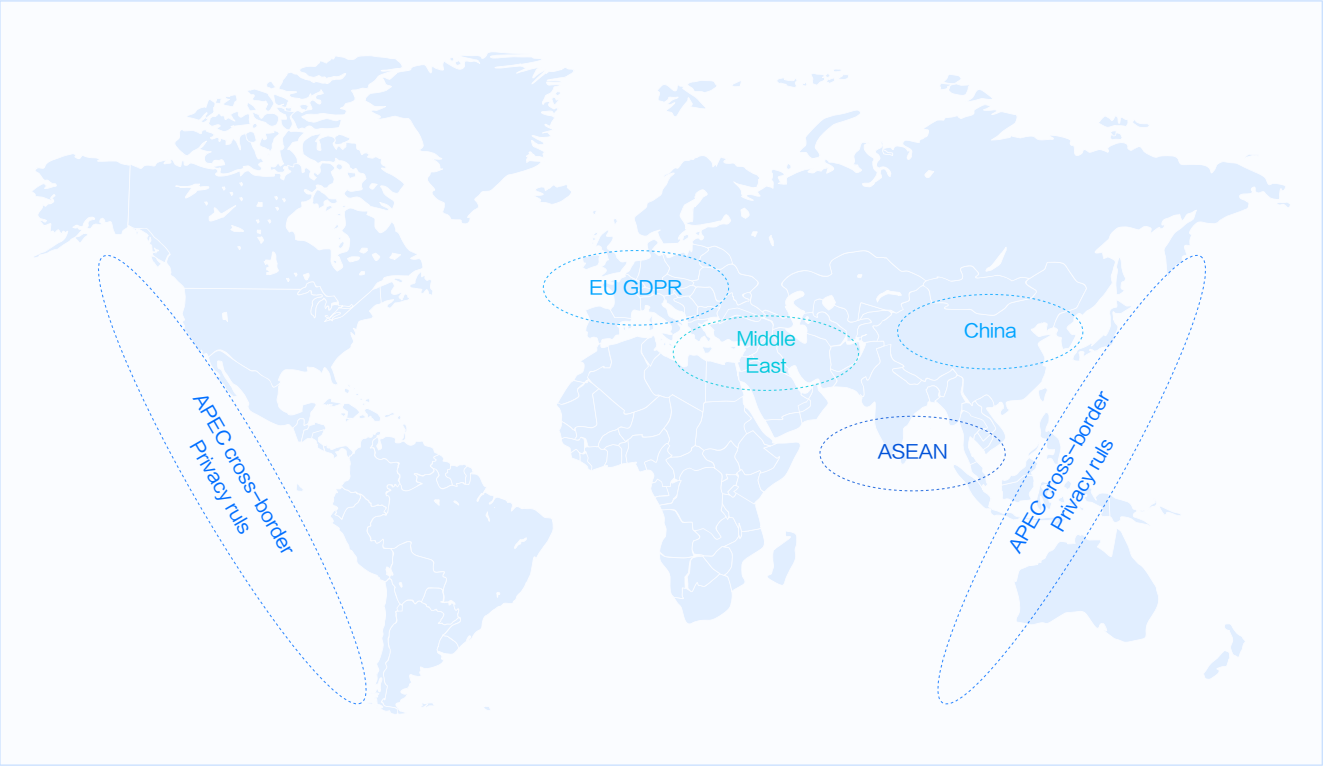
- **召回场景**

  OTA为修补部分汽车软件故障提供了便捷方案，但如存在硬件缺陷时不可使用OTA的方式代替传统召回。使用OTA对存在问题的硬件施加使用限制，则可能会造成更严重的市场反弹和监管关切。

6.4.3 腾讯云合规技术建议

全球部署

如同游戏平台服的全球合规部署架构（详见6.3.3.1节内容），车联网与自动驾驶平台在全球部署时会面临同样的约束，但显然由于平台收集、处理的敏感性，在本地化部署方面需要更多的倾斜和关注。因此我们调整游戏全球部署的合规与架构，如下图所示：



- 欧盟相关的业务推荐欧盟境内部署。
- APEC CBPR协议圈国家可以集中部署一套，如果对精简架构有要求，可以同一套架构再覆盖东南亚诸国。
- 中东国家集中部署一套。

数据采集与过滤

如6.6.2节所述的合规关注点，企业需要在汽车对周围环境进行采集的时候就需要进行过滤与脱敏，将道路上行人的个人数据（如人脸、车牌号等）进行过滤或脱敏才能进入车联网系统。此外，汽车座舱内采集的个人数据（如指纹、声纹、精确而密集采样的位置信息、驾驶员人脸、驾驶员行为习惯数据以及如血压、呼吸、心率等健康相关数据）也需要过滤或脱敏之后才能传往车外。

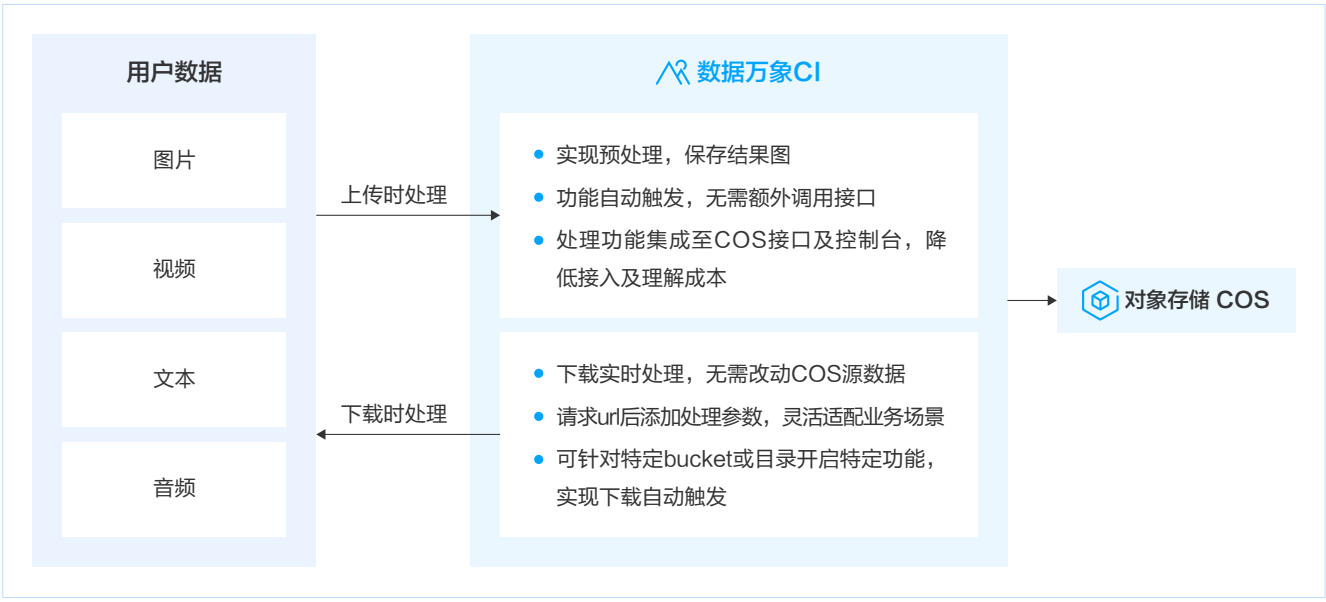
由于此时的算力承载是在车端，而不是云端，因此云端的诸多数据安全、数据合规的产品和方案都无法应用。目前能够在车端部署的腾讯云相关产品还较少。主要还要依赖于车端开发人员的能力。

腾讯云建议出海车企可以按照以下规则来对数据进行分级分类：

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

如果数据传到了云端，那就需要在云端对数据进行脱敏。这方面腾讯云的技术方案比较丰富。

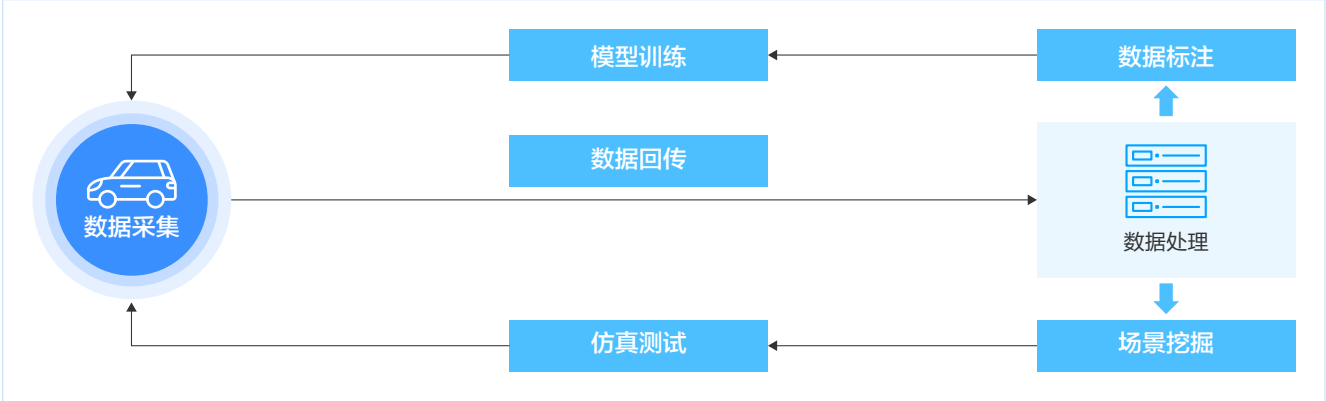
- 可以使用腾讯云数据脱敏解决方案，开箱即用，适合企业内部数据迁移与外部数据共享的场景。主要用于数据库中数据外发时的数据脱敏，详细信息可以参考5.3.1.4节“数据脱敏”的内容。
- 在大数据体系中也提供了数据脱敏的能力，详见5.3.6.4节的内容。
- 对于进出对象存储的数据和内容脱敏，可以使用腾讯云对象存储的数据处理方案。



数据标注与模型训练

数据标注与模型训练和数据合规息息相关。数据标注时，可以参考汽车行业数据分级分类的指导矩阵，从合规角度对数据进一步打标，从而可以使系统对高敏感数据做更妥善的处理，降低后续环节的合规风险。

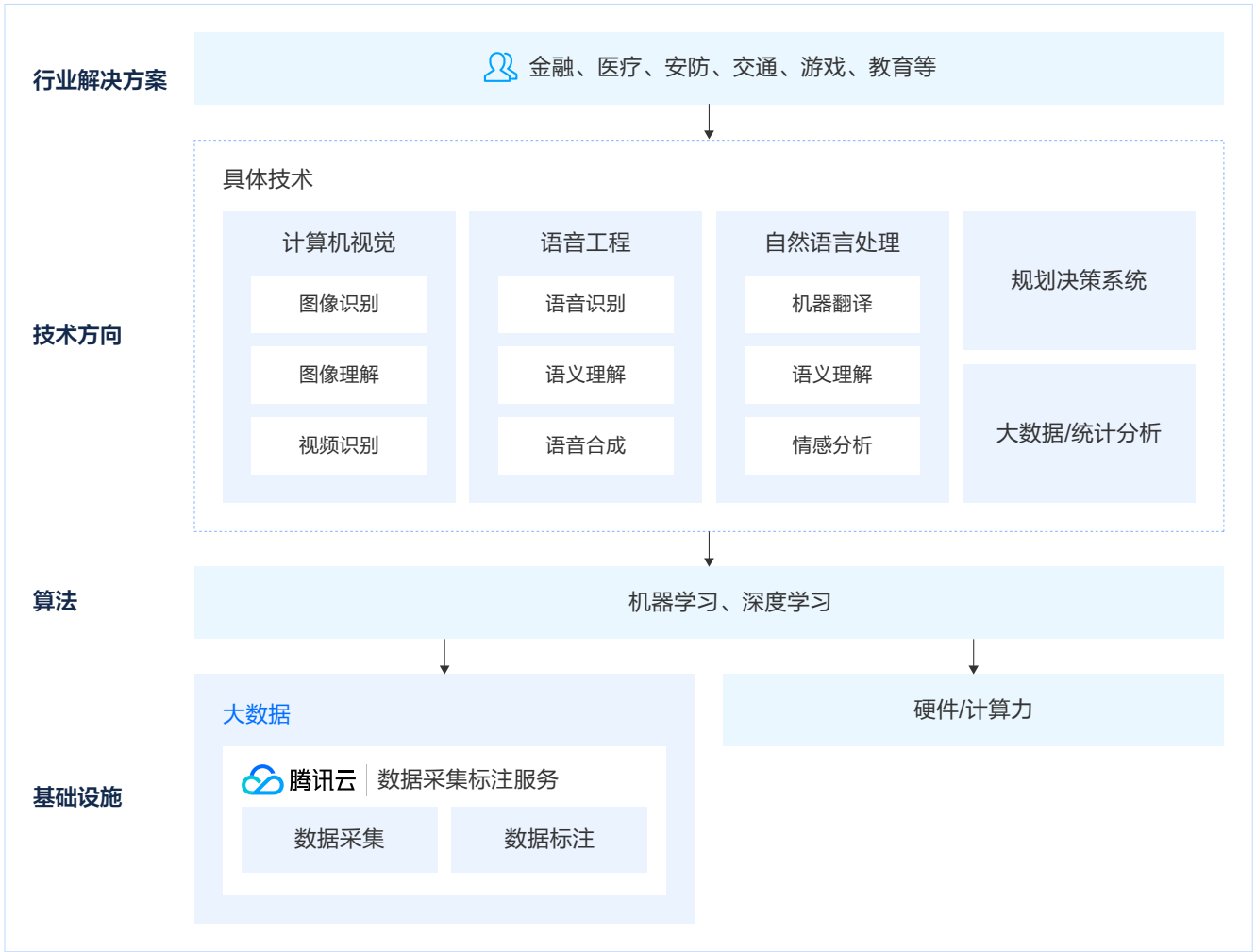
如下图所示，可以在云端进行的数据任务是数据标注与模型训练、仿真测试。仿真测试后面章节再展开，本小节主要介绍腾讯云数据标注与仿真测试解决方案。



关于数据标注，可以使用腾讯云的数据采集与标注解决方案。它基于智能化采集标注工具和成熟的数据服务体系，提供专业的数据采集和标注服务，高效交付高质量目标数据，帮助AI业务能力的快速提升。在数据标注环节，可以充分考虑当地数据合规的差异化要求对数据进行标注。

数据采集时可以针对客户的目标场景补充训练和评测数据，完成 AI 业务能的定向训练和优化。数据标注时，可以通过自动化处理能力和海量标注人力，帮助用户解决大量数据需要加工和标注的场景，让用户快速获取到加工后的目标数据。

官网介绍：https://cloud.tencent.com/solution/data-collect-and-label-service



在模型训练方面，可以使用腾讯云TI-ONE训练平台。TI-ONE 训练平台（以下简称TI-ONE）是为 AI 工程师打造的一站式机器学习平台，为用户提供从数据接入、模型训练、模型管理到模型服务的全流程开发支持。TI-ONE 支持多种训练方式和算法框架，满足不同 AI 应用场景的需求。

车联网移动应用安全方案

腾讯云移动应用安全（Mobile Application Security，MS）针对移动应用普遍存在的破解、篡改、重打包等各类安全风险，提供Android应用加固、iOS源码混淆、SDK加固等多种加固技术，拥有丰富的行业经验，已服务于金融、互联网、车联网、物联网，运营商等多个行业。稳定、简单、有效，让移动安全建设不再是一种负担。

它可以对敏感数据信息、核心算法逻辑、版本内容等需要进行保护，移动应用安全推出的安全加固支持本地资源加密，有效防止攻击者窃取用户敏感数据。



教育 6.5

6.5.1 行业监管概要

欧盟

- 通用数据保护条例（GDPR）：要求教育科技公司在处理个人数据时必须确保数据的安全性和隐私性，包括数据主体的访问权、更正权、删除权等。
- 儿童在线隐私保护法规：对于针对儿童的服务，需要获得家长同意，并采取更严格的数据保护措施。
- 电子隐私指令：保护用户的通信隐私，包括电子通信服务。
- 版权法：保护原创作品，教育科技公司在提供内容时必须确保不侵犯版权。
- 消费者保护法规：要求教育科技公司提供透明的服务条款和退款政策。

北美

- 美国儿童在线隐私保护法案（COPPA）：针对13岁以下儿童的在线服务，要求在收集、使用或披露儿童个人信息前必须获得父母的同意。
- 家庭教育权利和隐私法案（FERPA）：规定教育机构在处理学生教育记录时的隐私权和保护措施。
- 加州消费者隐私法案（CCPA）：提供加州居民更多关于其个人信息的控制权，包括访问、删除和拒绝出售个人信息的权利。
- 家庭教育权利和隐私法案（FERPA）：保护学生的教育记录和个人信息不被未经授权的披露。
- 学生在线个人隐私权法案（SOPIPA）：要求在线服务提供商在收集学生个人信息前必须获得同意。

东南亚

- 新加坡个人数据保护法（PDPA）：规定了个人数据处理的基本原则和要求，包括同意、访问和更正权。
- 马来西亚个人数据保护法（PDPA）：类似新加坡，马来西亚也有PDPA，旨在保护个人数据不被滥用。
- 印度尼西亚个人信息保护法：规定了数据收集、处理和存储的规则，以及数据主体的权利。
- 泰国个人数据保护法（PDPA）：从2022年起生效，要求组织在处理个人数据时必须遵守特定的数据保护原则。
- 菲律宾数据隐私法（DPA）：规定了数据保护的规则和数据主体的权利。
- 越南网络安全法：包括对个人信息的保护要求，要求在越南境内处理的数据必须遵守当地法律。

中东国家

- 沙特阿拉伯的数据保护法规：沙特阿拉伯的《个人数据保护法》要求企业在收集和处理个人数据时必须遵守特定的数据保护原则。
- 阿联酋的网络安全法：规定了网络安全和数据保护的要求，包括对个人信息的保护。
- 卡塔尔的数据保护法：保护个人数据不被未经授权的访问、使用或泄露。
- 科威特的数据保护法规：要求企业在处理个人数据时必须遵守数据保护法规，包括数据的收集、存储和传输。

6.5.2 合规关注要点

- **数据保护和隐私**：教育出海企业由于需要全球适配不同国家政策要求，需要遵守目标国家的个人数据保护法规，如欧盟的GDPR、美国的CCPA等。
- **儿童在线隐私**：面向儿童提供的课程及产品服务过程中可能会涉及儿童数据采集，针对个人敏感数据，需遵守COPPA（美国）或类似针对儿童在线隐私的法律。
- **知识产权**：教育内容类服务企业可能涉及知识内容的生产研发，将会存在内容借鉴二次加工的情况，在内容生产过程中确保不侵犯第三方的版权、商标、专利等知识产权。
- **内容审查**：面向一些属地国进行产品服务交付过程中可能存在不同区域禁忌内容的审核，遵守当地关于内容审查的法律，确保内容不违反当地文化、宗教或政治禁忌。
- **教育资质认证**：在提供线下或线下教育培训过程中涉及教师授课场景，针对招聘的国内及国外教师和教研内容，需要获取当地教育部门或专业机构的认证，证明产品和服务符合教育标准。
- **广告和营销法规**：在面向家长和潜在付费的教育用户群体进行市场营销过程中，遵守当地关于在线广告和营销的法律法规，特别是针对未成年人的广告限制。
- **消费者权益保护**：提供透明的服务条款、隐私政策和用户协议，确保消费者知情权，不可叠加潜在差异性收费服务条款。
- **产品安全**：授课教学过程中同步提供硬件及相关教学教具的场景下，确保产品符合当地安全标准，特别是儿童使用的产品。
- **跨境数据传输**：确保跨境数据传输符合目标国家的数据保护要求。
- **教育内容和质量**：遵守当地教育内容和质量标准，确保产品和服务的教育价值。

6.5.3 腾讯云合规技术建议

全球化部署

国家层面已经有比较明确的数据隐私保护法规和政策要求，因此在数据层面需要做好当地数据库存储用户敏感数据和部分当地授课过程数据，是需要通过独立站的设置解决数据本地化处理和服务的能力搭建，腾讯云全球主要国家的本地机房覆盖及内容分发网络的建设可以满足客户全球化部署的需求。

内容审核

针对青少年授课的教研内容需要进行严格审核检查，腾讯云具备内容审核方案，包括数据脱敏处理、敏感数据筛选告警、违规数据的监测和识别，尤其是涉及版权保护、内容防盗也有较为完善的保护溯源方案。

数据安全及跨境传输

现有出海客户在数据收集层面需要提前做好客户授权，腾讯可以提供网络安全、数据安全的产品服务，包括但不限于教学授课中涉及到的相关过程性数据的分权分域管理，针对图像和视频内容采集端的安全防渗透措施方案；另外在跨境数据传输过程中避免敏感数据回流到中国产生的监管敞口风险，腾讯可以提供数据库级别的过程管理，如各国本地数据处理的日志备份，防止监管过程中产生的纠纷。

金融服务 6.6

6.6.1 行业监管概要

随着信息技术的飞速进步，金融行业在开展传统信贷业务、资金业务等业务过程中均产生大量的数据，伴随着大数据、人工智能等前沿技术的深度融合，进一步凸显了金融数据在推动行业创新、优化服务、提升效率中的核心价值。在海外金融监管方面，数据合规是一个日益重要的议题。不同国家和地区都有各自的法规和监管机构来确保数据的安全和合规性，建议重点关注数据跨境传输及个人信息保护相关的法律法规。此外，在金融行业中，客户不仅是金融服务的接受者，更是金融产品和服务的最终使用者与体验者，所以应该重点关注消费者权益保护的相关法律法规。下面选取欧盟、美国、中国为例进行分析。

欧盟

在欧盟（EU），金融行业受到一系列严格的监管条规的约束，以确保市场的稳定性、消费者保护和数据安全。建议重点关注下述法律法规：

- **通用数据保护条例（GDPR）**

  GDPR 是一项强制性法律，适用于所有在欧盟境内处理个人数据的组织。它规定了数据处理的严格规则，包括数据主体的权利、数据保护影响评估（DPIA）、数据泄露通知要求等。

- **支付服务指令（PSD2）**

  PSD2 旨在促进支付服务的创新，同时确保支付数据的安全和保护消费者。它引入了强客户认证（SCA）的要求，并允许第三方提供商在获得用户同意的情况下访问支付账户信息。

- **欧洲市场基础设施法规（EMIR）**

  EMIR 要求某些金融衍生品交易必须通过中央对手方清算，以降低系统性风险。它还规定了交易数据的报告和存储要求。

- **证券融资交易条例（SFTR）**

  SFTR 旨在提高证券融资交易的透明度，包括回购和证券借贷交易。它要求交易双方报告交易数据到授权的交易数据库。

- **银行复苏和清算指令（BRRD）**

  BRRD 规定了银行在面临财务困境时的复苏和清算程序。它要求银行制定和维护恢复计划，其中可能涉及数据管理和信息系统的连续性。

- **反洗钱指令（AMLD）**

  欧盟的反洗钱指令要求金融机构进行客户尽职调查（CDD）和持续监控，以防止洗钱和恐怖融资。这包括对客户数据的收集、处理和存储。

- **电子身份、信托服务和电子签名条例（eIDAS）**

  eIDAS 旨在促进跨境电子身份验证和信任服务，确保电子交易的安全性和有效性。它规定了电子签名和电子印章的法律效力。

- **网络安全法案（NIS Directive）**

  NIS 指令要求关键基础设施运营商，包括金融服务提供商，采取适当的技术和组织措施来保护其网络和信息系统免受攻击。

这些法规和指令对金融机构的数据管理和处理提出了高标准的要求，以确保数据安全、保护消费者权益，并促进金融行业的整体稳定和信任。金融机构在欧盟运营时必须遵守这些规定，否则可能面临重大的法律和财务后果。

美国

在美国，金融行业受到联邦和州级监管机构的严格监管，以确保市场的完整性、消费者保护和数据安全。以下是一些与数据相关的主要金融监管条规。这些法规和规则要求金融机构采取适当的数据保护措施，确保数据的安全性和隐私性，同时遵守严格的报告和记录保存要求。金融机构必须遵守这些规定，以避免法律后果和罚款。建议重点关注下述法律法规：

- **格拉姆-里奇-布莱利法案 (Gramm-Leach-Bliley Act, GLBA)**：也称为金融现代化法案，GLBA 要求金融机构保护消费者金融信息的隐私和安全。它引入了消费者隐私通知和选择权，以及数据安全计划的要求。
- **多德-弗兰克法案（Dodd-Frank Wall Street Reform and Consumer Protection Act）**：多德-弗兰克法案旨在改革金融市场，提高透明度和消费者保护。它包括对数据收集、报告和共享的新要求，特别是在衍生品市场和消费者金融保护局（CFPB）的监管下。
- **加州消费者隐私法案 (CCPA)**：虽然这是一项州级法律，但鉴于加州庞大的经济体量，CCPA 对许多在美国运营的公司都有影响。它赋予消费者对个人信息的控制权，包括访问、删除和了解其数据如何被商业使用的权利。
- **证券交易委员会（Securities and Exchange Commission, SEC）规则**：SEC 制定了许多规则来规范证券市场，包括数据报告、记录保存和网络安全。例如，SEC 规则17a-4要求经纪公司和交易所成员保留电子记录，并采取适当的措施保护这些记录。
- **健康保险流通与责任法案（Health Insurance Portability and Accountability Act, HIPAA）**：虽然 HIPAA 主要关注医疗保健行业，但它也包含了对健康信息的隐私和安全保护的规定，这些规定可能适用于提供健康保险产品的金融机构。
- **国家安全与个人数据保护法提案 （NSPDPA)**：提出了对特定国家的数据传输限制，要求受管辖科技公司遵循数据最小化原则，禁止次级利用用户数据，提供用户删除权及访问权，限制数据传输，以及要求数据存储在美国境内 。

中国

中国数据安全合规监管要求严格且全面，旨在保护国家安全、公共利益以及个人和组织的合法权益，中国数据安全合规监管要求不仅涉及技术层面的安全保障，还强调法律法规的遵守和社会伦理的尊重，体现了国家对于数据安全的全面和深入考量。建议重点关注下述法律法规：

- **《中华人民共和国数据安全法》**：是针对数据安全具体工作的要求，如对数据实行分类分级保护、建立健全全流程和数据安全管理制度、明确重要数据负责人和管理机构、安全事件应急方案、风险评估、数据全生命周期安全等。明确数据要素市场化前需要溯源清晰等限制。为此数据安全体系的管理活动提供支持。
- **《中华人民共和国个人信息保护法》**：强调了信息处理者对数据的“保护”义务。指出：“处理个人信息应当具有明确、合理的目的,并应当限于实现处理目的的最小范围,不得进行与处理目的无关的个人信息处理。”和“处理个人信息应当遵循公开、透明的原则，明示个人信息处理规则。”归纳为要求数据采集应满足“最小够用”、“公开透明”、“有针对性”等原则。
- **《中国人民银行金融消费者权益保护实施办法》**：明确金融行业与国家法律法规之间的关系。定义金融消费者为消费自然人。明确金融信息包括：个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。
- **《个人信息出境安全评估办法》**：对个人信息出境前的申请流程和评估流程做出规定。聚焦跨境流动中的个人信息保护，突出对个人信息主体的权益保障：一方面是增加了个人信息主体的权利范围。规定个人信息主体是网络运营者与个人信息接收者签订的合同或者其他有法律效力文件的受益人，有权查询合同副本、更正或删除个人信息，并可举报违法行为并要求赔偿，从多个方面保障了信息主体对于其个人信息出境情况的知情权、访问权、更正及删除权以及救济权。另一方面是增加了个人信息主体的权利权限。对数据出境后的再次传输作出了规定，要求网络运营者将个人信息接收的第三方相关信息通知到个人信息主体，个人信息主体有权继续或终止数据的传输，极大地增加了个人信息主体对于维护其合法权益的权限。
- **《金融数据安全 数据安全分级指南》**：规定了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程，建立统一、完善的数据生命周期安全保护框架的基础工作，为金融业机构开展数据安全分级工作提供指导。
- **《金融数据安全 数据生命周期安全规范》**：针对金融行业数据安全的一项重要规范，其内容主要围绕金融数据在生命周期各阶段（数据采集、数据传输、数据存储、数据使用、数据删除、数据销毁）的安全管理要求。
- **《个人金融信息保护技术规范》**：规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

6.6.2 合规关注要点

金融数据安全评估

金融数据安全评估的重要性不言而喻，它是维护金融系统稳定、保障客户资金安全、以及促进金融行业健康发展的基石。金融企业/机构需要评估数据收集、存储、处理、传输等全生命周期的安全性，确保各个环节均符合相关法律法规和行业标准；其次，对金融企业/机构的信息系统进行渗透测试和安全审计，发现潜在的安全漏洞和弱点，并提出针对性的改进建议；同时，还需要对金融企业/机构的数据加密、访问控制、身份认证等安全机制的有效性进行评估，确保其能够有效防范内外部威胁；最后，根据评估结果，制定并实施相应的安全策略和措施，持续改进和优化金融数据的安全防护体系。因此，对金融数据进行全面、深入的安全评估，是预防数据泄露、抵御网络攻击、满足监管要求、以及提升整体风险管理水平的关键环节。

数据安全分类分级

金融数据安全分类分级的重要性在于它为金融企业/机构提供了一套科学、合理的数据保护框架，有助于精准识别不同类别、不同级别数据的敏感性和风险程度，从而实施差异化、精细化的安全管理和防护措施。金融企业/机构需要明确分类分级的标准和原则，根据数据的敏感性、重要性和潜在影响等因素，将数据划分为不同的类别和级别，并对金融企业/机构内部的数据进行全面梳理和分类，确保每一类数据都能得到准确、清晰的界定；进而，针对不同类别、不同级别的数据，制定相应的安全保护策略和控制措施，如加密存储、访问控制、数据脱敏、审计跟踪等；此外，建立健全的数据分类分级管理制度和流程，确保分类分级的准确性和时效性，同时加强对制度执行情况的监督和检查，确保各项安全措施得到有效落实。因此对数据开展分类分级可以提升金融数据的安全防护水平，降低数据泄露和滥用的风险，还能够优化资源配置，提高安全管理的效率和效果。

个人信息及隐私保护

金融行业个人信息及隐私保护的重要性在于维护客户权益、建立信任关系以及确保行业的可持续发展。随着金融业务的数字化和互联网化，个人信息的收集、处理、存储和共享变得日益普遍，但同时也带来了更高的隐私泄露风险。保护客户个人信息及隐私不仅是法律法规的强制要求，更是金融企业/机构履行社会责任、赢得客户信任的重要基石。金融企业/机构需要建立健全的个人信息保护政策和制度，明确个人信息收集、使用、存储、共享等环节的规范和标准，确保个人信息处理活动的合法、正当、必要和透明；其次，加强技术防护措施，采用加密技术、访问控制、数据脱敏等手段，保护个人信息在传输、存储和处理过程中的安全性，防止数据泄露和非法访问；同时，加强员工培训和意识教育，提升全体员工对个人信息保护的认识和重视程度，防止内部人员泄露客户信息；此外，还需要建立健全的投诉处理机制和应急响应预案，及时应对个人信息泄露等突发事件，减轻对客户的影响，并追究相关责任人的法律责任。通过这些工作内容的实施，金融行业可以为客户提供更加安全、可靠的金融服务环境，促进行业的健康、稳定发展。

数据跨境传输

在金融行业，数据跨境传输是金融企业/机构跨国经营、全球贸易及服务贸易的基石，更是推动国际经济一体化与金融合作的关键环节。随着全球经济金融联系的日益紧密，数据跨境传输成为资金、信息、技术、人才等资源要素跨国界交换、共享的重要渠道。数据跨境传输也伴随着诸多挑战和风险，如数据泄露、隐私保护、国家安全等问题。因此，金融行业在推进数据跨境传输时，必须严格遵守相关法律法规，如《中华人民共和国数据安全法》、《促进和规范数据跨境流动规定》等，确保数据传输的合法性和安全性；同时，金融企业/机构还需建立完善的数据安全保护机制，并通过技术手段落实传输加密、身份认证、防网络攻击等工作，以保障数据在跨境传输过程中的安全性和完整性；其次，金融企业/机构在进行跨国经营时，如设立海外分支机构或进行跨境投资，需确保大量业务数据的跨境安全传输，以保障业务连续性和运营效率，这些工作对于提升金融服务质量和市场竞争力至关重要。

数据共享与权限管理

金融行业数据共享与权限管理的重要性在于促进信息资源的有效利用，加强金融企业/机构之间的合作与协同，提升金融服务效率与质量，同时确保数据的安全性和合规性。金融企业/机构需要建立健全的数据共享政策和标准，明确数据共享的范围、方式、流程以及参与方的权利与义务，并构建统一的数据共享平台或接口，实现数据的集中存储、管理和交换，确保数据的一致性和可用性。同时，还需要实施严格的权限管理机制，包括用户身份认证、访问控制、数据脱敏、审计跟踪等措施，确保数据在共享过程中的安全性和合规性。此外，还需要加强对数据共享活动的监测和评估，及时发现并处理潜在的安全风险和问题，持续优化数据共享与权限管理机制。通过合理的数据共享机制，金融企业/机构可以打破信息孤岛，实现数据的互联互通，为客户提供更加全面、个性化的金融服务。而权限管理则是保障数据共享过程中数据安全的关键，通过精细化的权限控制，确保只有经过授权的人员或系统才能访问和处理特定的数据，防止数据泄露和滥用。

6.6.3 腾讯云合规技术建议

全球化部署

鉴于国家层面已确立清晰的数据隐私保护法规与政策框架，明确了数据分类与本地化策略，识别重要数据及个人信息数据，确保这些关键数据均在当地数据库进行安全存储。通过设立独立站点，采用数据加密、访问控制、审计追踪等技术手段，增强数据的隔离性和安全性，防止数据泄露和非法访问，强化数据的地域性隔离与合规性处理。利用全球CDN网络，将内容缓存到离用户最近的节点，提高访问速度和降低延迟。采用智能路由算法，根据网络状况和用户位置，动态选择最优的CDN节点进行内容分发，提升用户体验。

腾讯云在全球主要国家和地区都有公共云region，可以满足金融行业企业数据本地化存储的要求，为客户提供了强有力的技术支持，灵活应对不同地区的法规要求，满足客户的全球化业务需求，确保数据处理的合规性、高效性与安全性。



用户注册及登录

银行的网站和APP作为提供金融服务的重要渠道，不可避免地需要用户进行注册及登录。这一流程不仅是验证用户身份、确保账户安全的基本措施，也是个性化服务、交易授权及数据隐私保护的前提。通过注册，银行能够收集必要的用户信息，为用户提供量身定制的金融产品和服务；而登录则是用户访问账户、进行交易操作、查询信息等的必要步骤，确保每次访问都经过授权且可追溯。保障用户数据的安全性与隐私保护是首要任务，这需要金融企业/机构采用先进的加密技术和严格的身份验证机制，以防范信息泄露和身份盗用。随着网络攻击手段的不断演进，金融企业/机构必须不断升级其防护系统，以抵御钓鱼攻击、恶意软件及自动化攻击等安全威胁。同时，平衡用户体验也是一个重要挑战，既要保证注册流程的简便快捷，又要确保登录验证的严格性，以维护账户安全。跨平台兼容性、多因素身份验证的普及及密码管理策略的优化也是金融企业/机构在提升用户注册及登录体验方面需要持续努力的方向。在用户注册及登录环节，腾讯云可以为企业APP或网站提供如下解决方案与能力：

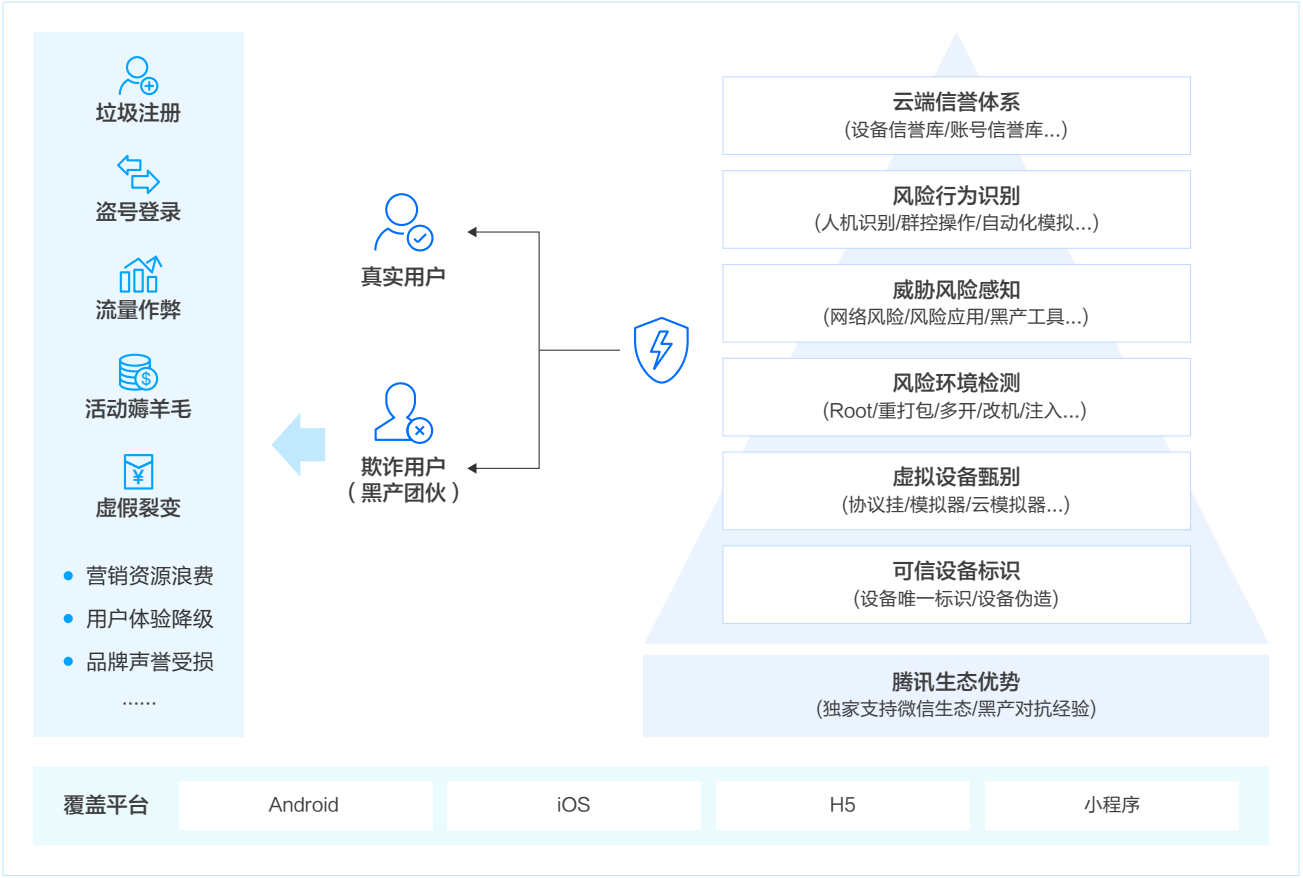
- **腾讯云慧眼人脸核身（原金融级身份证认证升级版）**

  腾讯云慧眼人脸核身（原金融级身份证认证升级版）：这是一组对用户身份信息真实性进行验证审核的服务套件，提供证件OCR识别、活体检测、人脸1:1对比等能力，以满足金融行业对用户身份信息核实的需求。



- **业务风控**

腾讯云全栈式风控引擎（RiskControlEngine，RCE）基于人工智能技术和腾讯多年风控实战经验，依托腾讯海量业务构建，以轻量级的SaaS服务方式接入，帮助企业快速解决注册、登录、营销活动等关键场景中的欺诈问题，实时防御黑灰产作恶，有效降低金融企业/机构APP/网站在用户拉新、促活等活动中的数据合规风险与业务资损风险。



跨境交易反欺诈风险识别

跨境交易反欺诈风险识别是一个高度专业化的过程，涉及对跨国交易中的潜在欺诈行为进行精准识别与评估。这一过程结合先进的技术手段与丰富的行业经验，通过分析交易数据、行为模式、历史案例及国际法规要求，快速识别出异常交易信号，如资金流动异常、虚假身份交易、重复支付请求等。同时，还需关注国际政治经济环境变化对欺诈风险的影响，以及不同国家和地区间法律差异带来的挑战。跨境交易反欺诈风险识别旨在保护交易双方的合法权益，维护市场秩序，确保跨境交易的安全与顺畅进行。腾讯云风控引擎RCE凭借其创新的交易反欺诈风险评分模型，在不触碰用户个人隐私数据界限的同时，实现了对黑灰产请求的精准捕捉与识别，显著降低因欺诈行为导致的拒付率，为构建安全、高效的交易环境提供了坚实保障。跨境反欺诈场景中RCE方案参照6.6.3.2 用户注册及登录中的内容。

数据安全及跨境传输

个人信息的采集工作的重中之重是获取客户授权。腾讯作为合作伙伴，提供全方位的网络安全与数据安全产品服务，涵盖客户办理业务过程中涉及的相关过程性数据的精细分权分域管理，并特别针对图像和视频内容采集端，定制高效的安全防渗透措施方案，以应对潜在的安全威胁。针对跨境业务、境外监管、委托处理等业务场景的跨境数据传输，敏感数据回流引发的监管风险是金融企业/机构面临的重大挑战。因此，腾讯特别提供了数据库级别的过程管理解决方案，包括在各国本地实施严格的数据处理流程，确保数据的本地化存储与处理，同时实施详尽的日志备份机制，以便在监管审查过程中提供清晰、可追溯的证据，有效预防并减少因数据跨境流动而产生的法律纠纷与风险敞口。

在数据安全方面，可参考5.3.1节“数据安全”的内容来落地技术方案。

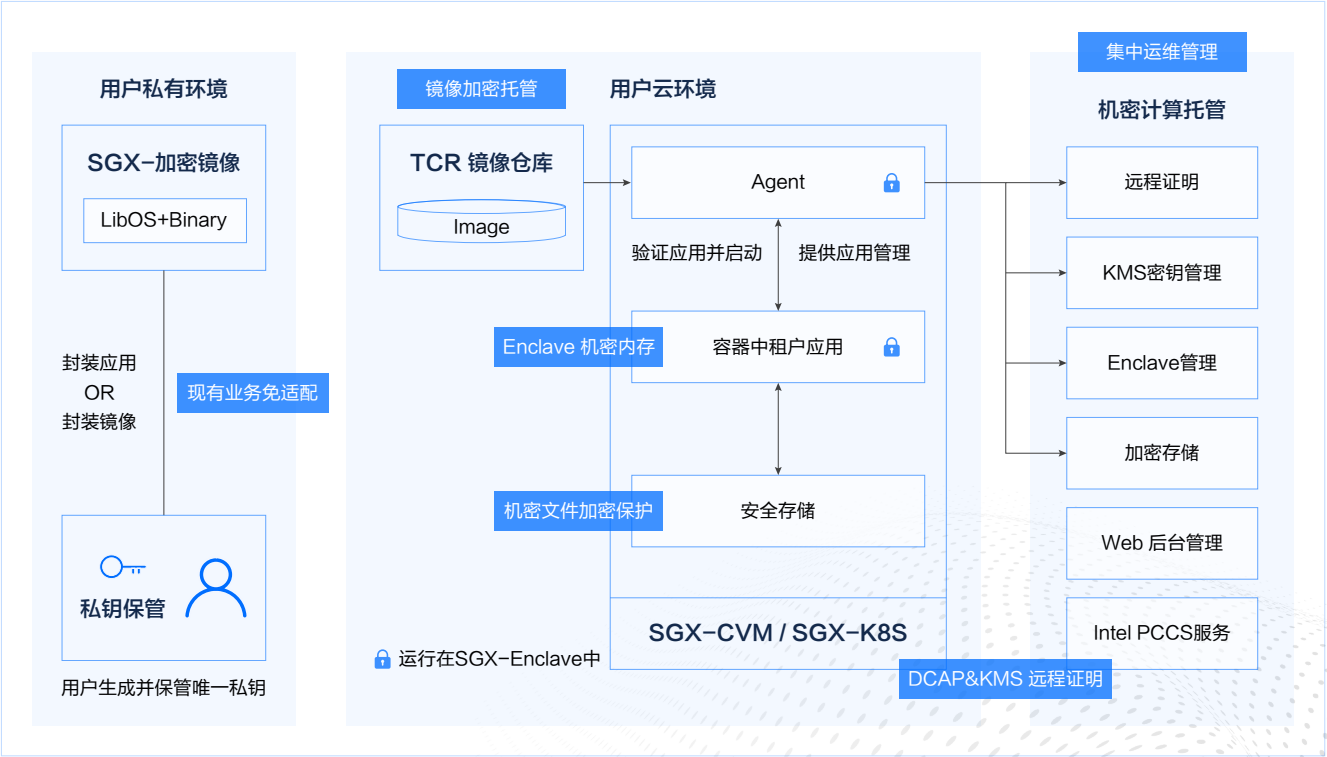
数据共享隐私计算解决方案

在其他行业，大部分场景下隐私计算属于“nice to have”的方案，但在金融行业，部分场景下隐私计算属于必需。金融企业/机构之间需要进行数据共享以增强风险评估、欺诈检测和信用评分等能力。隐私计算允许不同机构在不直接交换数据的情况下进行协作。腾讯云隐私计算解决方案可以帮助金融企业/机构客户实现数据可用不可见、用途可控可计量的数据可信流通范式，满足GDPR等数据合规的要求。腾讯云机密计算平台（Confidential Computing Platform，CCP）是基于可信执行环境（TEE）打造的隐私安全基础平台，为用户提供机密计算轻松接入、服务托管、一站式运维等功能，实现端到端全生命周期保护用户数据的机密性和完整性，满足用户多应用、多业务、多场景的安全需求。

以下是腾讯云CCP产品的能力特性。



下图是利用腾讯云CCP搭建的云上隐私计算平台：



内控方案

金融企业/机构必须建立有效的内部控制和审计机制，以确保其数据处理活动符合合规要求，并能够及时发现和纠正违规行为。在内控方面主要体现在三个子场景：账号管理与云资源的精细化授权，数据的精细化授权，内部数据安全风险的发现与处理。

- **账号管理与云资源精细化授权**：可参考5.3.2.2节“账号与身份管理最佳实践”与5.3.2.3节“云资源访问管理最佳实践”的内容。
- **数据的精细化授权**：可参考5.3.2.14“数据的精细化授权”与5.3.6.2节“权限管控与风险控制”的内容。
- **内部数据安全风险发现与处理**：可以使用腾讯云T-Sec安全运营中心。它以云原生技术为基础，仓湖一体化大数据平台为底座，MITRE ATT&CK技战术框架为指导，结合腾讯领先的威胁情报能力、AI和可视化技术，聚焦TDIR（Threat Detection，Investigation and Response），打造智能化安全运营平台，提升安全运营效率，实现企业全网安全态势可知、可见、可控。

审计方案

监管机构对金融企业/机构的数据合规审计通常有一系列具体的要求，以确保其在处理个人和敏感数据时遵守相关法律法规，如《通用数据保护条例》（GDPR）、《加州消费者隐私法案》（CCPA）及中国的《个人信息保护法》等。此外，金融行业不同子行业会有自己的行业标准，监管机构也会检查金融企业/机构的数据处理活动是否符合行业标准和最佳实践。腾讯云提供一系列的审计能力，帮助金融企业/机构提供足够的记录与文档，证明其有足够的安全能力、数据管理各环节合规措施实施到位、技术架构能有效防止数据泄露等。详见5.3.3节“数据合规审计”内容。

传统制造业 6.7

6.7.1 行业监管概要

随着制造业出海的趋势日益强劲，越来越多的制造企业面临着行业特有的数据合规挑战，如保障供应链中数据的安全性、强化物联网的数据安全、保护员工和客户数据的隐私、以及在云计算服务中维护数据的安全性和合规性。这要求企业不仅要紧跟数据保护法规的步伐，还要在全球化布局中，灵活应对不同地区的合规要求，构建起既符合国际标准又适应本土市场的综合数据管理体系。

6.7.2 合规关注要点

供应链

制造业通常面临复杂的供应链网络，例如原材料供应商、制造商、分销商、零售商和客户等，此外还包括云服务商、数据处理服务商和技术服务商等，涉及的隐私数据包括合作伙伴业务联系人姓名、职位、电话、电子邮件地址等，以及供应商的银行账户、交易记录、发票和支付信息等。供应链涉及大量的数据跨境、共享、交换，因此存在较高的数据安全和合规风险。

供应链数据管理涉及多个企业和跨境的合作，数据在不同系统和国家之间流动，需注意以下合规要求：

- a)跨境数据传输：涉及多个企业和跨境合作伙伴，数据在不同系统和国家之间流动。法律要求在跨境传输时，必须具备充分保护措施。例如欧盟《通用数据保护条例》要求使用标准合同条款（SCCs）或其他合适的机制来保障跨境数据传输的安全，中国《个人信息保护法》要求对跨境传输个人信息进行安全评估或签署标准合同，巴西《通用数据保护法》规定跨境数据传输需确保接收方符合数据保护要求。
- b)数据保护责任：供应链中的每个参与方都需明确数据保护责任，以保障数据在全供应链中的安全性。例如欧盟《通用数据保护条例》要求数据处理者和控制者明确数据保护责任，日本《个人信息保护法》规定数据处理者需采取适当措施防止数据泄露或滥用，澳大利亚《隐私法》要求处理个人信息的各方都必须承担数据保护责任。
- c)透明度要求：企业需告知数据主体其数据将被传输至何处、用于何种目的。例如美国《加州消费者隐私法》要求企业告知消费者数据的使用和传输情况，欧盟《通用数据保护条例》要求数据控制者向数据主体提供透明的信息，说明数据处理的目的和方式，巴西《通用数据保护法》：第9条要求企业告知数据主体其个人信息的使用目的。

物联网

近年来，越来越多的制造业通过使用物联网实现生产过程的实时监控与优化，提高了生产效率和产品质量，与此同时也带来数据合规的挑战。物联网在感知层利用传感网络和自动识别技术收集环境信息，在网络层通过互联网协议和云计算技术实现在物体间数据传输，在应用层进行计算和数据挖掘等智能处理，这个过程中涉及大量的数据采集、传输和处理，包括生产数据、设备性能参数、操作员信息等敏感信息，如遇篡改、破坏或泄漏可导致数据合规风险。

物联网数据管理的合规性集中在设备本身的安全设计和数据的合法处理上，需注意以下合规要求：

- a)隐私设计：物联网设备在设计时须考虑隐私保护，确保数据的收集、传输和存储过程安全可靠。例如欧盟《通用数据保护条例》要求在设计和默认设置中实施隐私保护（隐私设计理念）。
- b)设备安全性：设备制造商和运营方需确保物联网设备具备合理的安全功能，以防止未经授权的访问。例如美国《加州物联网安全法》要求物联网设备具备合理的安全措施，以保护设备及其中包含的任何信息免受未经授权的访问、销毁、使用、修改或披露。
- c)数据处理合法性：物联网设备收集的个人数据必须基于合法、必要和正当的目的，仅在明确同意或法律要求的情况下才能收集和处理用户数据。

人力资源数据管理

在制造业人力资源管理工作中，各个业务环节都涉及大量的员工隐私数据，例如招聘环节会采集和处理员工的基本信息、通讯信息、学历信息、工作经历信息等，入职环节会采集和处理员工的背调信息、体检信息等，日常管理过程中会处理和传输考勤信息、绩效信息、培训信息，薪资管理过程中会处理银行账户信息、薪酬信息等，因此企业应当重视人力资源数据的管控，降低合规风险。

在人力资源管理中，全球数据保护法律普遍要求雇主对员工个人数据的处理必须合法、透明并受到严格保护，需注意以下合规要求：

- a)**数据处理合法性与透明度**：雇主必须确保员工个人数据的处理合法、透明并受到严格保护。数据收集时需明确告知员工数据的目的、使用方式及保留时间。例如欧盟《通用数据保护条例》规定数据处理应合法、公正且透明，并要求提供清晰的隐私通知，告知数据主体数据处理的目的和方式，中国《个人信息保护法》要求数据处理应基于合法、明确的目的。澳大利亚《隐私法》要求数据收集时提供透明的信息，并说明数据的使用目的。
- b)**跨境数据传输**：在跨境传输员工数据时，企业需确保接收国的数据保护水平符合本国法律要求。
- c)**数据存储安全**：雇主应采取适当的技术和组织措施，防止员工数据泄露、丢失或未经授权的访问。

客户数据管理

制造业在国际市场上运营时，线上订单、客户服务、市场营销、产品使用反馈等多个环节都会涉及客户的数据，包括基本身份信息、通讯信息、交易信息、订单信息等，保护客户数据的安全性不仅是合规要求，也是维护客户信任和企业信誉的必要举措，任何数据泄露、滥用或未经授权的数据访问都会引发合规和信誉方面的风险。

在管理客户数据的过程中，需注意以下合规要求：

- a)**跨境数据传输**：企业在跨境传输客户数据时，必须遵循严格的合规程序，确保数据在传输至他国时依然受到法律保护。
- b)**数据主体权利**：法律赋予数据主体访问权、知情权、删除权等各项权利，因此当客户提出相应要求时，企业应及时响应。例如欧盟《通用数据保护条例》规定数据主体有权访问、纠正和删除个人数据，中国《个人信息保护法》赋予数据主体访问、更正和删除个人数据等权利。
- c)**数据处理和存储安全措施**：企业需要确保在数据处理和存储过程中采取适当的安全措施，以防止数据泄露或滥用。

云计算服务

在云计算环境中，数据安全问题相对复杂，涉及服务提供方、用户、为云平台提供产品和服务的第三方供应商等角色，平台上存储了用户上云的业务数据、生产数据，提供方依托云平台产生的日志、系统、操作、配置等数据，其中也会包含大量的个人信息和个人敏感信息。随着企业越来越多的数据上云，一旦数据安全管理不当，就会导致严重的合规风险。

在云计算服务中，需注意以下合规要求：

- a)**责任划分与数据保护**：法律普遍要求云服务提供商和用户明确责任划分，确保数据安全和隐私保护。云服务提供商作为数据处理者，需要确保基础设施的安全性，并提供适当的工具和机制帮助用户保护数据。例如欧盟《通用数据保护条例》要求数据处理者与数据控制者签订数据处理协议（DPA），明确数据处理的责任和安全措施。
- b)**数据传输与存储责任**：企业在使用云服务时，仍需对数据的传输和存储负责，特别是对于存储在云上的敏感数据，需采取额外的加密和访问控制措施。
- c)**跨境数据传输**：跨境数据传输是云计算服务中的重要合规领域，企业需确保数据在跨境传输过程中符合所在国家或地区的法律要求。

6.7.3 腾讯云合规技术建议

供应链数据管理

- **签署数据保护协议**：与供应链合作方签订数据保护协议，明确数据保护责任和义务。
- **实施适当的跨境数据传输机制**：签署标准合同条款、开展数据保护认证或其他合规程序，确保数据跨境传输的合法性。
- **数据来源合法性验证**：确保从上游供应商获得的数据的质量和合法性。
- **供应商安全审查**：建立供应商数据安全审查机制，选用具备充分数据安全能力的供应商。
- **数据存储和分析的本地化**：设备操作员的生物识别数据，用于启动或激活设备某些命令的应用程序建议本地进行存储，尽量规避传输至云端、甚至通过跨区域访问造成被动的数据跨境。设备主机厂、零部件供应商以及软件服务供应商，都需识别各类场景下需处理的数据类型、规模、敏感程度，注意评估数据回传的必要性。
- **与第三方信息分享的范围最小化**：除设备厂商自身对于设备内产生、收集数据的分析外，智能化功能也往往依赖于第三方提供的服务。例如设备提供当前所在区域的公共信息，终端设备向提供公共信息的供应商提供位置信息，由服务供应商反馈公共信息到设备终端。在这个过程中需要注意地理位置的获取需在设备终端获取同意，并且位置信息的提供为可满足服务的最小范围，例如仅到市、区级，而非具体的坐标信息，且该信息不应持续收集。

物联网数据管理

- **采用隐私设计理念**：在设备设计阶段实施隐私保护措施，确保设备具备数据保护功能。
- **确保具备安全功能**：为物联网设备提供适当的安全功能，如加密和身份验证，防止未经授权的访问。
- **确保数据处理的合法性**：确保在收集个人数据时获得合法同意，并确保数据处理基于合法的目的。
- **定期安全审计**：定期对物联网设备和系统进行安全审计，以识别和修复潜在的安全漏洞 。

人力资源数据管理

- **确保数据处理透明度**：发布员工隐私声明，告知员工数据收集的目的、使用方式及保留时间。
- **告知同意**：在处理员工敏感数据时，获得员工的明确同意，并确保处理符合合法性要求。
- **采取数据保护措施**：采取适当的技术和组织措施，保护员工数据的安全性，防止数据泄露或滥用。

客户数据管理

- **明确数据处理的合法性基础**：确保客户数据的收集和处理基于合法的基础，如获得明确同意、履行合同或合法利益。
- **响应数据主体权利**：提供客户访问其数据的权利，以便客户在必要时提出请求。
- **数据存储安全**：实施必要的加密和访问控制措施，以保护客户数据的安全性。
- **同意获取的方式**：在当前的设备上，与设备的交互主要通过集成终端进行，因此集成终端将成为同意获取以及同意撤销的主要窗口。设备软件设计过程中，应尽量避免打包同意的情况，针对于各项较为敏感的信息收集，建议以单独同意的方式为主，并且在不影响安全地前提下，可以便捷、快速地关闭授权。若涉及到跨区域或跨国家的场景，数据控制者发生变化时，需要提示告知设备使用者。
- **数据安全性保护**：设备运行相关的核心功能应与互联网功能相隔离，设备核心功能直接影响了设备以及使用者的安全性，互联网功能的宕机不应影响到设备的驾驶系统的正常运作。另一方面生物识别数据的收集、识别方案应当能够抵抗一定强度的攻击，并设置验证尝试的有限次数，避免对于生物识别信息或用户身份信息的原始信息的本地存储。

云计算服务数据管理

- **签署数据处理协议**：与云服务提供商签订数据处理协议，明确数据处理的范围、目的及安全措施，并在协议中明确责任划分，确保云服务提供商和用户各自履行数据保护责任
- **签署服务级别协议（SLA）**：确保其中包含明确的服务水平指标和补偿措施、检查SLA中的可用性、性能和故障恢复等方面的承诺，以确保符合业务需求
- **数据备份和灾难恢复**：确定云服务提供商的数据备份策略，以确保在发生灾难性事件时能够迅速恢复服务和数据
- **数据安全措施**：采取适当的技术和组织措施保护云中存储的数据，包括加密、访问控制和定期安全审计

智能终端制造业 6.8

6.8.1 行业监管概要

随着智能终端的技术不断发展，智能终端的应用场景和市场规模也在不断扩大。因消费者需求差异，不同品类的智能终端在不同国家地区所面临的竞争环境和监管环境都有差异，企业不仅需要考虑市场机会，也需要慎重应对不同国家和地区的法律法规要求。

智能终端收集并根据信息进行响应，并通过蓝牙、Wifi 等方式与Web、手机App 进行交互与数据传输，最终数据将通过Web 或App 传输至云平台进行管理。因此除了网络安全法规、隐私保护法规、数据安全法规等通用法规，还需要关注产品安全、无线通讯相关的法律法规，企业根据当地的法规进行适应性调整。

6.8.2 合规关注要点

产品及云端安全

出海智能终端企业应全面识别出海目标国家地区针对产品安全的相关安全标准和法律要求，如欧盟颁布的CE 认证标准，智能终端企业若要将产品在欧洲市场贸易，则必须通过CE 认证，并在产品上贴上CE 标签。

智能终端企业重视运用技术的同时也需要注意安全控制和满足合规要求，如欧洲电信标准协会(ETSI) 针对IoT 产品推出了ETSI TS 103 645 和ETSI EN 303 645 安全标准来保障的合规基础，企业应积极参考并保障产品满足合规基线。

另外，智能穿戴设备以及智能家居IoT产品在设计过程的安全性一般不如App 以及手机等设备的安全性程度，其漏洞的暴露可能使得攻击者以IoT 产品作为突破口，例如漫游获取Wifi 凭据，进一步获取连接到该网络的所有设备的访问权限，抑或是对目标直接发动攻击。

智能穿戴设备的多种功能也依赖于第三方SDK实现，在手机或设备端的应用包括地图类、统计类、广告类、短信验证类以及支付类SDK。在引入SDK 前，智能终端企业应对于SDK 的安全性进行测试，检查其是否存在安全漏洞、收集个人信息的范围是否合理、隐私政策告知内容与实际收集、处理机制是否一致等问题，并以书面形式协商双方的责任边界。

由于终端存储的有限性、以及对于云端分析的依赖，云端平台是众多终端设备数据的最终载体，因此云端的防护同样需要智能终端供应商重点关注，尤其是云上的数据库访问权限以及数据库内对数据本身的保护。

移动通信技术运用的合规

IoT 智能终端需要借助相关通讯技术（Wifi、蓝牙、RFID、MQTT 等）来实现与APP、平台、用户的交互，在使用这些通讯技术时可能会存在相关隐私泄露的场景，如IoT 设备的平台和APP 可能会在业务场景中收集用户Wifi 信息（ssid、密码、位置等）；智能终端之间通过蓝牙技术、MQTT 协议的交互可能会被监听或者重放；使用射频识别技术RFID 可能造成的隐私泄露风险等。

故而智能设备终端不仅需要从自身产品的安全性出发，也需要关注以下相关协会或联盟所制定的标准，并充分地实现合规。如欧洲的ETSI（欧洲电信标准协会）、日本的ARIB（社团法人电波产业会）和TTC（情报通信技术委员会）、中国的CCSA（中国通信标准化协会）、韩国的TTA（情报通信技术协会）、北美洲的ATIS（电信工业解决方案联盟）和印度的TSDSI（电信标准开发协会）。

海量IoT数据收集与传输

智能IoT终端安全运行时会随之而产生的海量数据，这些数据可能会直接或者间接的揭示用户的隐私信息，企业需充分考虑是否需要收集处理和储存该设备的运行数据，从而达到满足产品性能的同时也符合监管要求。例如在智能灯光系统及空调远程打开或预约回家时间，体重秤等健康类应用会通过设备、用户输入收集身高、体重、身体状态，甚至是饮食过敏信息。而像手环、手表等穿戴设备，除了监控用户日常的身体状态、运动状态、作息状态外，还有可能记录用户的日常访问位置、接打电话等通讯记录。

收集的数据类型的多样化，需要智能终端提供商梳理其可以收集的信息类型，分析其目的，制定与信息类型匹配的同意获取方式。例如仅在需要的时候获取地理位置信息，并且在第一次接入时告知收集目的并获取同意。

生物数据的收集与识别

智能终端可能会使用到用户的生物信息，如指纹、掌纹、声纹、面部特征等常见生物特征数据，例如指纹锁、人脸解锁、声纹唤醒等场景，在给用户带来便捷的同时，此类生物信息的特征化提取、原始信息的留存成为需关注的重点问题。企业应当特别关注并遵守当地对生物特征信息收集与使用的要求，并谨慎应对生物信息的收集与处理，如制定完善的隐私说明； 从业务逻辑出发实现生物信息本地存放；提供更多的可选项等应对措施。

维修及报废处理

由于智能终端的互联特性，在维修过程中存在其本地数据的被不当获取、甚至冒用权限的情况。智能终端企业出海后面临着在当地构建售后团队需细化维修人员可接触的数据边界及范围，并且在硬件层面严格遵循销毁标准要求；若通过远程方式进行售后，例如寄回维修， 则建议提醒用户提前对数据进行备份，在可开机的情况下删除数据再寄出，规避数据跨境和可能在寄送过程中的数据泄露。同时企业应提供一键清除设备内数据的功能，包括不限于用户信息、使用信息、日志信息，以免在报废或二手买卖过程中的信息泄露。

6.8.3 腾讯云合规技术建议

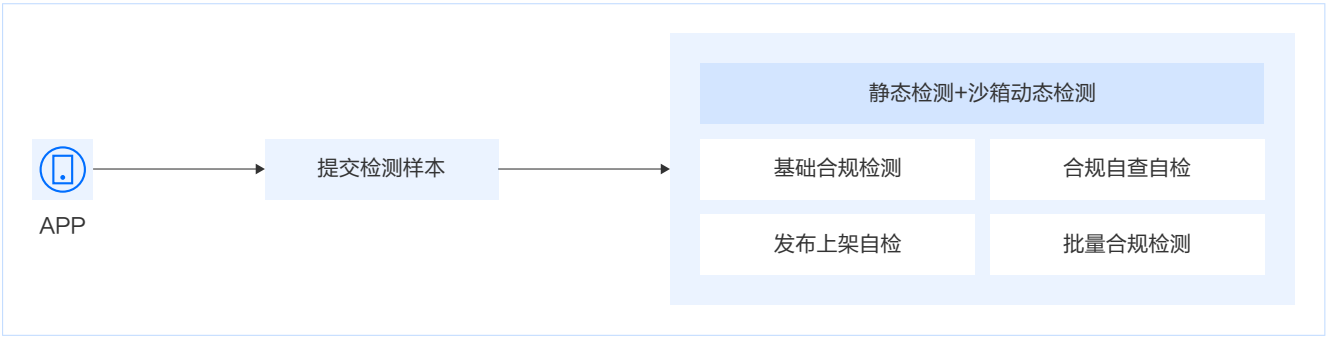
终端数据合规方案

大多数智能终端都会接触到消费者大量的个人数据。例如手机、智能摄像头、带拍照录像功能的无人机、带传感器和终端控制交互的智能家电等。所以终端的数据合规方案体现在数据采集环节的过滤与脱敏上。部分终端自带数据采集过滤与脱敏能力，例如部分摄像头自身就是一个计算单元，可以将拍到的图像或视频数据进行实时匿名化与压缩，然后再传给云端。但大多数终端设备采集的数据还是会在云端统一处理，其中包括数据脱敏的能力。

在该场景中，腾讯云产品会起到主要作用如下：

一是数据脱敏的Dmask（Data Masking）产品，它是一款敏感数据脱敏与水印标记工具，可对数据系统中的敏感信息进行脱敏处理并在泄漏时提供追溯依据，为企业数据共享、迁移、分发提供安全保护措施。它能够帮助终端采集的数据做脱敏，详情可参考5.3.1.4节“数据脱敏”的内容。

二是应用合规平台（Application Compliance Platform）。它是一款提供小程序、移动 App 应用隐私合规检测的产品，基于相关法律法规、国家标准、行业标准等，对小程序、移动 App 应用进行静态、动态的技术检测，结合腾讯灵犀隐私合规专家团队专业意见，帮助企业识别应用的数据隐私合规问题，助力企业安全合规。诸多终端的体现形式实际上是手机上的APP，APP在数据采集时不能逾权去采集不相关的数据，也不能将采集到的隐私数据发往未被授权的三方等。这一切能力的实现都需要依赖腾讯云的应用合规平台来实现。



数据存储合规方案

终端采集的大部分个人数据（手机相册，视频录像）由于是非结构化的，大都会存放在云上的对象存储里。从存储合规的视角来看，需要做好以下这三个方面：

加密存储

存储桶加密是针对存储桶的一项配置，通过设置存储桶加密，可对新上传至该存储桶的所有对象默认以指定的加密方式进行加密。目前存储桶支持的加密方式有两种，一种是SSE-COS 加密，即由对象存储（Cloud Object Storage，COS）托管密钥的服务端加密；另一种是SSE-KMS 加密，即使用 KMS 托管密钥的服务端加密。可以在创建存储桶时启用数据加密的能力，如下图所示：



或者在已经创建的存储桶中配置加密，如下图所示：



- **精细化授权**

用户可以通过对象存储控制台来设置或修改存储桶的访问权限。对象存储COS支持设置两种权限类型，一种是公共权限，即私有读写、公有读私有写和公有读写；另一种是用户权限，主账号默认拥有存储桶所有权限（即完全控制）。另外COS支持添加子账号有数据读取、数据写入、权限读取（即授予用户读取“存储桶访问权限”的权限）、权限写入（即授予用户写入“存储桶访问权限”的权限），甚至完全控制的最高权限。

通过存储桶的精细化授权，可以有效杜绝内外部对存储桶中个人数据的非法访问与获取。例如，手机相册被窃取、私人照片泄漏的情况就不会发生。



- **数据生命周期设置**

用户需要定期对指定对象进行存储类型转换或删除，这样不仅可以降低成本，更重要的是能够及时删除合规限制时间到期的数据，以降低合规风险。举例来说，当一个云相册用户注销之后，其原先放在对象存储中的个人相册就应该在一定时间内删除，以符合GDPR的要求。这完全可以借助腾讯云COS的数据生命周期管理功能实现。

当前腾讯云COS支持基于最后修改时间以及最后访问时间的策略创建生命周期规则。对象存储COS会按照您设定的规则对指定对象在指定的时间内自动进行存储类型转换或删除。详细设置信息可以参考官网：https://cloud.tencent.com/document/product/436/14605

▶ 数据处理合规方案

智能设备上传到云端的数据，在对象存储中存储之后，在很多场景下还会被进一步处理加工，以实现更高价值的应用。例如被用来训练AI模型，或者被智能化解析分析以便于用户后续的查阅（像云相册搜索“白云”便能找到拍摄的所有含有白云的照片），或者有时候会共享给三方做广告营销。这些场景自然在一开始就要和用户把数据用途说清楚并取得用户授权之后才可进行，这是数据合规的一方面。另一方面，在对数据进行加工以进一步实现上述的应用场景时，要注意数据最小使用原则，不能把不相关的数据、敏感的不能应用的数据一起放进来。

腾讯云提供的基于WeData的数据脱敏方案，以及基于对象存储和函数计算的数据处理能力，可以帮助企业实现上述合规场景。详情请参考4.2.4.2中“数据脱敏与匿名化”小节内容与5.3.6.4节“数据脱敏”内容。

行业案例梳理 6.9

6.9.1 某跨境电商企业数据合规审计体系化建设

某跨境电商企业A在跨境电商领域具有较大影响力。随着业务在欧美市场的扩展，企业A面临着复杂的数据合规挑战，特别是在遵循《通用数据保护条例》（GDPR）和《加州消费者隐私法》（CCPA）方面。

由于之前业务的高速发展，企业A在合规审计方面比较碎片化，完整度和体系化都较差。由于监管压力，也处于企业需要对公众和当地政府呈现出更加透明和负责任的形象，企业A基于腾讯云的日志服务、数据库审计等产品技术方案，启动了体系化的数据合规审计能力建设，确保所有数据处理活动符合相关法律法规。主要步骤包括：

- **数据映射与分类**：首先进行了数据映射，识别出所有个人数据的来源、存储位置和用途。这一过程帮助团队了解数据流动，确保每个数据处理环节都符合合规要求。企业A利用了腾讯云WeData产品进行了数据的映射与分类。
- **制定合规政策**：根据GDPR和CCPA的要求，企业A制定了详细的隐私政策和数据处理协议。这些政策明确规定了数据收集、使用、存储和共享的流程，同时规定了用户的权利和企业的责任。利用腾讯云数据脱敏相关的产品工具，企业A在数据共享环节大大降低了合规风险。同时利用腾讯云的在对象存储、数据库、大数据等产品领域的精细化权限管理能力，依据数据最小化权限的原则，落地了内部数据流转的最小化授权流程。此外，在存储个人数据的各存储产品中都统一进行加密，并用KMS来统一管理密钥，同时达到了合规、安全与高效的效果。
- **内部审计与评估**：企业A定期进行内部审计，评估数据处理活动的合规性。通过与合规团队和法律顾问合作，审计团队能够及时识别潜在的合规风险，并进行调整。利用腾讯云的数据安全中心和数据库审计等产品工具，审计团队能够快速高效的得到相关的审计日志，并洞察其中可能存在的问题与风险。
- **外部认证**：企业A通过自身合规能力的建设和外部咨询机构的协助，拿到了ISO27017、ISO27018等数据合规、隐私保护方面的认证，对用户传达了专业与透明的形象。

总的来说，企业A通确保了所有审计数据的统一管理，并建成了合规中台的能力，大大增强了其数据合规能力的可持续、可迭代与可信任。

6.9.2 某社交公司海外数据合规落地实践

某中国社交企业，在海外有庞大的用户，其在海外发育了社交、短视频、直播、内容社区等业务。随着其业务国际化尤其是欧洲业务的迅猛发展，其在数据合规方面面临诸多挑战，其在海外也建立了一定规模的法务合规团队，结合腾讯云的技术方案，在诸多业务和场景中大大降低了数据合规的风险。

欧洲的《通用数据保护条例》（GDPR）和《数字服务法》（DSA）对数据处理提出了严格要求，此企业内部也对这两部法规做了详细的研读和拆解。

首先，在用户注册和数据收集过程中，明确告知用户其数据将如何被使用。用户在使用平台之前，需同意隐私政策和服务条款。平台提供了清晰的说明，确保用户能够理解他们的数据使用情况。

其次，依托腾讯云欧洲、美国和新加坡的region，此企业分别建立了3个数据中心，确保用户数据一定的本地化存储。利用腾讯云COS、数据库以及数据安全中心的能力，此企业实施了数据的即时脱敏和分类管理，确保敏感数据与普通数据分开存储。并采用包括数据加密、访问控制和定期安全审计等技术与管理策略，确保数据在传输和存储过程中的安全性。

再者，由于业务本身特性，此企业有较多的与三方进行数据交互和共享的场景，与广告商和品牌合作时，确保只有在用户同意的情况下，才能共享个人数据。例如，与品牌合作进行市场推广时，提前告知用户其数据可能会被用于广告投放，并提供可供用户选择的退出机制。这种做法不仅符合当地的法律要求，还增强了用户对平台的信任。

最后，用户在平台上可以方便地查看自己的数据使用情况，并根据需要进行删除。例如，在APP的隐私设置中提供了“数据管理”选项，用户可以轻松查看和管理自己的个人信息。用户注销时平台会检查用户在平台各子系统中的个人数据，并做删除。

6.9.3 三一集团有限公司海外数据出入境合规管控

三一集团有限公司是一家全球化经营的工程机械制造企业，在各项业务出海过程中严格遵守国际规则和当地法律法规，借助腾讯丰富的海外数据合规经验，建立健全的数据合规体系，采取严格管控措施和技术，来保障数据合规性。

数据合规体系方面：建立矩阵型的数据合规组织，通过数据权限管理工具平台实现对组织、对象、作用域、作用时间等权限指标的精细化管理，采用统筹规划、建制度流程、监督检查等关键措施来推动数据合规工作。同时，制定严格的数据合规管理红线、指导手册、重要业务场景合规指引，及配套数据合规点检平台，有效保障数据合规工作运行。

- **数据合规管控方面**：严格遵守各国数据合规政策要求，基于全球数据法律法规、欧盟 0TA 认证、国家安全等驱动因素，形成数据全生命周期合规和业务过程合规“2条主线”，评估、采集、存储、传输、应用等“7个控制域”，合规影响评估、存储本地化、存储最小化、超期删除、加密存储等“29 项控制项”来保障业务数据合规性。
- **数据合规落地措施**：针对有本地化存储特殊要求的国家，严格按照当地要求进行本地化部署，针对敏感个人数据不能跨境的国家，在采集方面杜绝采集该类数据(如人脸、指纹等)，同时,涉及军政类客户的设备数据，一律禁止采集。对于部署在海外数智化系统合规性，建立由内部专业律师和外部当地律师双向影响评估，来确保满足当地数据合规性。此外，持续关注全球合规政策的变动情况，动态调整数据合规红线要求及指引，满足数据合规性。

6.9.4 某能源企业数据跨境合规项目

面对全球化业务拓展的迫切需求，某能源企业着手构建以SAP为核心的全球一体化业务管理与服务体系，旨在无缝连接总部与遍布30余个国家和地区的境外子公司，加速数据流通与业务协同。然而，项目推进过程中遭遇了严峻的数据跨境合规挑战。该企业不仅要面对欧盟GDPR这一全球性数据保护标准的严格要求，还需应对多国独特的监管环境，由于海外合规筹备不足，导致部分境外子公司因合规顾虑拒绝参与网络连通与数据测试，项目因此被迫延期超过半年，海外市场拓展战略受阻；且企业运营过程中收集的能源类数据属于国家重要数据，总部高管赴海外任职过程中，能够通过VPN访问重要数据，一旦其办公终端被当地政府监控或罚没，面临重要数据泄露的潜在风险。

为突破这一困境，该企业携手IBM安全合规团队，共同制定了针对性的解决方案。IBM团队首先深度解析了GDPR及目标国家的数据跨境传输合规要求，为企业指明了合规路径。随后，通过组建跨部门的联合工作组，汇聚法务、科技、业务及境外机构等多方力量，协同制定并实施了详尽的行动计划。在此过程中，企业不仅建立了完善的个人信息保护制度、数据主体权利请求（DSR）处理流程，还强化了SAP系统的安全基线配置，并制定了数据泄露应急预案，有效提升了整体数据防护能力。

为实现快速突破，项目团队优先推动了首批次系统的成功上线，并通过建立总分联动的协同工作机制，为后续批次系统的顺利部署奠定了坚实基础。同时，IBM还为企业规划了长远的数据安全实施路线图，分阶段构建全面的数据安全管理体系。通过实施数据的安全分级分类，企业能够根据不同数据的重要性与敏感性，采取差异化的保护措施。此外，针对不同业务场景，IBM还为企业量身定制了多样化的数据安全解决方案，确保数据在跨境流动中的合法、安全、可控。这一系列举措不仅有效解决了当前的数据跨境合规难题，更为企业的全球化战略提供了坚实的数据安全保障。

6.9.5 某制造业人力资源运营模式转型项目

为了优化全球人力资源配置，提升管理效率，某制造业巨头启动了以HR系统为核心的全球一体化人力资源管理体系建设项目，旨在覆盖德国、英国、巴西、阿根廷、智利、美国、加拿大、印度、印度尼西亚等多个国家和地区。然而，在推进过程中，企业面临着多重挑战：不同国家/地区对于个人信息保护的法律法规差异显著，要求企业采取差异化的管控措施，实现“一国一策”的合规解决方案；同时，总部在域外合规体系建设和与境外子公司的协同机制上存在空白，数据安全体系的不完善，数据保留期限与安全控制要求的不明确，进一步加剧了项目的复杂性。

针对上述痛点，企业携手IBM安全合规团队，展开了一场深度而细致的合规建设之旅。IBM团队首先深入研究了目标国家的数据保护法律，特别是德国、英国、巴西、阿根廷、智利、美国、加拿大等关键地区的合规要点，为企业提供了精准的法律指引。随后，通过对HR业务流程的全面剖析，团队梳理出涉及的各种数据载体，包括系统表单、电子表格、图片文档、纸质文件等，并对这些数据中的隐私信息字段进行了细致的评估与筛选，最终在HR系统中精确定义了约600项隐私信息。

基于这些隐私信息及其处理场景，IBM团队与企业紧密合作，制定并落实了一系列合规策略，确保隐私数据的合法处理与保护。同时，结合HR业务的具体需求，团队还设计了人力资源运营模式转型项目的隐私数据合规方案，从技术、合规、法务等多个维度出发，构建了全方位、多层次的合规保障措施。这一方案的实施，不仅有效解决了企业在全球化人力资源管理中面临的合规难题，更为企业的长远发展奠定了坚实的合规基础。

6.9.6 某制造业海外一体化运营项目

某集团聚焦于提升海外子公司的实控权与数据管理的合规性，旨在通过精细化管理与技术创新，实现全球业务的无缝对接与高效运作。

在海外子公司实控权方面，项目特别关注美国法律对“独立性”的严格界定，通过确保中方人员合规持有工作签证、构建完整的组织架构以及明确规章制度发布流程，有效提升了子公司的独立运营能力。同时，项目设计了分层级授权审批的业务流程规则，既保证了总部的战略导向，又赋予了子公司灵活的业务执行权，实现了总部与子公司间的紧密协作与高效沟通。

在数据收集、存储、处理与销毁环节，项目严格遵守美国及国际数据保护法规，确保数据处理的全链条合规。针对数据收集，项目采用隐私政策声明方式，确保数据收集的合法性，并在正式上线前对隐私声明进行再次确认，以匹配最新的法律监管要求。在数据存储及传输上，项目灵活应对，对于敏感性较低的直销客户/经销商信息，选择在新加坡云节点存储，既符合美国法律要求，又有效控制了风险。然而，针对敏感个人数据的跨境访问，项目严格遵循拜登行政禁令，禁止从中国跨境访问此类数据，以确保数据安全的万无一失。对于数据处理，项目特别谨慎，对于涉及美国人身份信息、银行账户等高度敏感信息，法务团队建议优先本地化部署或使用中立第三国服务进行处理，以降低数据泄露风险。同时，在业务操作中，项目采取脱敏措施，减少敏感信息的展示，进一步保护个人隐私。在数据销毁方面，项目建立了完善的清理机制，对于经销商退出或数据收集期限到期的情况，及时进行匿名化、删除或销毁处理，确保个人信息的安全与合规。此外，项目还通过更新经销商协议或相关合同，灵活调整数据收集期限，以适应业务发展的实际需求。

6.9.7 某生物医药企业数据跨境合规项目

某生物医药企业为加速国际化进程，实现业务全球布局，启动了数据跨境合规项目，以欧盟和南美为初期试点区域，并规划逐步将业务拓展至全球。然而，在这一雄心勃勃的扩张计划中，企业遭遇了前所未有的挑战：全球范围内多样化的数据保护标准，特别是欧盟GDPR的严格规定，以及各国特定的数据监管要求，构成了复杂的合规网络。这要求企业不仅要精通多国法规的细枝末节，还需构建灵活多变的合规策略，以适应多变的法律环境。尤为紧迫的是，企业的数据安全保护能力尚不足以满足法律要求的高标准，这成为制约其海外拓展的关键因素。

为破解这一难题，企业携手IBM安全合规团队，共同制定了针对性的解决方案。IBM团队首先帮助企业深入梳理了土耳其、智利等目标国家的数据保护法律及跨境传输合规要点，为企业的合规工作奠定了坚实的法律基础。随后，团队细致梳理了企业的数据跨境场景、涉及的信息系统以及数据类型，全面掌握了数据跨境的全貌。在此基础上，团队通过调研评估，揭示了企业在数据安全与隐私合规建设方面的现状与不足，并针对性地提出了整改建议。

为确保隐私合规工作的有效落地，IBM团队还协助企业制定了企业级个人信息保护制度、数据主体权利响应流程以及数据泄露事件应急预案等关键文件，为企业合规工作提供了明确的指导依据。同时，团队还规划了数据安全隐私合规建设的长远路径，从夯实体系建设入手，逐步建立业务合规框架，并最终达成安全运营能力的全面提升。这一系列举措不仅帮助企业顺利跨越了合规门槛，更为其全球化战略的顺利推进奠定了坚实的基础。

6.9.8 某国有大型银行数据跨境项目

面对全球化背景下客户统一管理的迫切需求，某国有大型银行启动了复杂而关键的数据跨境项目。该项目旨在将散布于全球61个国家和地区，特别是25个“一带一路”沿线国家的海外分支机构客户数据，高效且合规地跨境传输至国内总部。然而，项目推进过程中，银行遭遇了多重挑战。

然而，项目初期便遭遇了多重痛点，海外主要国家和地区普遍实施了严格的个人信息分类分级监管，对数据安全的管控政策因地区而异，银行总行与海外机构需在国内数据安全分级的基础上，进一步深入研究并遵守各国家/地区的法律法规，精确识别敏感数据，并制定相应的控制措施。此外，部分国家/地区还提出了数据本地化存储和隔离存储的特定要求，这无疑增加了银行在服务器部署与架构设计上的难度，要求银行在保障合规的同时，也要兼顾业务运营的成本与效率。

为解决上述痛点，银行携手IBM安全合规团队，共同制定并实施了一系列解决方案。IBM团队凭借其丰富的专业知识和实践经验，协助银行全面梳理了中国、欧盟、巴基斯坦、印度、俄罗斯、卢森堡、韩国等关键目的国家/地区的数据保护法律及合规要点。在此基础上，团队进一步梳理了数据跨境合规的管控要点，明确了总部与分支机构在数据处理过程中的角色与责任，并起草了详尽的数据跨境协议，以规范双方的责任与义务，确保数据跨境传输的顺畅与安全。

针对客户个人信息的保护，IBM团队根据信息的敏感程度，为银行量身定制了数据保护策略，涵盖了数据加密、数据脱敏、访问控制、隔离存储等多个方面，以确保客户信息在跨境传输过程中的高度安全。同时，针对部分国家/地区的数据本地化存储要求，团队还结合银行的业务发展规划与运营成本考量，对海外回传数据的存储架构进行了针对性的技术改造，实现了数据的安全、合规存储。

最终，在IBM安全合规团队的鼎力支持下，该国有大型银行成功克服了数据跨境项目中的重重困难，实现了全球客户数据的统一管理，为银行的国际化战略注入了新的动力。这一案例不仅彰显了银行在数据跨境管理领域的创新能力与决心，也为其他金融企业/机构提供了宝贵的借鉴与参考。

07

中国企业出海数据合规关键行动建议

精准识别：数据合规要求

精细梳理：数据出境场景

规范评估：数据合规差距

高效修复：合规改进建议

标准编制：出境评估报告

体系搭建：长效管理机制

为了加速推动中国企业在全球化浪潮中的数据安全与合规性建设，IBM携手腾讯，深度融合双方顶尖的解决方案与技术资源，共同推出了、的实战指南，旨在深入剖析企业当前状况，精准定制并高效实施合规优化方案，辅以监管申报与备案的全方位支持服务，保障企业数据在全球市场自由、安全且合规地流通与运营，助力企业在全球舞台上稳健前行，实现可持续发展。

精准识别：数据合规要求 7.1

中国企业国际化征程的起点，在于精确识别并深入理解目标国家的数据安全法律与监管框架。这需企业详尽调研目标市场的数据保护政策、隐私法律架构及行业专属规范，涵盖数据类型界定、跨境传输评估、适用条件与豁免条款等关键要素，以确保业务活动的全球合规性。进而，企业应开展深度数据合规适用性分析，建设数据跨境合规基线，将外部法律法规要求融入内部管理体系，实现外规内化，形成数据跨境合规库，确保企业运营流程与国际标准无缝对接。鉴于跨境数据流动的复杂环境，企业应建立合规基线动态跟踪体系，持续剖析跨境监管趋势，及时响应政策变动，构建坚不可摧的风险防御网，助力企业在全球市场的稳健拓展与持续繁荣。

参考本书第三章各国家地区数据合规法规概览，企业可快速掌握多国数据合规要点。

精细梳理：数据出境场景 7.2

中国企业出海第二步是要梳理数据出境场景。此过程需企业全面排查数据跨境传输的具体场景，确保无一遗漏。首要任务是细致分析这些数据在跨境过程中所涉及的具体类型，明确数据管控对象，主要聚焦对重要数据和个人信息的识别。在此基础上，企业应构建详尽的数据流转地图，清晰描绘数据的流动路径及处理活动。这一举措旨在实现对数据跨境活动的全方位、精准化监控与高效管理，确保数据流动的合规性与安全性。

参考本书第4.2.1节企业出海数据现状概览，企业可快速掌握数据出境场景梳理的具体方法与实践策略。

规范评估：数据合规差距 7.3

基于已识别的合规要求和梳理的数据出境场景，出海企业应启动数据合规差距评估工作。此环节的首要步骤是构建数据安全合规与风险评估模型，系统化捕捉企业在数据跨境传输过程中可能遭遇的合规短板与安全威胁，通过这一模型，企业能够深入剖析其数据安全风险现状与既有合规框架之间的偏差，为后续制定精准高效的合规策略与改进措施奠定坚实基础。

参考本书数据安全合规风险评估，企业可快速掌握数据安全合规风险评估的内容及方法。

高效修复：合规改进建议 7.4

在数据跨境合规的差距修复进程中，企业需从法务、管理及技术三个维度制定详尽的差距整改措施，并制定整改工作分工矩阵，明确各责任部门与个人的职责，并对整改进度进行持续跟踪与报告，确保整改措施的有效执行与合规目标的顺利达成。

- **法务层面，强化合规基石，筑牢法律防线：**重点在于优化合同协议条款、确保个人信息主体同意授权的有效获取，快速响应监管要求，不断修订和完善数据出境管理制度，确保制度的有效性和前瞻性。
- **管理层面，细化机制流程，培养合规意识：**根据数据的重要程度和危害程度，强化数据分类分级机制，并精细化落实数据分类分级工作；构建高效的数据主体权利响应机制，确保数据主体权利响应的有效落实；加强数据权限授权审批机制，实施严格的权限控制策略，防止数据泄露和滥用；建立定期的数据合规审计制度，定期开展数据合规审计等工作。
- **技术层面，创新技术手段，提升安全合规：**通过采取本地化存储策略、加强存储与传输过程中的数据加密措施，实施数据脱敏技术等工作，全方位提升数据跨境流动的安全性与合规性。

为了更高效地推进整改工作，确保短期内的显著成效，企业可以开展短期方案，包括但不限于：

- 组建专业合规团队，设立数据保护官（DPO）或数据安全官（CISO）负责整体数据合规策略的规划与执行，并组建一个包含法务、IT技术、业务部门代表等多部门成员的跨职能合规小组。
- 制定并执行紧急行动计划，快速审查与数据跨境流动相关的合同与协议，识别并修改不符合当前法律法规要求的条款，并启动数据分类分级工作，为后续的数据管理、存储和传输提供基础。
- 强化技术防护措施，部署临时数据加密方案，对跨境传输的数据进行加密保护，同时实施快速响应的数据脱敏技术，对非必要信息进行脱敏处理，降低数据敏感度，同时保持数据的可用性和完整性。

标准编制：出境评估报告 7.5

各国及地区均对数据出境的评估要求日益严格，部分国家更是明确规定了提交详尽数据出境评估报告的要求，以作为监管机构、合作伙伴及数据处理相关方评估数据合规风险的关键依据。以我国为例，数据出境自评估报告聚焦对出境数据的风险状况全面剖析、对境外接收方所在国或地区法律法规政策环境的细致审视以及企业为有效缓解风险而实施的具体保护策略与措施。因此，企业在完成数据出境合规差距的整改工作后，应紧密结合我国及目标国家/地区的具体监管要求，编制数据出境评估报告，准备监管申报材料。一旦获得监管部门的正式批准，企业方可正式开展数据出境活动。在开展数据出境活动中，企业应严格遵循评估报告中的数据出境计划及保护措施，确保数据出境流程的严谨执行。同时，建立健全的监控体系，以实现对数据传输、存储及处理等全活动链条进行合规性监督，确保符合监管合规要求。

体系搭建：长效管理机制 7.6

中国企业的出海之路，非一朝一夕之功，而是一场需要坚韧不拔、持续深耕的长期征程。为此，构建数据跨境合规管理的长效机制成为企业不可或缺的战略选择。通过建立数据跨境管理组织和制度，制定常态化的数据出境管理流程、工具和工作模板，构建数据合规技术和运营体系等工作，形成数据跨境管理的能力体系。企业可以基于组织、制度、技术、运营等方面建设数据安全与合规体系，在保障数据安全与合规的同时，加速其国际化步伐，拓展全球业务版图，赢得更加广阔的发展机遇与空间，实现企业的可持续增长与繁荣。

参考本书第4.2节数据安全与合规体系，企业可快速掌握基于组织、制度、技术、运营搭建数据安全合规体系的内容及方法。

【免责声明】

本文档提及的法律法规仅限于文档发布日期前所公开发布的法案，不包括未来可能出现的法律法规变更。本文档不由律师撰写，不构成法律意见或建议，资料的收集也难免存在缺失或遗漏，读者应根据自身企业状况咨询专业法律机构。对因该等信息的使用可能产生的任何责任，均由读者自行承担。

本文档为自最初公布日期起的最新版本，IBM 或腾讯保留随时对其进行修改的权利。IBM或腾讯并不一定在开展业务的所有国家或地区提供所有产品或服务。

本文档内的信息“按现状”提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 或腾讯产品根据其提供时所依据的协议条款和条件获得保证。

本文档的目的仅为提供通用指南。它并不旨在代替详尽的研究或专业判断依据。由于使用本出版物对任何企业或个人所造成的损失，IBM或腾讯概不负责。

本文档中使用的数据可能源自第三方，IBM或腾讯并未对其进行独立核实、验证或审查。使用此类数据的风险由读者自行承担，IBM或腾讯不作任何明示或默示的声明或保证。

每日免费获取资料

- 每日微信群内分享7+最新行业报告；
- 每周分享当周华为街日报、经济学人；
- 行业报告均为公开版，权利归原作者所有，参一江湖仅分发做内部学习。

| 英语外刊 | 行业报告 | 行业社群 | 参一江湖·聚焦行业前沿



关注公众号
领取粉丝福利