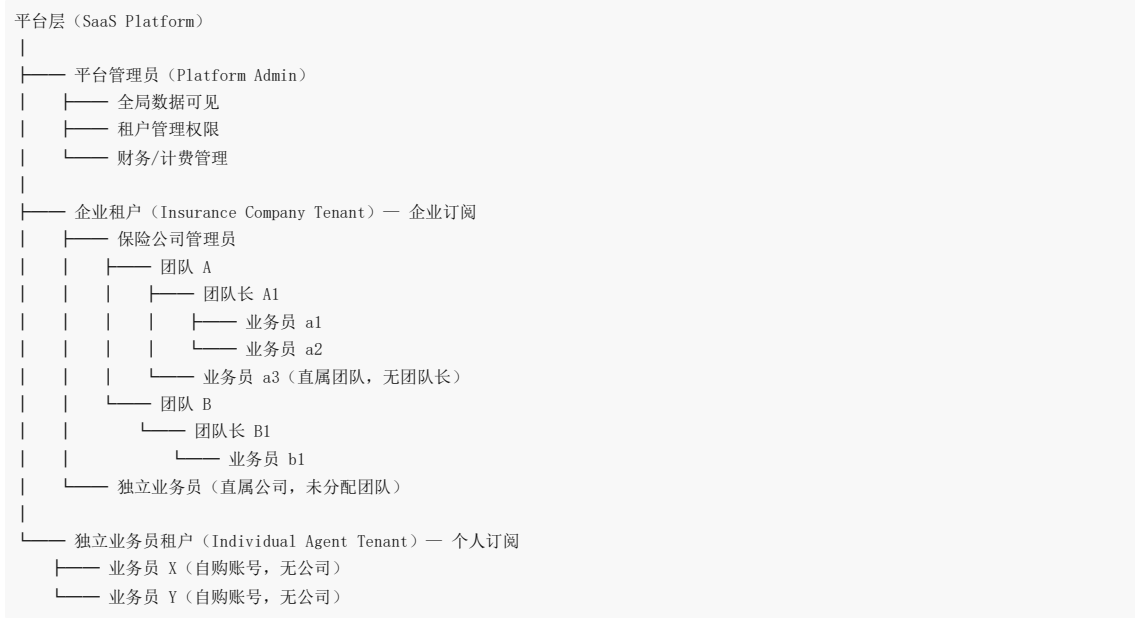


平台租户体系 & 权限设计规范

版本：1.0 | 日期：2026-02-19 覆盖端：平台管理员端·保险公司管理员端·业务员端（团队长视角） 设计原则：数据最小可见原则·权限最小化·租户严格隔离·账号开通流程标准化

第一部分：租户体系架构

1.1 租户层级结构



1.2 四类角色定义

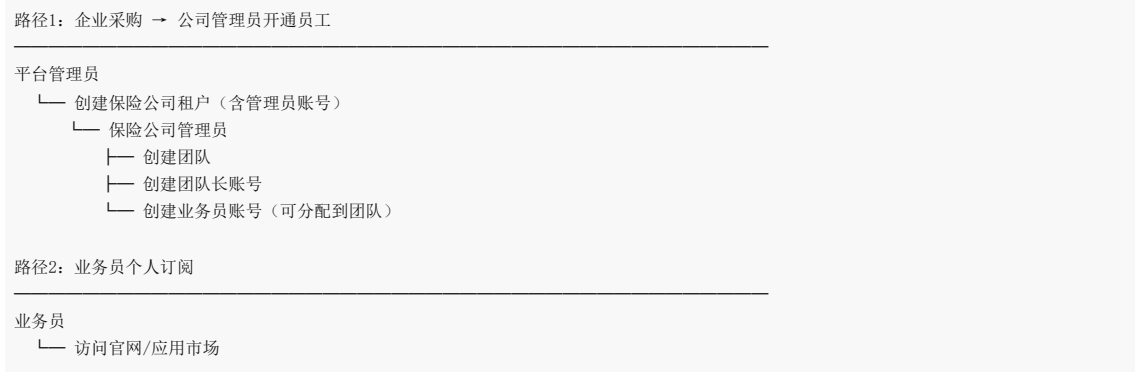
角色	所属层级	账号来源	数据可见范围	典型场景
平台管理员	平台层	内部创建	全平台所有公司/业务员数据	平台运营人员
保险公司管理员	企业租户层	平台管理员开通	本公司内所有团队/业务员数据	险企IT/行政/营业部主任
团队长	团队层	保险公司管理员开通	本团队成员 + 自身数据	营业组组长、主管
业务员	个人层	多渠道 (见1.3)	仅自身数据	保险代理人、经纪人

重要区分： 业务员存在两种形态：

- 企业业务员：** 归属某保险公司，由公司管理员创建账号
- 独立业务员：** 自行购买平台订阅，不归属任何公司（形成单人租户）

第二部分：账号开通路径

2.1 路径总览



└─ 自助注册

└─ 选择套餐并支付

└─ 账号自动激活（独立业务员身份）

路径3：平台管理员直接开通业务员

平台管理员

└─ 后台手动创建业务员账号

└─ 设置为独立业务员身份

路径4：邀请注册（业务员拉新）

已有业务员

└─ 生成邀请链接（含邀请码）

└─ 新业务员点击注册

└─ 完成支付 → 账号激活

└─ 邀请人获得积分奖励（平台配置）

2.2 路径1：企业租户开通流程

Step 1：平台管理员创建保险公司租户

操作路径：平台Admin → 租户管理 → 新建租户

字段	必填	说明
公司名称	✔	正式营业执照名称
公司简称	✔	用于后台展示，2-10字
营业执照编号	✔	合规校验
保险许可证编号	✔	合规必填
联系人姓名	✔	技术对接负责人
联系人手机	✔	将收到管理员账号激活短信
联系人邮箱	✔	账号初始密码发送至此邮箱
席位数上限	✔	企业购买的业务员账号名额上限
合同有效期	✔	订阅有效期起止日期
账号状态	系统	默认「待激活」，发送激活邮件后变为「正常」

创建完成后：自动生成保险公司管理员账号，发送激活邮件至联系人邮箱，管理员首次登录须修改密码。

Step 2：保险公司管理员创建团队

操作路径：公司管理后台 → 组织架构 → 新建团队

字段	说明
团队名称	如「光明营业组」「精英团队」
所属大区/分公司	多级组织（可选）如：华东区 → 上海分公司 → 精英团队
团队长	从已有员工中指定，或稍后分配

Step 3：保险公司管理员创建员工账号

操作路径：公司管理后台 → 员工管理 → 新增员工

字段	必填	说明
姓名	✔	真实姓名
手机号	✔	登录账号，同时接收激活短信
员工编号	✔	公司内部工号
角色	✔	团队长 / 业务员

所属团队	—	可不分配（独立于团队直属公司）
代理人证书编号	—	合规信息，非必填
入职日期	—	用于「新人追踪」功能

账号创建后：发送激活短信至员工手机，员工首次登录设置密码并完善个人资料。

席位余量逻辑：

- 每次创建员工账号，消耗1个席位
- 席位用完后提示「席位已满，请联系平台扩充席位」（不可自助扩充，须平台审批）
- 员工账号禁用后，席位**不自动释放**（防止恶意刷号），须由平台管理员手动释放

2.3 路径2：业务员个人订阅流程

页面流程（官网/App端）：

落地页（产品介绍）

→ [立即体验] → 手机号注册（OTP验证）

→ 选择套餐

- 个人版：¥59/月（月付）/ ¥588/年（年付，省96元）
- 团队版（仅限团队长+≥3人团队）：¥299/月（含5个席位）

→ 支付（微信支付 / 支付宝）

→ 账号激活，进入引导页

- 是否关联公司？
 - 是 → 输入公司邀请码（关联到企业租户）→ 转为企业业务员身份
 - 否 → 作为独立业务员激活

套餐说明：

套餐	价格	核心功能	限制
个人版（月付）	¥59/月	客户管理/信号工作台/计划书生成/积分功能	客户数上限500人
个人版（年付）	¥588/年	同上 + 行为数据看板	客户数上限1000人
团队版	¥299/月	含5席位 + 团队仪表盘 + 成员管理	可扩展席位+¥49/人/月

参考自第四轮头脑风暴定价研究：个人业务员≤59元/月接受度最高；团队长愿付299-499元/月。

免费试用：注册后前30天全功能试用（需绑定手机），到期前7天推送续费提醒。

2.4 路径4：邀请注册详细设计

- 业务员在「工具箱」生成个人邀请链接（含邀请码 referral_code）
- 被邀请人注册并完成首次付费后，邀请人获得平台奖励积分（由平台运营配置，如首月费用的20%积分奖励）
- 邀请记录在业务员端「推荐记录」中可查

第三部分：权限矩阵

3.1 数据可见范围（Data Scoping）

平台管理员

- 可见：全部公司 + 全部业务员 + 全部客户（跨租户汇总）

保险公司管理员（tenant_id 隔离）

- 可见：本公司内所有团队 + 所有员工 + 员工的客户数据汇总
- 不可见：其他公司数据；具体客户个人信息（仅看汇总指标）

团队长（team_id 隔离）

- 可见：本团队所有成员的业务数据 + 自身客户详情
- 不可见：其他团队数据；自身团队成员的客户个人信息（仅看汇总）

业务员（agent_id 隔离）

- 可见：仅自身绑定客户的完整数据 + 自身业务数据
- 不可见：任何其他业务员的数据

3.2 功能权限矩阵

功能模块	平台管理员	公司管理员	团队长	业务员
租户管理				
创建/删除保险公司租户	✓	✗	✗	✗
查看所有租户列表	✓	✗	✗	✗
调整席位数量	✓	申请	✗	✗
员工账号管理				
创建保险公司管理员	✓	✗	✗	✗
创建团队队长账号	✓ (独立)	✓ (本公司)	✗	✗
创建业务员账号	✓ (独立)	✓ (本公司)	✗	✗
禁用/启用员工账号	✓	✓ (本公司)	✗	✗
重置员工密码	✓	✓ (本公司)	✗	✗
调整员工团队归属	✓	✓ (本公司)	✗	✗
组织架构管理				
创建/编辑/删除团队	✓	✓ (本公司)	✗	✗
指定/调整团队队长	✓	✓ (本公司)	✗	✗
查看组织架构图	✓	✓ (本公司)	✓ (本团队)	✗
数据看板				
平台级大盘 (跨公司)	✓	✗	✗	✗
公司级大盘	✓ (只读)	✓	✗	✗
团队级数据	✓ (只读)	✓ (只读)	✓	✗
个人数据	✓ (只读)	✓ (只读)	✓ (只读)	✓
客户数据				
查看客户列表 (汇总)	✓	✓ (本公司汇总)	✓ (本团队汇总)	✓ (自己的)
查看客户详情 (个人信息)	✗	✗	✗	✓ (自己绑定的)
导出客户数据	✓ (脱敏)	✓ (本公司脱敏)	✗	✓ (自己的)
积分管理				
积分规则配置	✓	✗	✗	✗
查看积分大盘	✓	✓ (本公司客户积分)	✗	✗
营销策略				
创建/编辑营销策略	✓	✗	✗	✗
查看策略触达数据	✓	✓ (本公司范围)	✗	✓ (自己客户的)
内容管理				
内容审核	✓	✗	✗	✗
上传素材/话术	✓	✓ (本公司专属内容)	✗	✓ (个人话术收藏)
订阅计费				
查看全平台收入	✓	✗	✗	✗
查看本公司订阅状态	✓	✓	✗	✗
管理个人订阅	✗	✗	✗	✓ (自购用户)

3.3 客户数据归属规则

客户归属链：客户 → 绑定业务员 → 所属团队 → 所属公司

场景	规则
业务员离职/账号禁用	客户数据归属公司，保留原记录，公司管理员可重新分配给其他业务员
业务员转团队	客户随业务员转移，团队数据看板实时更新
独立业务员停止订阅	客户数据保留90天（只读），续订后恢复，90天后客户数据归档
同一客户被多个业务员联系	平台判重（手机号唯一），客户归属先创建的业务员，后续业务员只能申请转移

第四部分：各端UI设计

4.1 平台管理员端 — 租户管理模块（新增）

侧边栏新增：租户管理（在现有模块基础上扩展）

4.1.1 保险公司租户列表

租户管理 • 保险公司 [+ 新建租户]							
[全部 (12)] [正常 (10)] [试用期 (1)] [已到期 (1)] [已禁用 (0)]							
公司名称	席位	已用	到期日	状态	操作		
平安人寿（沪）	200	156	12-31	正常	[详情][配置]		
中国人寿（京）	500	312	06-30	正常	[详情][配置]		
太平洋保险	50	12	03-01	即将到期	[详情][续约]		
新华保险	30	3	——	试用期	[详情][转正式]		

席位使用率视觉：

- 使用率 < 60%：绿色进度条
- 60-85%：橙色进度条 + 提醒
- 85%：红色进度条 + 「建议扩充席位」

4.1.2 保险公司租户详情页

← 平安人寿（上海）				[禁用租户] [编辑]	
基本信息		订阅信息			
公司全称：平安人寿...		套餐类型：企业版			
许可证编号：XXXX		席位数：200个			
联系人：张经理 138xxxx		已用席位：156个（78%）			
注册日期：2025-01-15		到期日：2026-12-31			
		[调整席位] [延长有效期]			
Tab：[员工总览] [数据大盘] [操作日志]					
员工总览					
管理员账号：张经理（可重置密码）					
团队数：8个 团队长：8人 业务员：148人 未分配：0人					
		[重置管理员密码]			
数据大盘（只读汇总）					
本月新增客户	本月MAU	月测评完成率	本月成交保费（脱敏）		
1,234人	3,456人	68%	¥ 231万		

4.1.3 独立业务员管理

独立业务员管理 [手动创建] [导出]			
[全部 (523)] [订阅中 (401)] [试用期 (67)] [已过期 (55)]			

姓名/手机	套餐	客户数	到期日	操作
刘伟 188xxxx	年付个人	234	2026-08	[详情][强制续约]
王芳 139xxxx	月付个人	89	2026-03	[详情][续约提醒]

4.1.4 平台级跨公司大盘

平台总览大盘															[本月 ▼]					[导出报告]									
企业租户 独立业务员 席位总数 席位使用 全平台MAU 测评完成 K因子 月收入（脱敏）																													
12		523		1,280		891		28,345		61%		1.38		¥ 42万															
各公司业务对比（只读，不显示具体公司名称对外，仅内部可见）																													
公司A		MAU 8,234		测评完成率 72%		本月新增客户 456人																							
公司B		MAU 5,123		测评完成率 55%		本月新增客户 234人																							
•		•		•																									
收入趋势（月度折线图）															席位使用率分布（饼图）														

4.2 保险公司管理员端（新增专属门户）

技术栈: Vue3 + Element Plus + Tailwind CSS (PC端, 与平台Admin分离部署但共享设计系统)

顶部导航 (TopBar) :

[平安人寿（上海）Logo] [概览] [组织架构] [员工管理] [数据看板] [设置] [张经理 ▼]

側边栏（收起时显示图标）：

- 📊 总览大盘
- 📁 组织架构
 - 👤 员工管理
 - ↳ 全部员工
 - ↳ 团队管理
 - ↳ 待入职
- 📈 数据看板
 - ↳ 整体数据
 - ↳ 团队对比
 - ↳ 业务员排行
- 📁 内容管理（公司专属内容）
 - ⚙️ 公司设置
 - ↳ 基本信息
 - ↳ 席位管理
 - ↳ 通知设置

4.2.1 公司总览大盘

[illegible]

● 3名业务员账号已超过60天未登录	[查看详情]
--------------------	------------------------

4.2.2 组织架构页

展示形式：树形图 + 列表切换

组织架构	[树形图]	[列表]	[新建团队]	
平安人寿（上海）				
└─ 精英团队（12人）	团队长：陈志远			
└─ └─ 陈志远（团队长）	✓ 活跃			
└─ └─ 刘明（业务员）	✓ 活跃	客户：156人	本月新增：23人	
└─ └─ 王芳（业务员）	⚠ 低活跃	客户：89人	本月新增：5人	
└─ └─ ...				
└─ 成长团队（8人）	团队长：李华			
└─ └─ ...				
└─ 未分配（3人）	无团队长			
└─ └─ 张三（业务员）	❄ 未激活			
[调整团队归属] [设置团队长] [批量导入员工]				

4.2.3 员工管理 — 员工列表

员工管理

+ 新增员工

[批量导入]

[导出]

[全部 (156)]

[正常 (148)]

[待激活 (5)]

[禁用 (3)]

筛选：

团队

角色

活跃状态

入职日期

搜索姓名/工号

姓名	角色	工号	所属团队	客户数	最近活跃	操作
陈志远	团队长	A001	精英团队	156	今天	<div><div>[详情]</div><div>[重置密码]</div></div>
刘明	业务员	A023	精英团队	89	今天	<div><div>[详情]</div><div>[重置密码]</div></div>
张三	业务员	A089	未分配	0	从未登录	<div><div>[详情]</div><div>[发激活]</div></div>
王旧	业务员	A045	成长团队	45	65天前	<div><div>[详情]</div><div>[禁用]</div></div> <div>← 橙色行</div>

新增员工表单：

新增员工	[×
姓名 *	<input type="text"/>
手机号 *	<input type="text"/> （将作为登录账号）
员工工号 *	<input type="text"/>
角色 *	<input type="radio"/> 业务员 <input checked="" type="radio"/> 团队长
所属团队	[精英团队 ▼] （不选则为未分配）
代理人证书编号	<input type="text"/> （选填）
入职日期	[日期选择器]
<input checked="" type="checkbox"/> 创建后立即发送激活短信给员工	
[取消]	[确认创建]








批量导入（Excel模板）：

- 提供标准Excel模板下载（含字段说明和示例数据）
- 上传后系统校验：手机号重复、工号重复、格式错误
- 校验失败展示错误行列表，可下载错误报告
- 校验通过后预览导入结果，确认后批量创建

4.2.4 数据看板 — 团队对比

团队业务对比 [本月 ▼] [按新增客户 ▼排序]					
维度选择: <input checked="" type="checkbox"/> 新增客户 <input checked="" type="checkbox"/> 测评完成 <input checked="" type="checkbox"/> 月活 <input type="checkbox"/> 成交保费					
团队名称	人数	新增客户	测评完成	月活率	趋势
精英团队	12	102	78%	91%	↑ 较上月+12%
成长团队	8	45	62%	75%	→ 较上月持平
新人团队	6	12	40%	50%	↓ 较上月-8%
[柱状对比图, 每团队一色]					

4.2.5 数据看板 — 业务员排行

业务员排行 [本月 ▼] [按新增客户 ▼] [全公司 ▼]						
排名	姓名	团队	新增客户	测评率	月活	操作
	刘明	精英	45	88%	 高活	[查看详情]
	陈芳	精英	38	82%	 正常	[查看详情]
	王志国	成长	32	75%	 正常	[查看详情]
•	•	•	•	•	•	
154	张旧员	未分配	0	0%	 沉睡	[查看][提醒]




4.3 业务员端 — 团队长专属视图扩展

(在现有agent-app-ux-spec.md基础上, 增加团队管理权限说明)

团队长可执行 (相比普通业务员新增) :

功能	团队长权限	说明
查看团队仪表盘		团队成员活跃度/新增客户/转化漏斗 (已有设计)
查看成员业务数据 (汇总)		不含成员客户个人信息
设置团队任务	 (Phase 2)	给团队下达阶段目标
新增团队成员		无权限, 须公司管理员操作
删除/禁用成员		无权限, 须公司管理员操作

团队长视角 — 查看成员客户汇总 (仅聚合数据, 不可下钻到个人客户) :

← 刘明 的业务数据	
精英团队 • 业务员	
本月 (2026年2月)	
新增客户	测评完成 K因子 月活客户
45人	88% 1.6 156人
客户质量分布	
高意向	 34人
保障缺口大	 67人
沉睡中	 12人
⚠ 团队长注意:	
该成员上月K因子1.6, 本月目前1.1	
[给刘明发消息]	

4.4 业务员端 — 个人订阅管理

位置： 个人中心 → 我的订阅

←	我的订阅	
[个人版 • 年付]		
✔ 订阅有效		
到期日：2026-08-15（还有 177天）		
客户数：234 / 1,000人上限		
<div><div></div></div> 23%		
[立即续费] [升级套餐]		
订阅记录		
2025-08-15 年付个人版 ¥588		
2024-08-15 年付个人版 ¥588		
推荐奖励		
累计推荐：3人 获得积分：+1,500		
[获取推荐链接]		
— 我的企业归属 —		
当前：独立业务员（无公司）		
[输入公司邀请码关联企业]	← 可随时关联到企业	

订阅到期提醒推送：

- 到期前30天：站内信提醒
- 到期前7天：APP推送 + 站内信
- 到期前1天：APP推送 + 短信
- 到期后：功能降级为只读，客户数据保留90天

第五部分：数据隔离技术规范

5.1 租户隔离方案

采用：共享数据库 + 行级安全 (Row-Level Security)

核心原则：所有业务表添加 `tenant_id`，通过数据库RLS策略 + 应用层双重校验确保隔离。

关键表字段设计:

```
-- 租户表
tenants (
  id UUID PRIMARY KEY,
  tenant_type ENUM('platform', 'company', 'individual'),
  company_name VARCHAR(100),      -- 企业租户: 公司名称
  license_no VARCHAR(50),         -- 营业执照编号
  insurance_license_no VARCHAR(50), -- 保险许可证编号
  seat_limit INT,                 -- 席位上限
  seat_used INT DEFAULT 0,
  subscription_status ENUM('trial', 'active', 'expired', 'disabled'),
  subscription_expires_at TIMESTAMP,
  created_at TIMESTAMP
)

-- 用户账号表
users (
  id UUID PRIMARY KEY,
  tenant_id UUID REFERENCES tenants(id),
  role ENUM('platform_admin', 'company_admin', 'team_leader', 'agent'),
  team_id UUID REFERENCES teams(id) NULLABLE, -- 团队归属
  name VARCHAR(50),
  phone VARCHAR(20) UNIQUE,
```

```
employee_no VARCHAR(50), -- 企业员工工号
status ENUM('pending_activation', 'active', 'disabled'),
last_login_at TIMESTAMP,
created_at TIMESTAMP
)

-- 团队表
teams (
  id UUID PRIMARY KEY,
  tenant_id UUID REFERENCES tenants(id), -- 所属租户
  name VARCHAR(100),
  leader_id UUID REFERENCES users(id) NULLABLE, -- 团队长
  parent_team_id UUID REFERENCES teams(id) NULLABLE, -- 支持多级团队
  created_at TIMESTAMP
)

-- 客户表（行级隔离）
customers (
  id UUID PRIMARY KEY,
  tenant_id UUID REFERENCES tenants(id), -- 所属租户
  agent_id UUID REFERENCES users(id), -- 绑定业务员
  phone VARCHAR(20),
  name VARCHAR(50),
  -- ...其他字段
  created_at TIMESTAMP
)
```

应用层数据查询规则：

调用角色	WHERE条件	说明
平台管理员	无限制	跨租户查询
公司管理员	tenant_id = current_tenant_id	仅本公司数据
团队长	team_id = current_team_id OR agent_id = current_user_id	本团队+自身
业务员	agent_id = current_user_id	仅自身

5.2 席位控制

```
-- 席位使用校验（创建员工账号时）
IF tenants.seat_used >= tenants.seat_limit:
    RAISE EXCEPTION '席位已满，请联系平台扩充席位'
ELSE:
    CREATE user
    UPDATE tenants SET seat_used = seat_used + 1

-- 席位释放（平台管理员手动操作）
UPDATE tenants SET seat_used = seat_used - 1
-- 注：禁用账号不自动释放席位，须手动操作
```

5.3 跨租户数据禁止清单

- ✗ 不允许任何角色查看其他租户的客户个人信息
- ✗ 不允许公司管理员查看平台级财务数据
- ✗ 不允许业务员查看其他业务员的客户列表
- ✗ 平台管理员查看客户数据时，手机号/身份证号等必须脱敏展示
- ✗ 数据导出API必须校验导出范围与用户权限匹配

第六部分：账号安全规范

6.1 密码与登录

规则	说明
初始密码	系统随机生成，通过短信/邮件发送，首次登录强制修改

密码强度	8位以上，含大小写字母+数字
密码有效期	90天强制修改（平台管理员、公司管理员）；业务员无强制
登录失败锁定	连续5次失败→账号锁定30分钟，通知账号持有人
多设备登录	默认允许，业务员可在设置中关闭
Session有效期	移动端：7天；PC端：8小时

6.2 操作日志

所有账号管理操作（创建/禁用/重置密码/权限调整）强制记录操作日志：

字段	说明
operator_id	操作人ID
operator_role	操作人角色
target_user_id	被操作账号ID
action	操作类型
ip_address	操作IP
user_agent	浏览器/设备信息
created_at	操作时间

操作日志保留期：180天。

附录：角色权限快速参考卡

角色权限速查卡					
能力	平台管理员	公司管理员	团队长	业务员	
创建公司账号	✓	✗	✗	✗	
创建员工账号	✓	✓	✗	✗	
创建团队	✓	✓	✗	✗	
看全平台数据	✓	✗	✗	✗	
看本公司数据	✓只读	✓	✗	✗	
看本团队数据	✓只读	✓只读	✓	✗	
看自身数据	✓只读	✓只读	✓	✓	
看客户个人信息	✗脱敏	✗脱敏	✗	✓自己的	
导出客户数据	✓脱敏	✓脱敏	✗	✓自己的	
积分规则配置	✓	✗	✗	✗	
营销策略配置	✓	✗	✗	✗	
内容审核	✓	✗	✗	✗	
管理个人订阅	✗	✗	✗	✓自购	

本文档配合以下规范使用：

- [客户端UI/UX规范](#)
- [业务员端UI/UX规范](#)
- [平台运营端UI/UX规范](#)
- [积分与活动体系设计](#)
- [客户标签与营销自动化](#)