Neocrm 销售易

销售易信任白皮书

销售易研究院

销售易研究院

目录
CONTENTS

1 数据安全成当今企业必修课

1.1 数据安全事件频发 各国立法严惩

数字经济的到来就像是一把双刃剑。一方面“数字经济”已经成为当前各国在下一阶段的重要发力点，甚至有人指出掌握数字经济发展的先机就是掌握了“强国密码”。另一方面，在发展数字经济的过程中，**由于企业重视程度不够、监管法规尚不完善，引发了数据安全及隐私保护问题。**仅2021年全球范围内就发生了多起影响恶劣的数据安全、隐私保护事件。

* 2021年部分数据安全及隐私保护事件

注：DDoS攻击、黑客加密勒索、数据泄露等，都是通过破坏数据的保密性、完整性、可用性影响企业，都属于数据安全事件范畴，随着数据安全和隐私保护的边界逐渐模糊，当泄露的数据包含个人信息时，也可称为隐私保护事件或者隐私泄露事件。

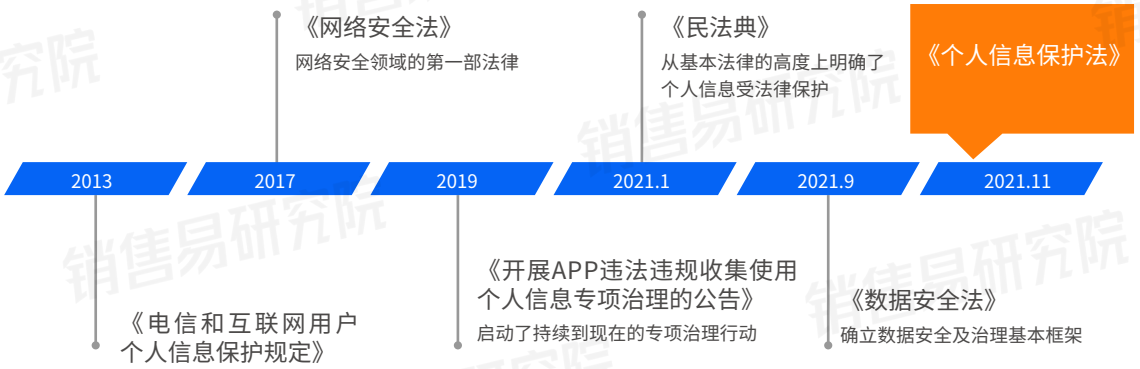
数据安全、隐私保护事件频发，促使各个国家纷纷出台相关法律，加强数据监管。目前全球已经有80%国家完成相关立法工作。

- 2018年5月25日，欧盟出台《通用数据保护条例》，即GDPR。
- 2018年7月，印度发布了《个人数据保护法案(草案)》（PDP）。
- 2018年8月，巴西通过了第一部综合性的数据保护法，《通用数据保护法》(GDPL)。
- 2020年CCPA作为美国“最全面的个人隐私保护法”在加州开始实施。

立法逐渐完善的同时，处罚也在逐渐加重：

- 2018年，伦敦英国航空公司因为违反GDPR的隐私规定，被开出2000万英镑的罚单。
- 2019年，万豪酒店因为黑客窃取数据，导致3.39亿条客户信息外泄，被英国监管机构罚款1.6亿元。
- 2020年，Facebook因为剑桥事件，导致用户数据遭到泄露，被罚50亿美元，成为美国政府开出的最大一笔罚单。

我国也随之启动相关动作，继《网络安全法》后，2021年出台《数据安全法》和《个人信息保护法》，并引入了处罚机制。《个人信息保护法》规定，情节严重的违法行为，最高可处5000万元或者上一年度营业额5%的罚款，并可以对相关责任人员作出相关从业禁止的处罚。



* 我国在数据安全和隐私保护方面的立法动作

立法加快、处罚加重让数据安全、隐私保护等问题在明确的条例下规范管理，有效促进了数字经济有序运转。但另一方面，全球范围内加快推进数据安全和隐私保护立法，企业需要不断理解并适应新法，确保业务合法合规开展，**对于企业来说，尤其是跨国企业和出海企业，因业务覆盖多个国家和地区，需要满足不同地区的法律要求，无形中增加了企业的合规难度和合规成本。**

1.2 危机背后，企业何去何从

从集中立法到巨额处罚，可以看出数据安全、隐私保护、合规已经是数字时代的全球话题，也是当今企业的必修课。然而在大多数企业中，相比数据安全问题带来的损失，业务投入带来的增长对企业来说更具有确定性，所以数据安全、隐私保护、合规一直都处于“重要但不紧急“的尴尬状态，优先级放在业务发展之后。在安永发布的《2021全球信息安全调查报告（GISS）》中称，“约三分之二的中国公司表示诸如勒索软件等破坏性网络攻击的数量在过去12个月中有所增加，但应对网络安全风险的预算仍然很少”。**数据安全需要持续投入人力和物力，而大多数中小企业无力支撑或者支撑不全面。**

那么企业应该如何在保障数据安全、隐私保护、合规的同时兼顾业务发展？如何在较低的成本投入下获得安全能力最大化，让数据安全为业务发展保驾护航？

不少企业选择了自研或购买软件进行安装部署的方式，但是这种方式需要企业采购设备并投入运维团队长期维护，除此外，传统软件模式灵活性差，无法应对业务的快速调整。而SaaS模式因其订阅制付费方式，帮助企业省去基础设施采购费用和安全维护费用，并且具备灵活性和敏捷性，在降本增效方面具备天然优势。成为企业兼顾业务发展和数据安全的解决方案。

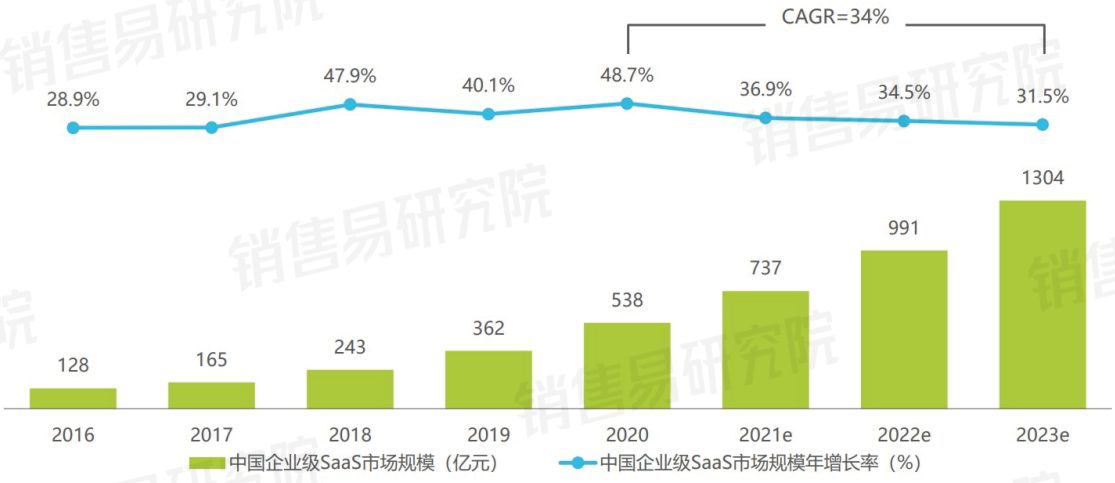
2 CRM安全性对企业至关重要

企业在数字化运营过程中，往往会通过CRM、ERP、PM、HRM等线上系统完成数据的收集和沉淀。其中，CRM系统更多地用于收集和沉淀企业的业务数据和个人数据，其安全性对企业来说至关重要。

2.1 传统软件模式和SaaS模式的安全差异

当前企业的CRM选型多面临传统软件模式或SaaS模式的选择。随着SaaS在国内的发展与成熟，其相对传统软件模式**开发时间短、投入成本低、更新迭代快、更具开放性，逐渐被企业接受和认可。**艾瑞咨询在《2021年中国企业级SaaS行业研究报告》指出，SaaS行业在近几年保持了高速稳定的增长，2020年中国SaaS市场达到538亿人民币，预测2023年达到1304亿人民币，可见在业务的驱动下企业上云已逐渐成趋势。

2016-2023年中国企业级SaaS市场规模及预测



* 图片来自艾瑞咨询

即便如此，依旧有企业倾向于将数据存储在自己的服务器上，对SaaS模式下将数据存储在云上感到不安。根据近期Gartner发布的《中国云安全市场概览》分析，**“国内市场对于数据物理位置的关注超越了安全本身”**，也印证了这一观点。

企业是选择传统软件模式，还是选择SaaS模式，类似“钱放在家里还是放在银行”，需要辩证来看。

传统软件模式**将软件部署至企业本地服务器**，数据无需上传至第三方服务器或云端，对企业来说数据更加私密可控，可以满足特殊行业的合规要求。**但**传统软件模式**同时面临着所有安全责任都需要由企业自行承担所带来的压力。即便企业自行管理数据中心和业务系统，如果没有完善的安全**

防护体系、安全架构、技术防护能力和专业安全人才，依然有可能遭到黑客攻击或内部人员数据泄漏，造成巨大的经济损失。这一点从以往的数据安全事件中就能看出：

·2018年，台积电在台湾的生产基地遭遇勒索软件攻击，随后台积电高层发表声明称病毒入侵为人为疏忽导致的。

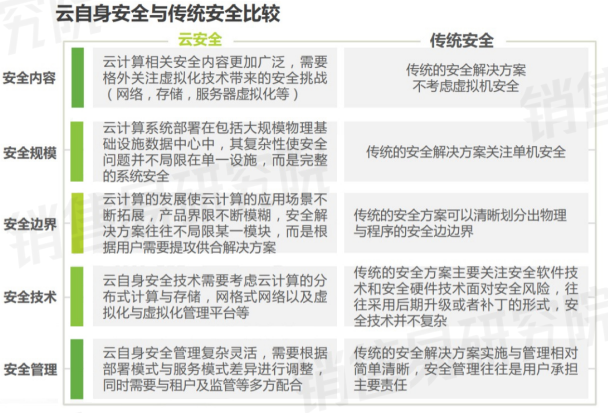
·2020年12月，富士康的墨西哥工厂遭遇软件攻击勒索，攻击者获取了未加密的富士康文件，之后对相关设备进行了加密，向富士康索要价值约2亿元人民币的比特币。

·2021年4月,软件巨头SAP就向客户发出警告，本地部署系统被黑客攻击。而在这种情况下，如果企业不具备漏洞检查修补的安全能力，将遭受到巨大损失。

另外，传统软件模式由于部署在企业内网，为安全起见一般不允许访问外网，或者不允许互联网请求进入。难以适应当前开放、合作的网络环境，既无法实现多种客户端的支持（如手机APP，微信小程序等）也不利于与优秀的第三方互联网应用（如企业微信、钉钉）及企业合作伙伴实现生态集成。

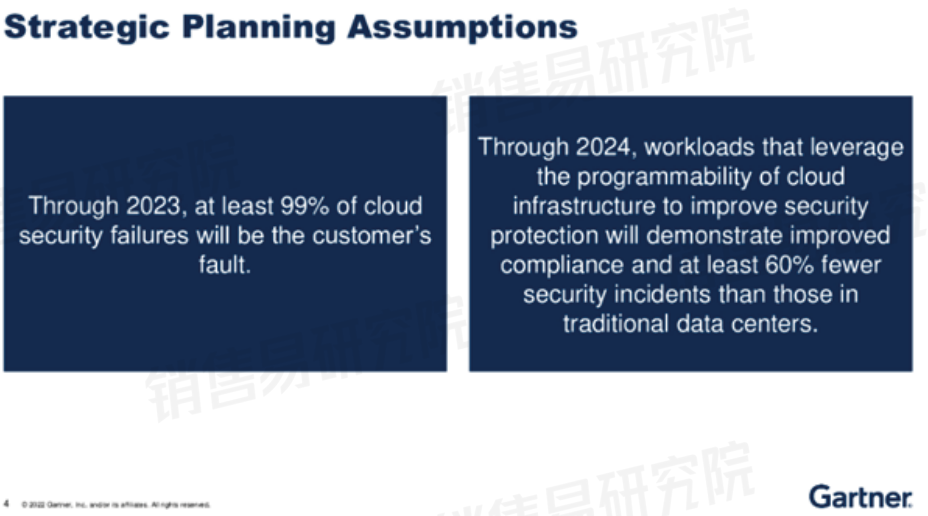
* SAP向客户发出的警告，图片来源于网络

而在SaaS模式下，**SaaS厂商通过云安全责任共担模型，与企业双方共建安全，让企业在人力财力有限的情况下更聚焦于企业需要承担的安全责任上。其次，一般SaaS厂商除了具备完善的安全管理制度外，还非常重视数据安全建设，往往具备全面的安全防护手段、开放且安全的软硬件环境、专业的安全团队、容灾措施等。**



* 图片来自艾瑞咨询《2021年中国云安全行业研究报告》
从五个维度列举了传统安全和云安全的差异

对于“数据存储在云上是否安全”这一问题，Gartner在《中国云安全最佳实践》报告中提到，据Gartner预测，到2023年，主流的云服务提供商出现重大安全事件的概率将非常低，99%以上的安全问题并非由云服务本身引起的。而到2024年，云基础设施将展现出比传统数据中心更好的合规性，并减少至少60%的安全事件。 可见数据存储在云上本身是安全的。



* 图片来自Gartner《中国云安全最佳实践》

总结来说，对于资源能力有限、安全能力不全面或安全投入较少、希望在保证数据安全性的同时平衡业务发展、尽快实现企业数字化转型的企业来说，SaaS模式是更佳选择。

2.2 CRM安全选型清单

“安全”作为一个体系，不只涉及到SaaS服务一个方面，安全管理、产品安全能力、安全制度等也是保障数据安全的重要因素。对于准备使用或已使用SaaS产品的企业来说，如何评估SaaS厂商的安全能力，成为企业需要关注的重点。企业对于“SaaS不安全”的误解，大部分原因是SaaS厂商不具备足够的安全能力而导致的。回到SaaS-CRM的选择上，由于CRM系统涉及到企业业务数据和个人用户数据，企业对CRM厂商的安全性、隐私性、合规性要求更高。在安全能力评估上，企业可以从以下几方面入手综合评估CRM厂商的安全能力。（见下页）

当然，CRM厂商想要具备以上安全能力，仍然需要多年的建设和持续的资金、人力投入。作为国内CRM领导者，销售易经过多年积累已经在安全、隐私、合规三个方面取得成果。

CRM厂商安全选型清单

安全模块		参考权重	指标解析	
硬指标	产品能力	★★★★★	登录安全	全面完善的密码安全策略，包括但不限于：密码有效期、密码长度、密码复杂度、密码历史、修改密码登出、账号锁定等
				安全灵活的登录安全策略，包括但不限于：Web页面空闲时间、移动端免登录时间、Web端互踢及移动端互踢、移动端绑定、双因素或多因素认证、Web页面IP限制、按需授权登录（内部/外部人员）
			权限管控	提供标准的基于组织架构或岗位职能的业务功能权限管理
				提供全面、细粒度化的数据权限管理，包括数据的读取、修改、删除、转移等
				应提供根据业务特性自定义规则的权限管理
				应支持上述权限元数据的导出和安全审计
			数据安全	应提同时支持Web和移动端的页面水印
				应能对自开发代码的出站行为，API接口的入站行为进行管控
				应能对敏感字段进行加密存储，并按需脱敏显示
			安全审计	应具备全面、详细的日志审计功能，包括但不限于：用户登录日志、数据导入导出日志、用户及权限管理日志
	技术安全	★★★★★	物理安全	应部署在业界知名公有云上，所在数据中心具备充分的物理安全防护和监控能力，同时满足业界的建设标准（如T4）
			网络安全	应采用多链路多ISP网络接入，且具备常见的网络防护能力，如DDoS防护、网络隔离
			主机安全	应具备常见的主机安全防护和监控能力，包括资产管理、入侵检测、安全基线等必备要求
			应用安全	应具备Web防护能力能防范常见应用风险如OWASP Top 10
			数据安全	应具备多种安全能力保障线上数据安全，如加密传输、数据加密存储（包括移动端数据库）、访问控制
	安全架构	★★★★☆	多云 多区域 多站点	主要考核CRM厂商服务的可用性和灵活性，对于厂商是否能有效抵御不可抗力的安全威胁（例如战争、地震）具有参考意义
软指标	最佳实践	★★★★☆	服务多行业企业	如金融、电信等行业对数据安全要求更为严格，通过不同行业客户可佐证CRM厂商的安全能力
			服务多类型企业	跨国企业、出海企业等在数据出境、数据合规方面面临更复杂的问题，可侧面印证CRM厂商的安全能力
	安全管理	★★☆☆☆	安全组织保障	应具备健全的组织架构来保障实施安全工作，包括但不限于公司级的信息安全治理组织（如信息安全领导小组）、专门的信息安全团队、独立的审计部门
			安全人员保障	应具备全面的人员保障体系，包括但不限于：覆盖全员的安全意识培训与考核、针对特定人员（如运维人员）的安全培训与考核、覆盖全员的全岗位生命周期（入职\调岗\离职）的账号及权限管理
			安全管理制度	应实施全面的安全管理制度与流程，涵盖办公、开发、运维等业务场景
	资质认证	★★★☆☆	1SO27001	应具备国际认可的信息安全管理体系认证
			ISO20000	应具备国际认可的信息技术服务管体系认证
			ISO27701	应具备国际认可的隐私信息管理体系认证
			等保三级	应通过等保三级的安全测评并具备备案证书
			三方安全渗透测试	应具备独立权威第三方出具的安全渗透测试报告

3 销售易合规性

数据合规是指企业及其员工的数据活动需要符合相关的法律法规。随着数据作为生产要素的经济价值凸显，数据收集和处理被各个国家谨慎对待，在立法层面出台相关法律法规加以规范和保护，对于企业来说符合相关要求成为必修课。其中欧盟率先在2018年颁布GDPR（《通用数据保护条例》），其他国家和地区以此作为参考加快立法步伐。我国也不例外，在2021年出台了《数据安全法》《个人信息保护法》。

销售易积极响应并落实《网络安全法》《数据安全法》《个人信息保护法》的要求，按照国际公认的信息安全和IT管控标准，不断完善信息安全管理体系和技术体系，为客户提供经第三方权威评测及认证机构审核过的SaaS服务。 同时，销售易凭借服务不同行业、不同类型企业积累的宝贵经验，帮助企业实现业务安全与合规。

3.1 销售易合规认证

销售易致力于为客户提供稳定性高、安全性强、合规风险低的产品和服务。目前，销售易已经通过ISO27001信息安全管理体系认证、ISO27701隐私信息管理体系认证、ISO20000信息技术服务管理体系认证、ISO9001质量管理体系认证、信息安全等级保护三级认证，并获得数据中心联盟颁发的移动信息化可信选型认证。

3.11 ISO 27001

ISO 27001是国际上被广泛采用和接受的**信息安全管理体系**认证标准，是全球领先的安全标准之一。基于保密性，完整性和实用性三大原则，涵盖信息安全方针、信息安全组织、人力资源安全、资产管理、访问控制、加密、物理和环境安全、操作安全、通信安全、系统的获取开发维护、供应关系、信息安全事件管理、信息安全方面的业务持续管理、符合性共14个方面。

ISO 27001

3.12 ISO 27701

ISO 27701是业内公认的最具权威性的隐私管理体系建设指导标准。如果说ISO 27001是对企

业信息安全管理的整体要求，那么ISO27701则更侧重企业隐私信息管理，可以看作是ISO 27001在隐私方面的扩展。

ISO 27701

在ISO 27701的附录中直接与GDPR进行了映射，可以理解为通过ISO 27701认证的企业或组织，已经很大程度上覆盖了GDPR的要求，而很多国家的信息保护法都以GDPR为参考，因此通过ISO 27701认证可以帮助企业大大降低合规风险和合规成本。

3.13 ISO 20000

ISO 20000是信息技术服务管理领域的国际标准，为企业提供了一套包含设计、建立、实施、运行、监控、评审、维护和改进服务管理体系的要求，确保企业可以提供有效的IT服务来满足客户和业务的需求。ISO 20000也为IT管理者提供了一套管理IT部门的参考框架。

对于客户数据，除了外部病毒和黑客攻击外，内部运维过程中的操作规范也至关重要，ISO 20000标准定义了一套全面、紧密、安全的服务管理流程。因此，ISO 20000认证可以作为客户选型过程中，判断SaaS厂商的内部安全管理制度和人员控制的参考标准。

ISO 20000

3.14 ISO 9001

ISO 9001是质量管理体系认证的标准，用于证实组织具有提供满足顾客要求和适用法规要求的产品的能力，目的在于增进客户满意度。获得ISO9001认证可证明企业已建立符合国际标准的全面完善的质量管理系统，可以保障其产品服务的可靠性、稳定性等。

对于SaaS厂商来说，获得ISO 9001认证可证明其产品质量已经符合相关法律法规要求。

ISO 9001

3.15 网络安全等级保护三级认证（DJCP）

网络安全等级保护是国内各企业/组织进行网络安全建设的依据，是网络安全工作的基本制度。

分级保护是指对信息系统中使用的安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级进行响应、处置。等级划分从一级到五级，一级为最低（自主保护级），五级为最高（专控保护级），三级属于“监管级别”，是非银行机构的最高标准。除了通过认证外，还需要每年进行一次测评。

DJCP

3.16 移动信息化可信选型认证

移动信息化可信选型认证是数据中心联盟“开放移动互联委员会”根据《移动信息化可信选型认证评估方法》和《移动智能终端应用软件安全技术要求》等标准对移动信息化产品与服务开展的评估认证。

旨在推进移动信息化产品与服务的标准化与规范化，为政企采购部门选购移动信息化产品提供参考和实践案例。进一步推动移动办公应用在政务、金融、医疗、能源、公安、物流等各个领域的信息化引领作用。

3.2 企业合规 应该如何做

3.21 本土企业：承担法律义务 保障数据安全

《数据安全法》第四章第27条明确了企业在数据安全方面需履行的义务：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。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

本土企业应该注意什么

· **从源头关注数据安全：**在信息系统搭建之初就要考虑数据安全问题，并在收集用户信息时，做好数据的安全监控，关注是否有数据过度采集或者来源不明情况；

· 数据主体在新法出台后会更加关注自身数据的安全性，**企业需要随时准备回应数据主体的质疑，配合数据主体行使相关权利；**

· 企业需要在组织建设层面设立数据安全部门，引进或培养数据安全人才，并在内部定期开展安全培训；

· 《数据安全法》和《个人信息保护法》的出台是为了更好地规范数据的使用，让数据创造更多价值，因此**企业应该正确理解法律法规，让数据在法律框架内为企业所用，平衡数据安全和业务发展，**在合法前提下使用数据，让数据效益最大化；

· **参考已有标准，建立及评估数据分类分级标准。**比如金融、电信行业已形成了分类分级标准，可以参考这些标准对企业内部的分类分级标准进行评估，同时关注主管部门发布的标准规范，对企业的分类分级标准进行调整；

本土企业合规 销售易可以做什么

销售易将数据安全融入产品能力，采取相应的技术措施和其他必要措施，保障数据安全，帮助企业更好地履行数据安全、隐私保护义务。企业可以使用销售易产品中“数据加密存储”“数据脱敏”“数据访问日志”“数字水印”“密码设置”等功能，帮助企业实现安全、合规的目的。

3.22 跨国企业的国内分支机构：关注国内合规

以往，跨国企业为实现统一管理，通常要求国内分支机构将产生业务数据跨境传输到总部。但在新法出台后，由于数据本地化要求，跨国企业在数据的跨境传输上面临挑战。

《网络安全法》第37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个人信息和重要数据应当在境内存储”。

《个人信息保护法》第四十条规定：“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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。

跨国企业应该注意什么

· 两部法规对数据本地化都做出明确规定，**数据收集和存储应遵循 “境内存储” 原则。对于在中国境内运营的跨国企业来说，应优先考虑在中国境内设立数据中心，以符合本国的合规要求；**

早在2017年，苹果公司就与云上贵州合作，将大陆地区用户的icloud服务交给后者运营，以保障数据不出境。特斯拉也在2021年5月宣布在国内设立数据中心，实现数据本地化储存。

·跨国企业的国内分支机构，如涉及数据跨境传输，**在满足国内合规要求前提下，也需要满足接收方所在地的相关要求，而不同国家或地区的法规不尽相同。当这种情况出现时，企业需要关注两个国家或地区的立法差异，同时满足双方合规性；**

·**《数据安全法》《个人信息保护法》出台后，企业需要紧密关注陆续出台的相关细则和法规的落地，帮助企业明确合规工作方向。**

7月7日，《数据出境安全评估办法》正式出台，明确了数据出境的情形、评估流程、评估范围以及评估时间。为企业管理数据跨境活动提供法律依据和指导。

跨国企业的困境

跨国企业由于对国内市场环境不了解（比如对国内安全技术和安全工具的应用不熟悉）、对立法背景不熟悉会增加合规风险和合规成本。

目前《数据安全法》《个人信息保护法》作为纲领性法规，对于企业该“如何具体落地”法律要求尚未给出全面的指示。例如个保法中提到的数据分类分级制度，除少数行业给出标准外，大多数行业没有形成明确规范。

跨国企业合规 销售易可以做什么

销售易在北京，广州设立数据中心，可以满足跨国企业“境内存储”原则，帮助跨国企业规避因跨境传输带来的合规风险，更好地满足国内的合规要求。此外，相比Salesforce、微软等国际品牌，销售易也更加了解国内的立法环境和监管要求，可以为跨国企业提供建议。

3.23 中国企业出海：关注潜在合规风险

中国企业在出海的过程中，在数据安全和隐私安全方面面临来自海外的合规难题。根据亚马逊云科技的调查显示，**近60%的受访企业认为出海服务，安全合规最重要。**

出海企业应注意什么

根据联合国贸易发展组织统计，截止到目前，全球约80%的国家已经完成数据安全和隐私保护立法，或已推出相关草案。在复杂的立法背景下，除了关注法律法规本身外，还要关注潜在的合规风险。

·对于业务覆盖范围广的出海企业，每个国家和地区新增或修改法律条规，都可能影响企业业务发展。此外，不同国家在立法上可能存在偏差，也需要企业关注：比如**对于“敏感信息”的定义，《个保法》将不满14周岁的未成年人个人信息列为敏感信息，而印度的PDPB则在法案中将儿童定义为未满18周岁的人，将儿童数据划分为敏感数据；**

·不同国家因其文化、宗教等原因，在监管执行上可能存在 “本土特色”，如果企业对这些特色不了解，也会面临合规风险：比如**西方国家更关注个人隐私，监管机构对于隐私泄露事件的容忍度更低，在判罚上会表现得更严厉；**

·地区性保护法规，比如GDPR，也会存在不同国家执法力度不同的问题：比如GDPR下的每个国家的DPA（Data Protection Act 数据保护部门）执法力度差距较大，从判罚案例上看，匈牙利、捷克、德国等执法力度更强，而意大利、荷兰、瑞典等执法力度偏弱；

·企业可以通过研究各国数据保护法下的执法案例，理解所在国执法和监管的态势，比如在GDPR实施后，对于违反数据保密性和完整性原则而产生的执法案例明显较多；

中国出海企业合规 销售易可以做什么

出海企业在应对合规难题时，除了**“观察外部”“审视自己”“找差距”“做决定”“实施落地”**五步走，还可以通过与销售易这样具备国际化能力的CRM厂商合作，分担企业的合规压力。销售易目前已取得ISO27701认证，有能力帮助出海欧盟的中国企业实现GDPR合规。除此外，销售易还在新加披等地建立数据中心，满足大部分出海东南亚企业的合规需求。销售易目前已经服务诸如海康威视、固德威等多家出海企业，积累了成熟经验。

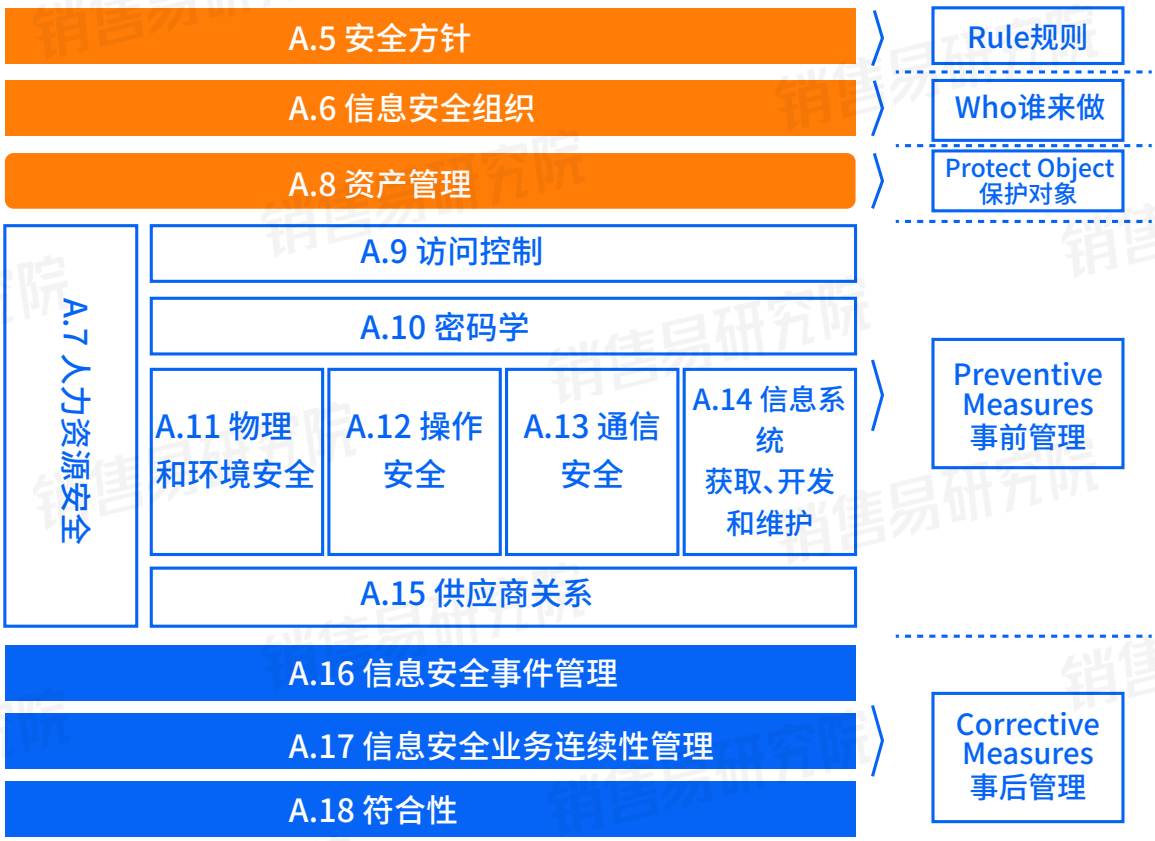
4 销售易的数据安全管理体系

数据安全管理建设，是全方位多角度的安全体系建设，不仅包含基础设施和硬件，更涉及到人员组织管理，制度建设等方面。

4.1 销售易的信息安全建设框架

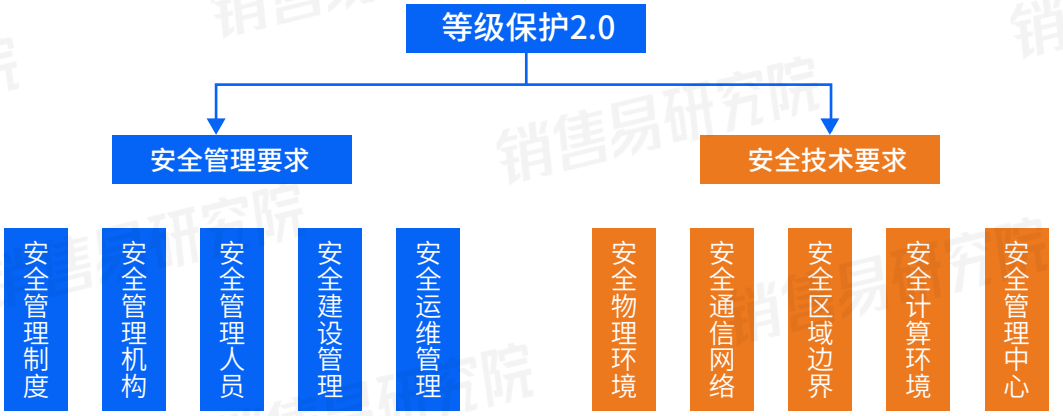
销售易的信息安全体系在设计之初就充分调研了国内外的安全标准及业界最佳实践，参考了ISMS标准规范，和国内最新等级保护2.0标准，并结合销售易自身的业务特点、组织架构、技术现状和企业文化等因素来因地制宜地开展体系化的信息安全建设。

销售易在设计和建设安全管理体系过程中，主要参考了国际信息安全管理体系ISMS（Information Security Management System）。它是从英国BS7799发展起来的信息安全领域中的一个最佳实践模型，是管理体系（Management System，MS）思想和方法在信息安全领域的应用。近年来，伴随着ISMS国际标准的发展，ISMS迅速被全球接受和认可，成为世界各国、各规模组织解决信息安全问题的主流方法。



* 信息安全管理体系控制域分布

除参考国际通用安全管理体系外，销售易还主要参考目前国内最新的等级保护2.0标准的三级要求，从安全管理、安全技术两大维度综合考虑，涵盖安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理、安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心十个子类。



* 等级安全保护2.0通用安全体系

销售易信息安全保障体系的建设，以自身信息系统的实际情况和现实问题为基础，参照ISMS标准及国家信息安全等级保护的要求，充分借鉴成熟的信息安全理论成果，设计出兼顾整体性、可操作性，并且融合策略与组织、安全防护、安全监控、安全运行、应急恢复等为一体的信息安全保障体系，保障销售易信息系统的安全运行。

* 销售易信息安全保障体系框架

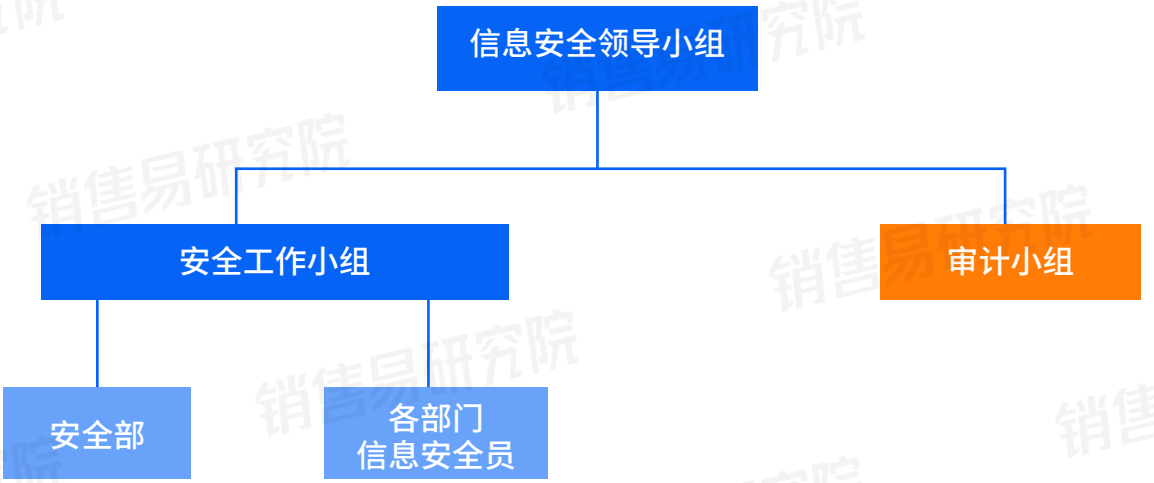
售易依据ISO27001安全体系框架、等级保护要求并结合企业自身现状形成了当前的安全建设体系，具体全景图如上

4.2 组织与文化保障

信息安全体系的建设和落地都离不开“人”这个最核心的要素。在ISMS和等级安全保护2.0通用安全体系中，都对“人员安全”做出了相应规范。销售易一直将人员安全作为信息安全的重要一环，从组织架构、制度与流程、安全团队建设和人员安全管理等多个方面来进行组织和人员保障，确保信息安全体系能够正常运转并持续优化。

4.21 安全组织架构

为使信息安全工作在公司全面推行及落地，销售易成立内部信息安全组织机构，包括信息安全领导小组、下设信息安全工作小组和审计小组。领导小组领导公司信息安全工作，负责信息安全策略和目标制定，安全工作小组主要负责信息安全的规划设计和落地，审计小组主要负责安全工作的监督与追踪。



4.22 制度与流程

根据ISMS和ISO 20000的要求，销售易制定了一套完善的IT服务和安全管理体系规范，包括ISMS的14个领域（安全策略、安全组织、人员安全、资产安全、物理和环境安全、访问控制、密码管理、信息系统开发和获取、供应商管理、安全事件管理、业务连续性管理、符合性管理），同时涵盖了ISO 20000体系的管理要求。（包括服务级别管理、服务连续性和可用性管理、供应商管理、事件和服务请求管理、问题管理、配置管理、变更管理和发布管理）。

4.23 信息安全团队建设

根据公司安全战略目标，销售易组建了一支专业的信息安全团队，包含安全架构师，渗透测试工程师，安全运维工程师和安全合规工程师等岗位，具备了安全风险管理、防范、发现、处置与应急响应的能力。团队成员来自包括安全厂商、互联网公司、安全测评机构等不同背景的企事业单位，在甲方安全建设方面具备丰富的经验和能力，能够将信息安全保障体系在企业内部成功“落地”并有效运转。

4.24 人员安全管理

根据ISMS要求，销售易建立了完善的人员安全管理体系，贯穿入职前、任用中、调岗和离职管理。

入职前

员工在入职之前，销售易在法律范围内通过背景调查确保入职员工符合公司的行为准则、保密规定、商业道德和信息安全政策。背景调查涉及刑事、职业履历和信息安全等方面。

任职中

员工在入职后，所有的员工必须签署保密协议，确认收到并遵守销售易的安全政策和保密要求，所有新入职员工都必须参加并通过信息安全意识培训和考核。关于客户信息和数据的机密性要求也在入职培训中被重点强调。除此外，销售易的信息安全部门还将定期开展数据安全讲座或集中开展数据安全活动来持续加强和提升全员信息安全风险意识。销售易还依据员工的工作角色进行额外信息安全培训，确保员工管理的用户数据必须按照安全策略执行。

离职和调岗

员工离职需通过流程审批。信息安全管控环节包括工作文档交接，应用系统及邮箱帐号权限回收，VPN及网络访问帐号回收，公司电脑回收及门禁卡收回等，账号和权限将在员工离职的第一时间被接管。员工如果涉及调岗，则其原有业务系统的权限会被回收，如新岗位需要，则根据当前岗位需求进行重新申请。

4.3 安全技术保障体系

安全防护	安全监控	安全运行

依据业界最佳实践与当前的技术现状，销售易搭建起以安全防护、安全监控、安全运行为一体的，覆盖业务系统全生命周期的安全技术保障体系，具体如下：

4.31 安全防护

物理安全

销售易系统均部署在如腾讯云、AWS（中国区）等业界知名公有云上，所在数据中心都有充

分的物理安全监控和管控措施。相比自建机房的厂商，在安全能力积淀、安全组织、标准规范、持续运营方面更加领先。并且自建机房的厂商需要单独投入运维人力，安全团队的时间精力被分散，难以专注且持续地打造和提升SaaS的产品安全能力。

网络安全

销售易使用多链路、多ISP网络供应商接入服务，保障网络链路的高可用性。并采用云端的ELB机制（Elastic Load Balance-弹性负载均衡）可以有效防御常见类型的DDoS攻击。生产系统通过VPC（虚拟私有网络）与外界网络隔离，并在VPC中划分不同的子网，不同的子网有不同的安全访问策略与限制。公网只开放服务端口，禁止互联网开放高危端口和服务，内部后台应用仅对办公网络开放。

主机安全

线上服务均使用内部管理的可信操作系统镜像，安装软件必须由运维人员从公司系统团队维护的可信安装源下载和安装。对通用的系统软件均制定了对应的安全配置规范。对于生产服务器，运维人员需要先登录堡垒机之后，才能登录其他生产服务器。堡垒机只对特定的办公网段开放，并长期存储运维人员的操作记录，便于责任管理。

运维人员登录服务器前，需要先提交权限申请，且访问权限有时间控制。在通过审批后，才能获得对应服务器的登录权限。运维人员离职、岗位发生变动、申请的权限到期时，都会在对应的服务器上删除对应的帐号。

应用安全

销售易通过IAM机制（身份和访问管理）、访问控制（ACL）设置等给客户提供细粒度的权限管控能力，可以满足客户各种安全需求，降低客户的数据安全风险。通过提供个人用户账号安全、密码安全设置等功能，以及后端风控体系来实时监测账号破解、撞库与刷库等攻击行为，并将发现存在风险的账号及时告知客户以便进行账号密码的修改。销售易还提供客户详细全面的日志审计功能，可以覆盖管理员和普通用户的所有操作，并且操作记录长期保存以便客户事后查询和取证分析。

此外，销售易使用WAF（Web Application Firewall，网站应用级入侵防御系统。）对DDoS攻击，以及SQL注入、XSS、命令注入等OWASP TOP10的常见攻击手段进行严格地检查和过滤。

数据安全

销售易从数据传输、存储、访问至销毁的数据安全生命周期，使用了数据分级、数据加密等措施，保障了数据的保密性、完整性、可用性、真实性、授权、认证和不可抵赖性。

所有数据在公网传输时均使用SSL/TLS安全协议加密传输。同时销售易为个人和企业数据提供访问控制保障。通过访问IP限制、细粒度的权限管控、数字水印、数据导入导出日志为企业人员的数据访问安全提供全面的防护和保障。同时销售易对app客户端的数据库进行整库加密存储，保护用户在客户端存储的敏感信息不会被攻击者非法获取。

销售易使用云服务商中对象存储和云数据库两种数据存储服务，均承诺可保障数据99.99% 的可用性和 99.999999999% 的持久性。同时销售易通过多数据中心的主从实时同步、额外的数据备份方案，来保证数据的完整性和可用性。

* 销售易CRM水印功能效果

* 销售易CRM日志导出功能效果

4.32 安全监控

应用监控	网络监控	主机监控	数据监控

应用监控

销售易使用Web应用防火墙来实时对应用系统入侵、SQL注入攻击、XSS攻击、命令注入攻击等行为进行监控和拦截。同时对公司网站进行实时监控，一旦发现网站安全漏洞或风险可以实时报警并处理。

网络监控

销售易同时使用内部监控系统与第三方服务监控外网访问性能与连接状态，可以实时监测和发现异常网络情况并及时采取应对措施。

主机监控

销售易的业务系统均部署功能全面的主机安全监控产品，可以对云主机上的安全状况进行监控，对于暴力破解、异常登录、反弹shell、本地提权、Web后门等主机入侵行为均具备安全检测

和处理能力。

数据监控

云端的安全审计覆盖租户下所有用户数据活动的详细跟踪记录，生成审计人员所需要的信息。生成的操作记录详细全面，如数据下载、数据上传等，做到所有用户操作有踪可寻。

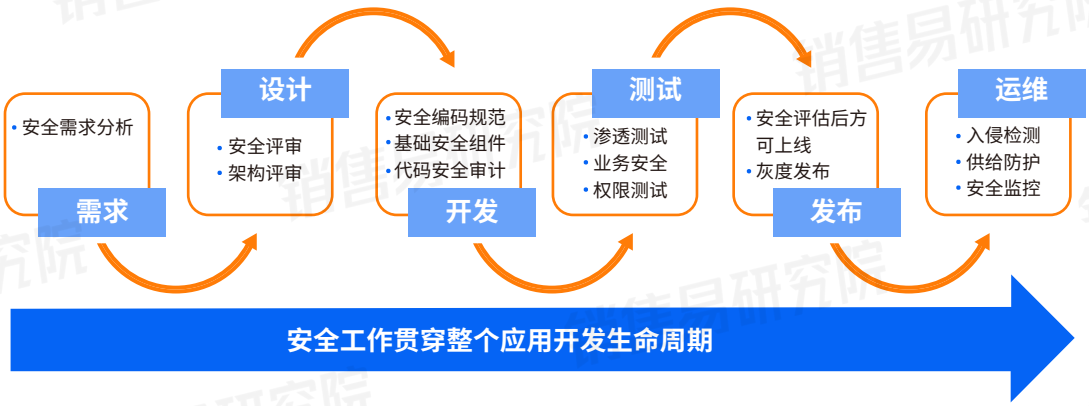
4.33 安全运行

安全开发	安全运维

安全开发

销售易产品在项目开发流程中引入了SDL(Security Development Lifecycle软件安全开发周期)，借鉴了微软推广SDL的经验，并结合企业级安全需求以及销售易自身的项目开发流程，控制项目整体的安全风险。

销售易每年聘请外部专业安全公司，组织针对应用系统的渗透测试，及时发现并修复应用层面的安全漏洞。同时销售易使用基于业界知名开源软件搭建SCA（软件组成分析）平台，并定期对应用系统使用的第三方组件进行全面细致地分析，从而发现存在高危风险的第三方组件并推动修复。

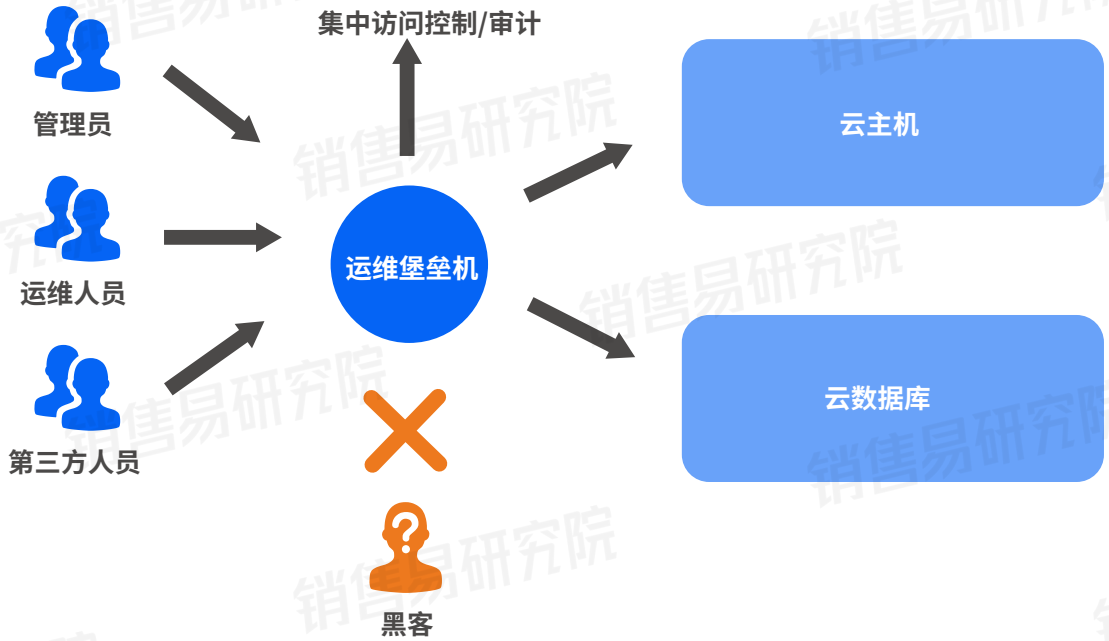


* 应用安全——安全开发周期SDL

安全运维

销售易根据ISO20000服务体系，**建立了一套完善的运维服务流程，包括事件管理流程、服务请求管理、问题管理、变更管理流程、配置管理、发布管理等。**

所有的运维操作必须通过运维堡垒主机认证、授权以及审计，所有操作都可审计查询。同时通过ACL（Access Control Lists，访问控制列表）来限制可以访问生产系统的运维IP地址范围。



* 可审计的安全运维

4.4 安全运营保障体系

安全事件管理	应急处理机制	业务连续性管理

除上述的组织保障、文化与制度建设、安全防护技术外，销售易通过安全事件管理、建立应急处理机制、业务连续性管理等来支持和实现“可持续地”安全运营，最终保障线上业务系统的安全、稳定运行，具体如下：

4.41 安全事件管理

销售易制定了完善的信息安全事件管理规范和处理办法，对信息安全事件分类、信息安全事件分级、信息安全事件报告及处理、信息安全事件的处理和解决、信息安全事件的反馈和关闭、信息安全事件的通报、信息安全事件回顾和分析做出了明确定义。

4.42 应急处理机制

销售易制定了一套完善且适用于自身业务的通用应急预案及专项应急预案，成立专门的应急响应团队（由公司高管、运维部、安全部组成），建立规范的应急处理流程，并且每年启动一次应急预案的演练。

4.43 业务连续性管理

销售易能够应对线上各类风险，具有自动调整和快速反应的能力，保障销售易业务连续运转。销售易通过了ISO20000认证，以国际安全认证标准保障服务的连续性，服务可用性可达99.9%。

保持业务连续性，可以将企业因数据丢失、数据加密勒索、DDoS攻击等导致的损失降至最低。国内某电商服务企业曾曝出删库事件，其生产环境遭到恶意破坏，入驻的线上商家业务被迫中断。并且从删库事件发生到数据恢复时隔数天，企业和入驻商家都遭到了巨大损失。由此可见保持业务连续性的重要程度。

销售易的灾难恢复机制，建立在公有云提供的服务基础上，主要通过以下方面来保障：

- 系统环境：通过快照的方式保存在对象存储上，供快速扩展和环境恢复。
- 数据信息：一方面定时快照到对象存储上，另一方面利用云数据库的跨AZ（多个数据中心）同步机制，共同保障数据的安全和完整。若需要恢复或调整，则使另一数据中心的副本自动升级为主实例即可，并且可以保证数据完全一致。如果实时切换失效，还可以根据对象存储上的每日定时快照，恢复数据到前一天。
- 系统代码：采取本地备份和云端对象存储双备份机制。

5 销售易隐私体系建设

销售易作为企业数字化转型的赋能者，除提供专业领先的产品、方案及服务，还力求在个人隐私数据保护上与客户同发展、共进步，时刻关注国内外信息安全和隐私保护相关规定，持续对个人隐私数据保护进行完善和提升，从企业自身安全建设到产品安全能力设计不断优化更新，将保障企业客户数据安全以及个人隐私安全作为服务的重中之重。

5.1 销售易与企业责任共担

5.1.1 安全责任共担模型

安全不仅仅是SaaS厂商或客户某一方的单方面责任，需要双方共同关注。每一方在数据处理中的角色不同，所承担的责任也各不相同。在安全责任的划分上，云计算领域的最佳实践 “安全责任共担”模型已经被普遍使用，作为划分客户和厂商安全责任的依据。销售易也采用了安全责任共担机制，与企业客户共同保障云上数据的安全。

在通用的安全责任共担模型中，客户和云服务提供商所承担的不同责任如下图所示。

* 安全责任共担模型中，客户和云服务提供商所承担的不同责任

5.1.2 销售易的责任

· 物理安全：负责通过严格筛选和评估云服务商来保障业务系统所在数据中心的物理安全。
· 基础设施安全：负责通过实施安全防护和监控措施（如HIDS）来保障承载业务系统的云主机、数据库等基础设施的安全。
· 网络安全：负责通过实施网络划分与隔离（如VPC）、网络访问控制（如安全组）等安全防护措施保障业务系统的网络安全。
· 应用安全：负责通过使用应用安全防护（如WAF）、修复业务应用漏洞及组件漏洞等安全措施保障业务系统的应用安全。
· 租户安全：负责通过合理的设计与实施保障租户之间的隔离与安全，并提供对应的产品安全能力可让租户安全地使用服务。

5.1.3 企业或组织的责任

· 账号安全：负责通过密码策略、双因素认证、移动设备绑定、IP限制等措施来保障自身的账号安全。
· 数据安全：负责通过权限控制、API限制、数据加密、启用水印等多种措施来保障自身的数据安全。
· 终端安全：负责通过系统补丁安装、病毒查杀、终端管理等多种措施来保障自身的终端安全。
· 内容安全：负责使用销售易产品服务过程中存储或处理内容（包括但不限于数据、文件、软件、图像、音频、视频等类型）的安全，确保不涉及黄、赌、毒等违规内容。

同时，销售易提供了多种安全和隐私保护服务能力，帮助企业或组织实现全面的隐私保护合规。

安全功能	详细介绍	实现价值
数据加密存储	1）线上数据库使用高强度的整库加密进行存储 2）APP移动端的数据库也使用整库加密存储（加密密钥保证每个客户端唯一） 3）提供字段级数据加密，可以根据需要对敏感字段开启加密存储	数据加密可降低数据泄露的风险，也可以防止数据被篡改，提升数据安全性
数据脱敏显示	对于个人用户的敏感信息提供脱敏显示能力，管理员可在后台进行配置脱敏规则来保护个人用户敏感信息	防止客户真实信息泄露及企业个别内部员工滥用个人用户信息的行为发生
数字水印	管理员可以根据自身需要启用web端、app端的数据水印功能，可以有效威慑内部人员数据泄露行为以及事后追溯	可以有效威慑内部人员数据泄露行为，便于事后追责
数据访问日志	为客户提供详细的数据访问日志功能，全面记录企业客户内部人员的各种数据敏感行为，包括数据上传及下载、数据导出等	记录和监测企业内部人员的各种数据敏感行为
数据交换安全	客户需要通过API接口与外部第三方进行数据交换时，提供网络层面限制的能力。客户可以自行设置API调用的IP白名单，只有授权范围内的IP地址才可以调用客户的API接口	保护只有客户授权的第三方可以通过API方式访问数据，避免数据泄露

* 销售易部分产品数据安全功能

5.2 隐私保护体系建设

销售易隐私保护体系秉承七大原则，通过组织建设与人员管理、流程管理、技术控制三个维度对客户的隐私数据进行全方位的安全保护。

5.2.1 销售易隐私保护7大原则

合法公平透明

销售易对个人用户数据的处理，无论是收集、传输还是使用，均符合法律规定，且符合透明化的要求。此外，无论是企业客户还是个人用户（游客身份），销售易都保证以最高规格保护客户数据，承诺最大限度保护数据安全；

目的限制

销售易在个人用户数据的处理上满足正当要求，其后续的数据处理也不会违反初始目的；

数据最小化

销售易按照业务需要的最小范围划分个人用户数据的处理量，即仅收集实现产品或服务业务功能所必需的个人用户数据，不收集任何非必要的个人用户数据；

准确性

销售易确保个人用户数据的使用真实准确，在个人用户数据更新时，销售易将会对个人用户数据及时同步；

储存限额

销售易只收集业务必须的个人用户数据，且只在必须时间内储存，并对敏感数据的储存进行加密，数据处理目的完成后，销售易将按照当地法律对用户数据进行删除或匿名化处理；

完整性和机密性

销售易在个人用户数据处理过程中，数据获取者会经过严格的授权，避免数据被非法处理和泄露。**销售易将个人用户数据作为公司的最高机密之一，**对个人用户数据保护设有完善的内部流程，任何操作信息都将记录在日志中；

责任原则

销售易致力于长期保护客户的个人数据隐私安全，为客户提供安全、合规的数据环境。

5.2.2 内部管控措施

数据保护影响评估

销售易将定期对销售云、伙伴云、营销云、服务云、智能分析云、电商云、SCRM产品进行数据保护影响评估，在涉及处理个人用户数据的产品开发或需求变更的情况下，会由个人用户数据保护小组参与需求评审，对高风险处理活动（例如在采用新的数据分析技术、处理大量敏感个人用户信息等场景）的合理性，执行数据保护影响评估。

销售易安全开发生命周期（Security Development Lifecycle）

销售易产品在项目开发流程中引入了SDL(Security Development Lifecycle)，并结合企业级安全需求以及销售易自身的项目开发流程，控制项目整体的安全风险。

隐私设计理念（Privacy by Design）

销售易将隐私设计理念融入现有安全开发周期SDL中，对所有涉及个人用户数据功能及服务的系统开发和产品设计均执行隐私设计安全开发流程。

· 在需求设计阶段，充分考虑所涉及隐私安全的需求，根据业务内容、业务流程、隐私框架与安全团队进行沟通，确保隐私安全保护要求的落地实行；

· 在系统开发阶段，充分考虑开发环境、测试环境、源代码及应用本身的安全性，进行个人用户数据保护能力测试；

· 在应用系统上线阶段，确保严格遵循信息系统的安全基线要求；

安全需求评估

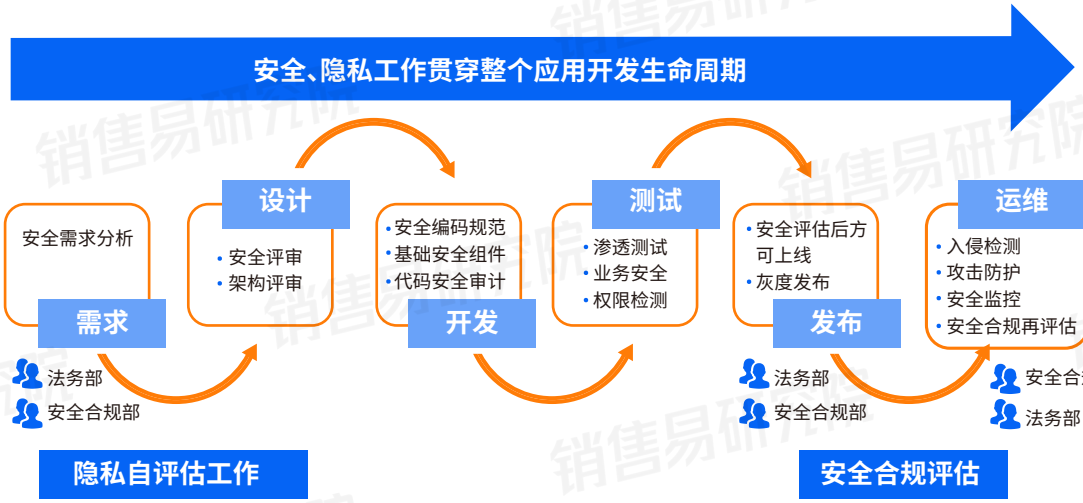
产品技术人员在需求评审后增加**隐私自评估（同时维护数据清册）**环节，之后由安全合规和法务人员判断需求是否进行**安全合规评估**。评估包括**埋点设计评估；权限范围评估**等；最后推动数据清册的更新以及隐私合规评估意见。

上线安全评审

在产品验收之前增加**强制性**的上线安全评审卡点，由安全技术人员、安全合规人员和法务人员通过监测工具查看产品/服务**收集的权限与隐私说明的差距；跨境流量，数据收集范围，埋点数据范围，人员权限范围，并针对有问题的部分给出安全、法务评审意见。**

安全合规再评估

在发版后，安全合规人员和法务人员需要**紧跟相关政策和法规的动态**，持续关注上线产品或服务并给出合规再评估意见。



* 销售易隐私设计理念

事件应急响应

销售易设有专门的安全和运维团队，负责个人用户数据和隐私保护相关的请求处理。当接收到外部通报或监测到数据泄露时，安全运维团队将于72小时内通知客户数据泄露情况，并上报相关监管机构；同时执行应急预案，追溯数据泄露源头、恢复线上数据，以降低对客户的影响。

销售易对于安全事件的管理建立了成熟的机制流程，在捕捉到安全事件后，将第一时间进行追踪以及修复，若安全事件涉及客户的数据安全，安全团队会及时响应，并采取措施以防止此类安全事件再次发生。

5.2.3 技术保护措施

传输加密

销售易全站已经启用基于HTTPS/TLS技术的数据加密传输，有效防止网络中嗅探、中间人劫持等攻击行为。

数据加密

销售易对数据库、对象存储服务采用了云端加密手段，防止有权限的运维人员直接查看数据。同时，系统提供了对业务对象中手机号码、邮箱及其他文本类型字段进行加密存储的能力，管理员通过简单的配置即可轻松完成数据加密操作。

租户隔离

销售易将以租户为维度对存储在销售易上的数据进行隔离，未经租户同意，任何用户无法随意访问。

日志监控

为了保障客户账号安全，降低被破解的风险，销售易安全团队对外部威胁进行监控，可迅速做出响应，将威胁扼杀在早期，保护客户的数据安全。为确保内部操作的安全性，所有对IDC(数据中心)的访问记录均需通过堡垒机进行双因素认证和审计。销售易规定，各子系统保存操作日志不少于六个月，以满足审计需求。

身份识别与访问管理（IAM）

在销售易系统中，客户必须先建立一个账户并授权该账户，然后才能进行资源配置。典型的配置方案包括权限映射和授权、机密材料管理、实施职责分离和最小权限访问、即时权限的管理。

抗攻击防护

销售易公有云系统基于业内云安全最佳实践，部署了抗DDoS攻击、Web应用防火墙、主机安全防护等产品，有效检测及拦截攻击行为。

销售易系统接口具有重放攻击防护，证书白名单策略有效检测异常数据流量屏蔽白名单以外的来源。同时通过登录失败锁定、密码周期更换、密码复杂度设置、IP白名单及双因素登录等功能，有效保证登录账号的安全性，并符合企业客户安全策略要求。

5.3 个人用户数据生命周期管理

销售易作为数据控制者，为确保个人用户数据安全性，并更好地保障个人用户数据权利，销售易将个人用户数据保护划分为六个阶段实施全生命周期管理和技术安全管控。

个人用户数据收集

销售易在收集提供服务所必需的个人用户数据前，将向用户展示《隐私声明》，并说明所收集的个人用户数据类型、目的、处理方式、同意及撤回同意机制等内容。在获得用户同意后，开始收集用户个人数据。

个人用户数据存储

销售易采取严格的管控措施保护客户个人用户数据，对数据的接入、认证、授权、存储等进行统一管理。个人用户数据是销售易保密等级最高的数据，销售易采取严格的数据加密机制和访问控制措施，销售易员工仅在必要情况下，通过完整的授权流程，才可以访问个人用户数据。作为数据控制者，企业可以定义个人用户数据保存期限，对超出保存期限的个人用户数据定期进行删除或匿名化处理（已成为不活跃用户的前提下）。

个人用户数据处理

销售易会按照事先声明的用途对个人用户数据进行处理，在数据使用过程中，将对数据进行严格保护，进行传输和存储加密以及日志记录和审计。同时进行日志回溯审计，定期审查人员的操作行为，进行严格的权限访问管控。

个人用户数据销毁

在数据使用过程中，除法律法规规定的特殊情况外，个人用户可通过电话或邮箱进行账号注销，或依照法律规定要求官方删除个人用户数据信息。（如需获知请求的受理情境、受理流程、例外情况等，请参照销售易官网《隐私声明》）。

销售易会依照法律法规要求和业务需求保存个人用户数据，当超过法律限制保存时间，且不再是业务必需保存的情况时，销售易会及时删除或匿名化处理。

向第三方披露

销售易内部有严格的数据披露和对外分享的管控流程，除法律法规、监管机构要求的特殊情况外，在数据被披露前，会事先获得个人用户授权同意，并对其进行脱敏处理。

销售易对个人用户数据相关的供应商执行调研和审查流程，确保其个人用户数据保护能力符合要求。销售易会与供应商签订数据处理协议，规定其作为数据处理者须承担的个人用户数据保护义务。

数据跨境传输

销售易在多个国家建立数据中心，以更好地符合有数据本地化要求的国家及地区的数据安全法规。如涉及到数据跨境传输，销售易遵循国内和当地法律法规的要求，进行严格的内部评审，确保个人数据的传输过程经过评估，数据跨境传输风险可控、正当合法。

5.4 个人隐私权利保障

用户知情权

销售易会提醒个人用户使用销售易所提供的各项服务前，仔细阅读《隐私声明》，在确定充分理解并同意后，方可使用销售易的服务和产品。

《隐私声明》采用标准化图标，以简洁明了、清晰可视、晓畅易读的方式向数据主体提供信息，阐明了数据处理的目的、来源、处理过程及个人用户可享有的基本权利。

用户访问权及更正权

销售易的个人用户可通过销售易网页版或手机客户端，随时访问、更正或补充企业信息或个人信息。

个人用户还可通过联系销售易在线客服、拨打销售易客服热线（4000-122-980）或发邮件至隐私保护邮箱（privacyofficer@neocrm.com）寻求帮助，来协助进行查询、更正或补充信息。

用户删除权

销售易的用户可通过销售易网页版或手机客户端，随时删除部分个人用户信息。同时可通过APP联系在线客服、拨打客服热线（4000-122-980）或发邮件至隐私保护邮箱（privacyofficer@-neocrm.com）提出删除个人用户信息的请求，但需要满足相关的前提条件（如不再使用销售易的产品或服务，可主动注销账号）。

用户撤销权

除为了满足平台正常运营所必需提供的信息外，个人用户可以自行操作改变授权同意范围。用户可以通过邮件退订、修改移动设备设置、关闭应用内功能开关等方式来取消之前的授权。

当用户撤销授权后，销售易将不再处理相应的个人信息（撤销授权前所进行的个人信息处理，将不受影响）。

用户拒绝营销权

销售易会在法律允许的前提下，经用户的同意后，向其推广介绍销售易的产品。如果个人用户不希望将联系方式继续用于营销目的，可与客服人员联系（客服电话4000-122-980），也可通过邮件取消订阅功能拒绝接收营销邮件。

用户注销账号权

当个人用户所在企业或组织注销销售易企业账户时，销售易将一并注销个人账户，并将根据适用法律要求删除个人用户信息或做匿名化处理。

个人用户可向所在企业组织管理员申请注销个人账户，也可拨打客服热线（4000-122-980）或发邮件至隐私保护邮箱（privacyofficer@neocrm.com）主动申请账户注销，销售易将协助用户完成注销账户。

6 最佳实践

6.1 国内出海企业-固德威

固德威长期专注于太阳能、储能等新能源电力电源设备的研发、生产和销售，并致力于为家庭、工商业客户及地面电站提供智慧能源管理等整体解决方案，目前已登陆科创板。固德威也是国内高新技术企业的出海代表，其光伏逆变器大规模销往全球100多个国家和地区，户用储能逆变器市占率全球第一。

企业安全隐私合规挑战

固德威的海外业务涉及欧盟国家，因此所选择的CRM厂商，不但要满足国内《数据安全法》《个人信息保护法》的相关要求，更需要满足欧盟GDPR（即《通用数据保护条例》）的相关规定，而GDPR被誉为“史上最严”数据保护法，在对数据安全、隐私安全方面进行了严格的规范。

销售易在与固德威合作之前，服务过众多世界五百强企业，并帮助多家企业完成由国际CRM到国产CRM的替代，安全实力已经得到验证。

销售易如何满足固德威安全隐私合规需求

1/**首先，固德威对销售易进行了隐私安全合规性评估，**评估涉及企业治理及管理、数据处理、数据传输、数据存储安全、数据收集、隐私权利响应6个方面，并要求销售易对现状及差距进行分析，并给出对应改进建议，跟进整改进程；

2/**其次，固德威还对销售易产品下不同的个人用户数据类型的传输路径、传输方式、存储位置、跨境情况、存储期限及是否传输第三方等进行深入了解；**

3/再次，**固德威还聘请了荷兰律师事务所，按照GDPR要求对销售易进行评估，以确保销售易作为“数据处理者”身份满足合规性，**最终销售易通过了评估，安全能力得到了固德威的认可；

6.2 世界五百强电气企业-国内分支机构

选择销售易的这家世界500强电气巨头，总部位于欧洲，为100多个国家的能源及基础设施、工业、数据中心及网络、楼宇和住宅 市场提供整体的解决方案。 已经扎根中国市场30余年，在国内设立了几十家工厂和办事处，并建立覆盖全国的销售网络。

企业安全隐私合规挑战

该企业与销售易合作始于 2021年6月。此时全球范围内对于数据安全、隐私保护的立法步伐加快，欧盟、美国、日本、新加坡等通过了一系列法案，国内相关立法工作也在进行中。另一方面，中美贸易摩擦下，已有美国软件公司断供中国企业的先例，这让Salesforce等国际品牌在服务稳定性和数据安全性方面存在诸多不确定因素。在这种形势下，该企业选择销售易替代Salesforce以确保数据安全合规。

销售易如何满足500强企业的安全隐私合规需求

1/在项目开始前，该企业通过问卷形式对销售易开展供应商安全评估。问卷涉及“本地部署”“SaaS”及“外部托管”三种部署方式，问题角度涵盖安全技术、管理制度、合规性、认证等方方面面，严格考核销售易的隐私保护能力，数据安全能力及合规性。最终销售易通过了评估测试，满足了该企业的要求。仅用7个月的时间就完成对Salesforce的替代，将其在海外的部分IT系统和数据迁移到了国内；

2/销售易在产品中内置了多项安全能力，能帮助企业保障客户数据安全：

*销售易提供三个维度的加密方式，用户可以根据需要对敏感字段开启加密存储。数据加密可降低数据泄露的风险，也可以防止数据被篡改；

*对于个人用户的敏感信息**提供脱敏显示**能力，管理员可通过配置脱敏规则来保护个人用户敏感信息，**防止客户真实信息泄露及企业个别内部员工滥用个人用户信息的行为发生；**

*管理员可以根据需要启用web端、app端的**数字水印功能，可以有效威慑内部人员数据泄露**

行为，便于事后追责；

*为用户提供详细的**数据访问日志功能，可记录和监测企业用户内部人员的各种数据敏感行为，包括数据上传/下载、数据导出等；**

通过替换Salesforce，销售易满足了该企业在国内的数据合规要求。销售易所提供的产品安全能力，可以帮助该企业更好地履行数据安全和隐私保护责任。

6.3 世界五百强金融集团

该企业是世界五百强企业、美国最大的金融机构、美国最大的人寿保险公司之一，业务范围涉及保险、证券经济、金融顾问服务、资产管理等。

企业安全隐私合规挑战

金融行业因为掌握着大量客户数据，因其所收集和处理信息的敏感性，是被重点监管的行业。除此外，金融也是遭受网络攻击最多的行业之一。业务属性决定了金融行业对CRM厂商的数据安全隐私安全方面要求极高。

该企业的业务遍布全球多个国家和地区，在东南亚这一新兴市场，该企业在新加披、马来西亚、印尼三国都设立了分支机构。其中印尼作为GDP贡献最高的国家，在东南亚市场中占有一席之地，但印尼在法律层面明确要求数据本地化，要求企业将数据存储在印尼境内。因此该企业需要选

择一家能够满足数据本地化要求的CRM厂商。

销售易如何满足金融集团的安全隐私合规需求

1/该企业选择销售易作为全球多业务地区的CRM供应商，并将印尼作为试点。**销售易除了在新加坡设立了数据中心外，在印尼市场也设有单独的数据中心，可以满足该企业在印尼本地的数据合规要求；**

2/在数据安全方面，该企业作为金融行业巨头，在内部早已建立了一套严密的数据安全管理体系，**要求销售易就《外部服务商问卷》的27个维度的不同问题进行书面回答，**对于不明确的问题开会进行澄清；

3/**除此外，对于金融行业重点关注的业务连续性问题，销售易单独提交了报告，以证明销售易在容灾方面具备充分的技术保障。**最终销售易在经过了一系列安全评估后，与该企业达成合作。

销售易一直关注东南亚市场发展，印尼和新加坡数据中心的建立，能够覆盖东南亚市场安全合规方面的要求。除此之外，销售易还在新加坡设立业务部，以更好的理解和服务东南亚市场。

6.4 北欧汽车品牌-国内分支机构

该企业创立于欧洲，距今已有百年历史，在豪华汽车中占有一席之地，一直以“低调、安全”著称。此次与销售易合作的卡车业务，长久以来坚持“品质、安全、环保”理念，已经在全球100多个国家和地区设立数千家经销商和维修站，以保证售后服务。

企业安全隐私合规挑战

该企业对数据安全隐私保护要求极高，对销售易的安全评估历时两个月，**分别从企业微信、第三方安全公司、微软经典防御模型、企业内部安全标准出发，进行了四轮调研和评估，**以确保深入了解销售易的安全能力。

销售易如何满足汽车企业的安全隐私合规需求

1/企业微信是该企业计划开展业务的重要渠道。**因此，销售易的企微登录认证能力、与第三方统一认证平台对接能力、以及客户同步能力成为该企业对销售易进行安全评估的第一步。**销售易还根据该企业要求梳理了企微登录、与第三方统一认证平台对接的详细处理流程，并为其提供了专门的配置文档；

2/**销售易需要登录安全公司NETSCOPE网站，回答100多个关于安全威胁处理的问题，主要评估销售易面对安全攻击和其他突发情况时的应急能力。**在通过问卷后，企业还安排第三方安全厂商对销售易进行了安全渗透测试，并出具报告，证明销售易SaaS站点不存在高危、中危漏洞的威胁。在此基础上，销售易每年进行渗透测试，以确保安全能力的持续性；

3/**基于微软中的STRIDE防御模型回答50多个安全防御相关的问题。**微软SDL-STIRDE威胁建模是基于数据流图去识别不同环节是否存在仿冒、篡改、抵赖、信息泄露、拒绝服务、权限提升几个维度的安全威胁，并制定对应的消减措施，落实并验证的一个过程；

4/**该企业从内部安全控制标准规范出发，对销售易进行问卷调查与评估。**问卷涵盖应用错误处理、客户端会话保护、解决方案配置及组件文档化、正确使用加密、开发过程源代码安全管理、密码管理文档化与正确实现，开发、测试、生产环境安全隔离、安全日志审计等维度，主要考察销售易在安全设计、管控流程方面是否符合其规范要求。

在每一轮调研后，销售易还与该企业就部分问题开展澄清会进行充分讨论和说明，帮助客户明确销售易的安全能力。通过四轮调研与评估，该企业与销售易最终达成合作。销售易也成为该企业在国内合作的第一家CRM厂商。

结语

数据安全、隐私保护、合规是每个数字化浪潮下的企业都需要持续学习的必修课。只有确保数据的安全性、隐私性、合规性，才可能取得客户的信任，对销售易来说也是如此。作为CRM领军厂商，数据安全、隐私安全、合规是销售易的战略底线和生存之本，作为企业数据的守护者，销售易将继续为客户提供安全、隐私、合规的产品而努力。

如需进一步了解销售易安全性隐私合规实践，您可扫码下载

《销售易安全白皮书》

《销售易隐私白皮书》

出品

销售易研究院

主编

高建彬

特邀顾问

刘志强、张英男、李哲祎、杨帆、林雨、
李军、吴云、徐昭、马亮、韩宋、褚衍臣、傅盛戎、吴焱、朱冠亮、吴振海

关于销售易研究院

销售易研究院是国内企业级 CRM 领导者销售易的智库，以销售易丰富的最佳实践、成熟的产品体系和领先的行业洞察为支撑，聚焦政策环境、企业案例、行业态势、选型策略等研究方向，致力于通过持续性的深入研究，打造开放合作的研究平台，进一步推动中国软件产业、CRM行业又好又快发展，加速企业数字化进程，为更多企业打造以客户为中心的数字化运营带来全新的思考和启发。