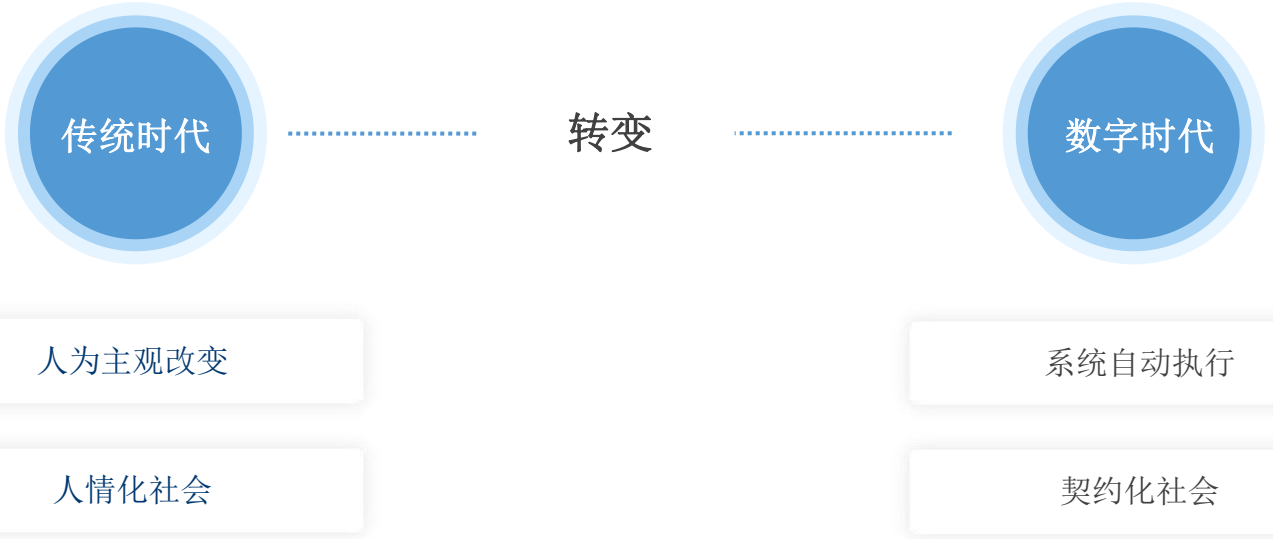
CSA研讨会-SaaS安全护航企业合规经营

数智化签约的数据合规性探讨

主讲人：Devin Pan

契约是数字经济时代的根基



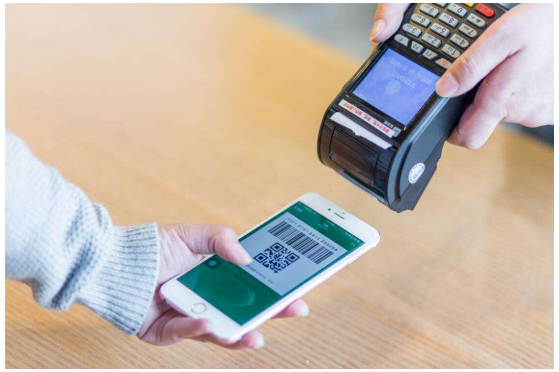
信息 + 数据

数字化社会遵循一切有数据、有记录、有事实基础上的实证。

Copyright © 2022 BestSign Inc. 保留所有权利。

电子签约把企业商业行为以合同签署为节点云化、数字化

契 约



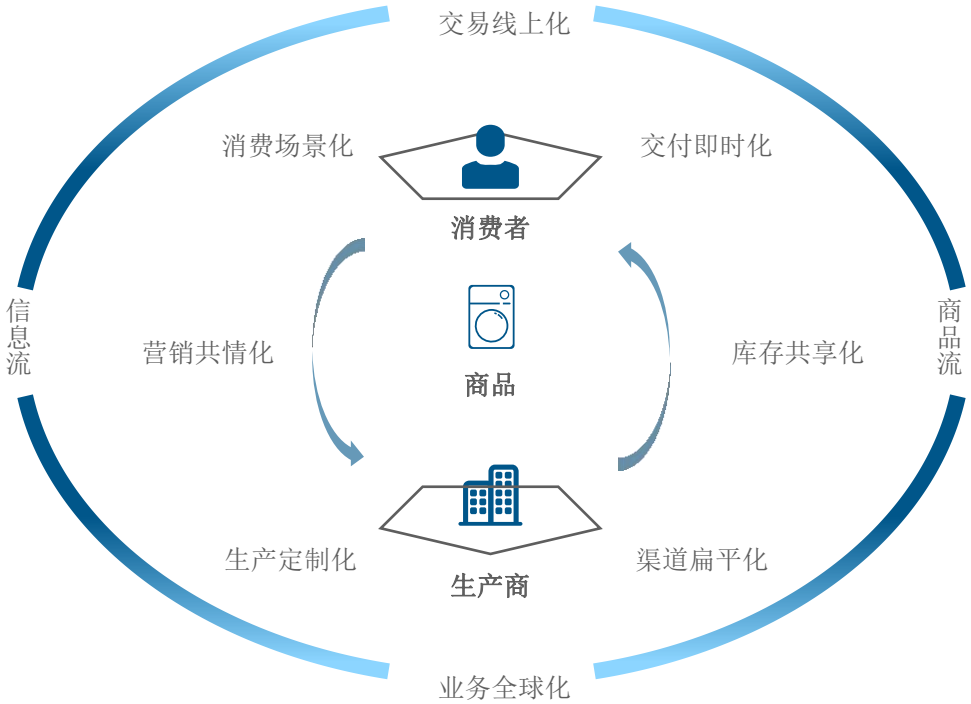
支 付

交 付

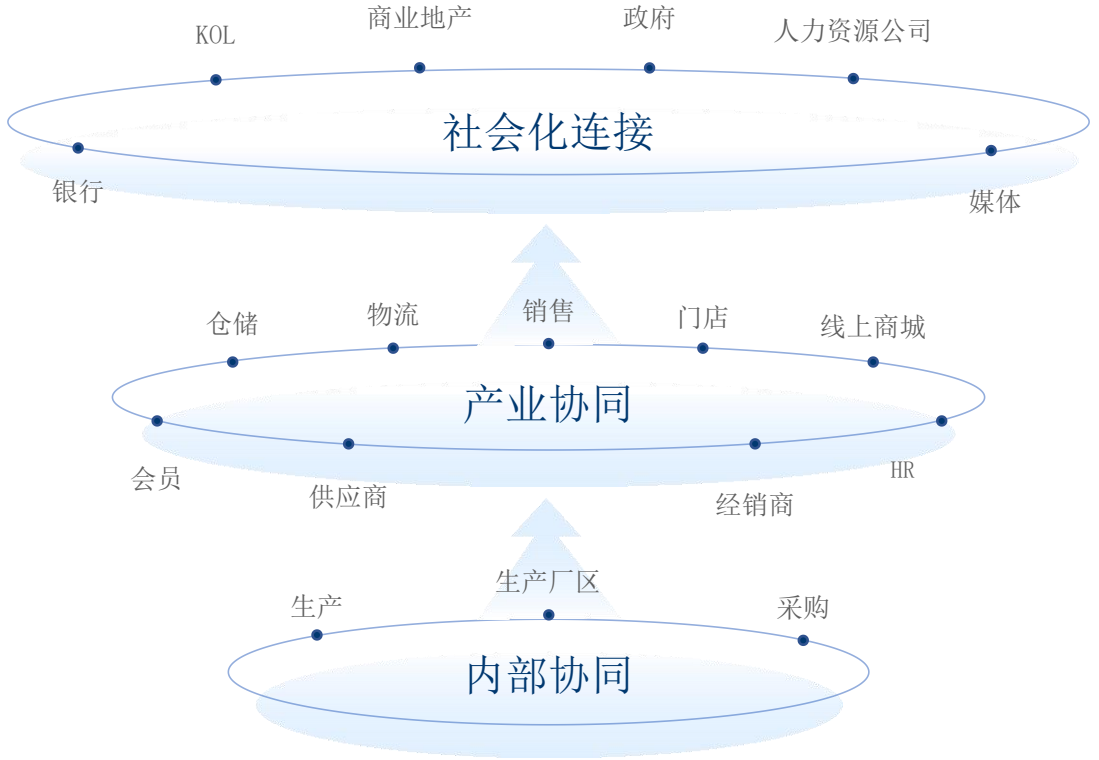
完整的数字化基础设施

Copyright © 2022 BestSign Inc. 保留所有权利。

电子签约同时具备构建跨组织的协同能力



高效零售&智能制造



基于互联网构建产业链协同体系

Copyright © 2022 BestSign Inc. 保留所有权利。

数字化管控信用风险和法律风险

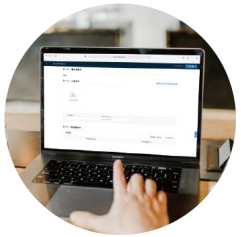
Copyright © 2022 BestSign Inc. 保留所有权利。

电子签约的本质：构建数字社会的信任底层设施

无纸化

成本节约

电子签名
电子印章
电子合同



线上化

效率提升

审批即发送
发送即接收
签署即归档

可视化

管理赋能

签约管理
风险管控
数据分析

多方可信

可信连接

连接多方
主体可信
可信流转

Copyright © 2022 BestSign Inc. 保留所有权利。

企业面临哪些合同数据管理挑战？

1. 传统的合同文档管理意识薄弱
2. 本地数据保存设施存在隐患
3. 内部安全管理制度不够完善
4. 缺乏专业可靠的数据安全专家

全面构筑中国信息及数据安全领域的法律框架

《网络安全法》

《数据安全法》

《个人信息保护法》

违规造成风险：

① 业务中断
② 巨额罚款
③ 信誉损害
④ 客户及收入的损失

Copyright © 2022 BestSign Inc. 保留所有权利。

个人信息处理方面的总体思路

（一）个人信息收集

① **合法性：**取得个人的同意、知情权，不隐瞒产品或服务所具有的收集个人信息的功能；

② **最小必要：**收集的类型与产品或服务的业务功能有直接关联，间接获取个人信息的数量是实现产品或服务的业务功能所必须的最少数量；

③ **自主选择：**产品或服务提供多项需收集个人信息的业务功能时，不违背个人信息主体的自主意愿。

（二）个人信息处理

未对用户个人信息进行特殊处理，包括利用大数据和算法对用户进行画像分析，只有在合同签署和法律出证的时候会使用到个人信息。

（三）个人信息存储

通过数据加密和密钥管理为敏感数据提供保护，如个人/法定代表人证件号采用国密算法SM4进行加密存储，有效保护了个人信息的存储安全。

实时公证

针对合同签署过程中的关键节点进行在线公证，确保能够实时留痕，不可篡改，在面对个人信息风险事件时，企业能做到自证清白。

效益：企业借助电子签约严格落实法规制度，规避合同业务风险

Copyright © 2022 BestSign Inc. 保留所有权利。

个人信息处理规则（一）

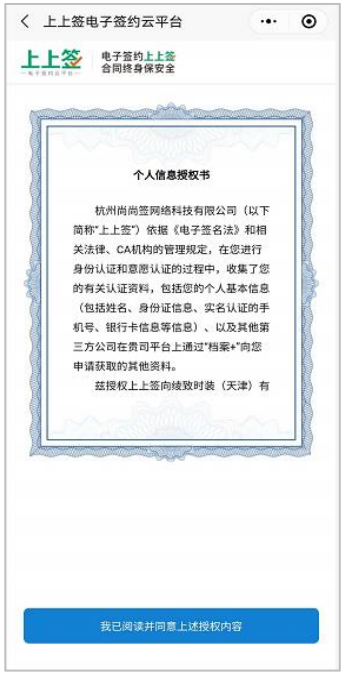
确立个人信息处理应遵循的原则，强调处理个人信息应当遵循*合法、正当、必要*和诚信原则，具有*明确、合理的目的，限于实现处理目的的最小范围，公开处理规则*，保证信息准确，采取安全保护措施等，并将上述原则贯穿于个人信息处理的全过程、各环节。(第五条 至 第九条)

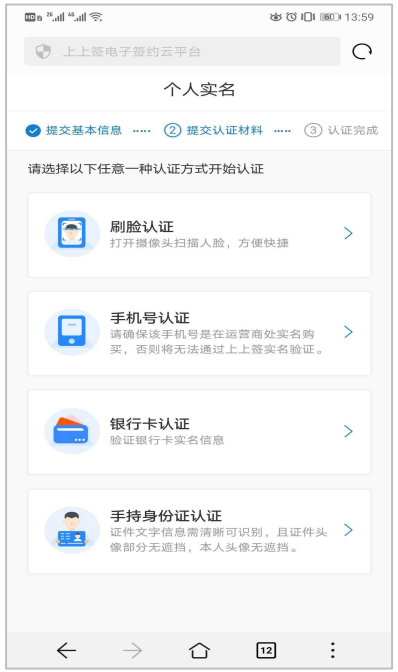
- **合法正当性：**上上签通过让用户勾选同意《上上签服务协议》、 《隐私政策》 和《数字证书使用协议》告知用户并取得用户的同意才会收集用户信息
- **必要性：**上上签仅会收集和电子签约业务相关的信息 ，包括身份证/护照身份证明或面部生物特征信息，并用于法律规定的实名认证以及正常使用发起合同、申请公证、享受上上签的会员服务
- **公开处理：**上上签在《隐私政策》 中明示个人信息处理的目的、方式及范围，例如将个人身份信息会传输至电子认证服务机构(CA)或个人身份信息及签约合同信息传输至公证处，由 CA 以出具数字证书之目的或公证处以出具公证文件之目的使用并保存

Copyright © 2022 BestSign Inc. 保留所有权利。

个人信息处理规则（二）

确立以"告知-同意"为核心的个人信息处理一系列规则，要求处理个人信息应当在事先充分告知的前提下***取得个人同意，并且个人有权撤回同意***；重要事项发生变更的应当重新取得个人同意；***不得以个人不同意为由拒绝提供产品或者服务。***考虑到经济社会生活的复杂性和个人信息处理的不同情况，本法还对基于个人同意以外合法处理个人信息的情形作了规定。(第十三条 至 第十六条)





- 在合同签署业务流程中，涉及到处理用户信息的，会让用户先授权
- 上上签的人脸识别技术是联合外部合作伙伴提供，每次均会提示用户需单独同意
- 提供多种实名认证和签署意愿校验方式，包括但不限于使用人脸识别技术

Copyright © 2022 BestSign Inc. 保留所有权利。

CA数字证书生命周期管理

颁发后

- 通知告知用户其证书发放时间和存储位置

使用中

- 签署意愿校验，比如短信验证码、刷脸等

续期

- 提前通知并同意
- 或者下次签署时先同意

颁发前

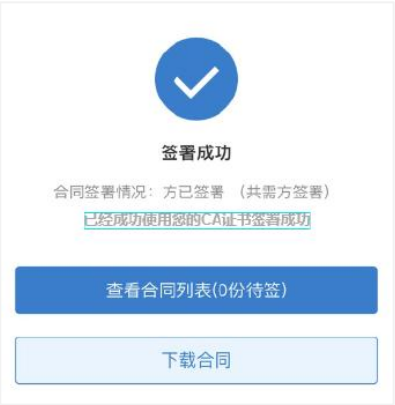
- 《数字证书使用协议》并告知用户
- 实名认证一致性 + 意愿性校验

使用前

- 文案告知用户即将调用数字证书进行签署

使用后

- 文案告知用户已成功调用数字证书进行签署



Copyright © 2022 BestSign Inc. 保留所有权利。

个人信息保护的合规检查点

① 实名认证（必须）

- 申请数字证书
- 出证服务

是否必须
主动勾选

- 《服务协议》
- 《隐私政策》
- 《数字证书使用协议》

选择刷脸

- 是否有明确的、单独的文案提示需要采集用户的生物信息，用户可以同意或中止流程

② 档案采集（可选）

- 甲方客户业务需要

发起采集

- 签署文案是否体现收集企业及目的，并告知解除授权路径
- 用户登录是否必须勾选三大协议，主动告知并签署《授权书》
- 企业信息采集过程中，是否通过自定义资料字段单独采集法定代表人和经办人的个人信息

Copyright © 2022 BestSign Inc. 保留所有权利。

提供全过程关键节点实时公证服务

免证效力

已为有效公证书证明的事实

无序当事人举证

优势证据效力

公证书的效力大于其他证据的效力

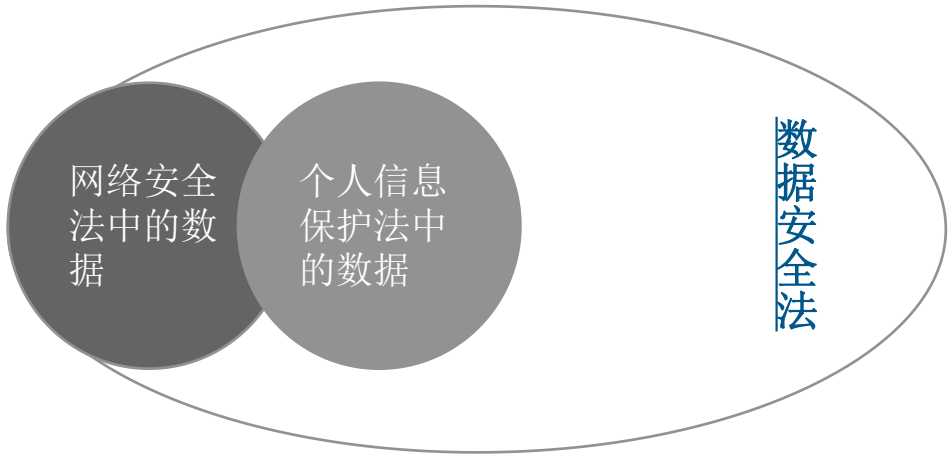
Copyright © 2022 BestSign Inc. 保留所有权利。

数据安全法推动外部数据储存保障

① 更好的保障数据安全有效

② 减少在数据安全性上的投入成本

与专业第三方服务商进行合作



Copyright © 2022 BestSign Inc. 保留所有权利。

数据生命周期管理

数据安全即以数据为中心的安全，保障数据的可用性、完整性和机密性。上上签数据安全策略立足于合规要求，从组织建设、制度流程、技术工具以及人员能力等方面入手，依据数据安全生命周期，建设数据安全保障体系。

数据采集	数据传输	数据存储	数据处理	数据销毁
最小够用原则；选择同意原则。	传输采用SSL/TLS加密信道，数据在落库的时候就是加密态，做到链路安全与支付宝一致。	个人隐私数据是国密4算法加密的，合同数据是用AES256 一文一密加密存储，数据中心在阿里金融云，做了网络隔离，外部无法直接访问。	想要访问到生产环境，需要VPN+堡垒机+workstation的工作模式，所有在生产环境的操作都会被录屏，目前只有核心运维人员有完整的权限。	遵从银行级的安全监管与合规要求，当客户要求删除数据时，遵循严格的数据销毁标准。

Copyright © 2022 BestSign Inc. 保留所有权利。

全球顶级安全权威资质认证

ISO27018
个人隐私保护国际认证

ISO38505
数据治理认证

ISO27001
信息安全管理体系认证

ISO22301
业务可用性认证

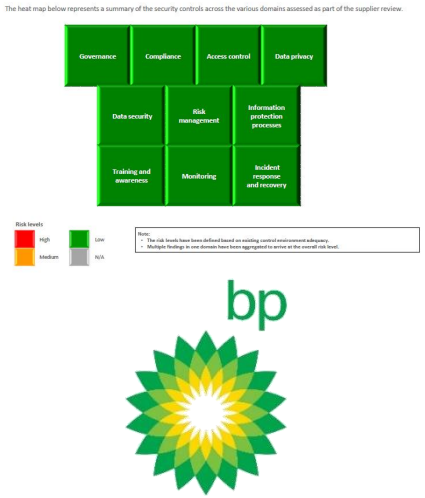
国家工信部
可信云服务认证

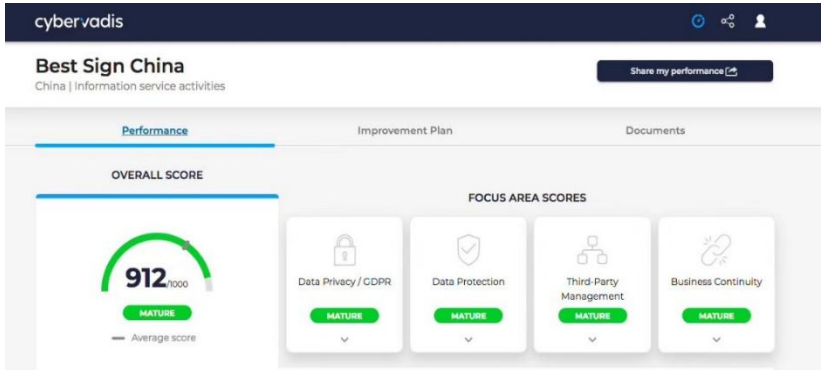
公安部
等保三级2.0认证

Copyright © 2022 BestSign Inc. 保留所有权利。

多次通过世界500强客户安全审计

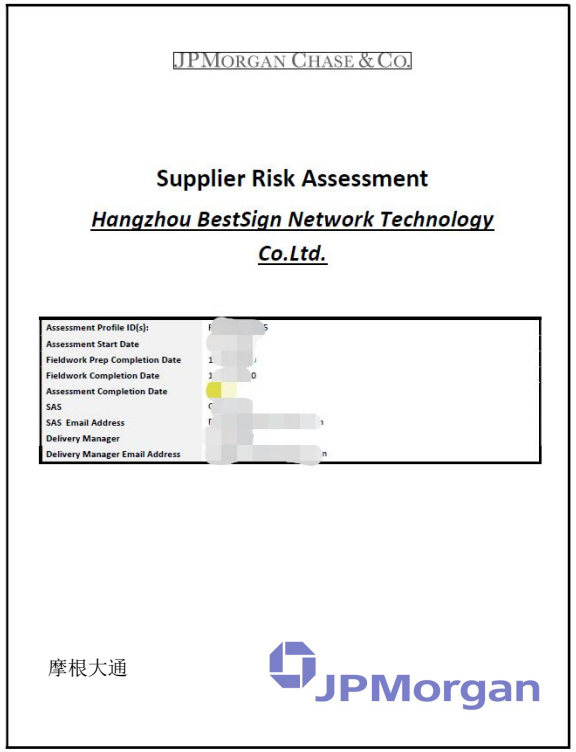
- 由第三方专业审计机构安永负责对上上签的产品、服务与公司管理进行安全审计
- 安全评估范围包括公司治理、数据安全、安全事件响应及恢复、访问限制、信息安全保护流程等10大方面
- 无中高风险项目，满足BP安全审计要求





- 独立第三方欧洲专业测评公司CyberVadis进行的供应商安全测评，上上签获得供应商有史以来最高分912（满分1000分，高于850分就被归类为最高等级的成熟系统）

- 向摩根大通新加坡进行汇报
- 通过摩根大通安全审计



Copyright © 2022 BestSign Inc. 保留所有权利。

好丽友案例：将伦理经营导入公司经营战略

- 对内

好丽友大力倡导员工志愿活动，积极推动节能减排、绿色工厂以及社区关爱等活动。

- 对外

依托开展多年的爱心厨房、全国儿童食品安全守护行动等项目持续助力青少年健康成长。

好丽友合规管理的重点领域包括食品安全、合同管理、知识产权与信息安全、劳动用工、反商业贿赂、进出口贸易合规等。

Copyright © 2022 BestSign Inc. 保留所有权利。

好丽友案例：保持公司基础数据的准确性和真实

电子签约合规管理

实名认证

档案+

经销商实名认证　　经销商数据采集　　核验数据的真伪　　确保基础数据的准确性

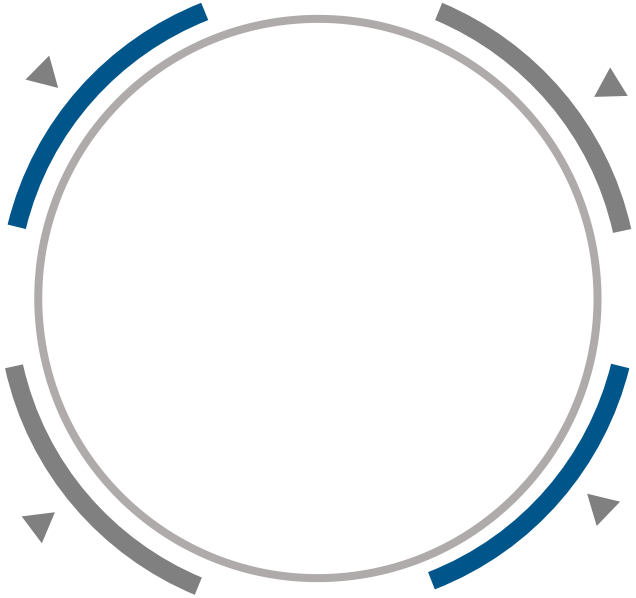
- 我们拿到的准确数据是法务在公司经营管理中最重要的一个贡献，在此之前，公司很难准确统计“到底每天有多少家经销商”
- 通过实名认证、基础数据的核验，可以筛查出证件造假、过期、人证不符等不合规情况，筛查出一批不符合规范的经销商

Copyright © 2022 BestSign Inc. 保留所有权利。

好丽友案例：企业与团队价值的双向提升

合规体系建设不断完善

线上自动化认证，经销商合规和信息真实性的环节做到最大程度的把控；
始终保持公司基础数据的准确性和真实，公司数据收集和存储正规化；
合同模板、印章、合同文件管理可控



业务运营和管理革新

多个系统业务数据不断沉淀和整合，形成整体业务的线上闭环；
经销商数据的动态管理，法务风控，还是合同管理协作，供应商网络管理等多个方面的效率都得到了极大的提升

法务团队价值显著提升

电子签约将法务团队从流程化的工作当中适当地解放出来，使他们可以把更多的精力投入到比较复杂、需要运用综合法务经验去处理的事务当中，赢得了业务部门的信任和公司的认可

伦理经营战略取得成果

法务团队荣获了集团伦理经营优秀案例；
沈阳工厂入选工信部"绿色制造名单"，获评国家级绿色工厂，在推进垃圾分类、电子签约等方面取得初步成效

Copyright © 2022 BestSign Inc. 保留所有权利。

合同数据储存的方案对比

	电子签约SaaS云服务	传统私有化部署
数据价值	在确保符合规范、国家安全要求下，**促进数据流动**	与法规设定的初衷相违背，容易**形成数据孤岛**
采集认证	基于告知+同意原则，最小化收集信息，通过身份认证且不可篡改，**避免合规风险**	采集认证过程在自己平台完成，**合规风险由企业独立承担**
产品设计	严格按照数据安全法、个人信息保护法以及电子签名法的要求设计，控制合规风险，**并承担作为平台的责任**	将个人信息保护合规要求嵌入本地产品全生命周期管理，包括产品开发、数据导入、数据存储、数据传输以及第三方合规审计等，**实施难度和面临的合规风险将大幅提高**
安全运营	平台具备完善的信息安全基础设施，提供**强大、持续**的 安全运营服务	需采购网络防火墙、服务器杀毒、数据泄露保护、漏洞检测与管理、入侵检测、操作审计等一系列的安全基础设施与软件
人员投入	平台建立专业可靠**安全团队**，企业只需要定期进行评估监督	需配备**专职安全工程师**来处理各种本地安全风险，每年需花费数十万元来保障服务安全

Copyright © 2022 BestSign Inc. 保留所有权利。

电子签约 x SaaS

携手共建数字化信任网络

1486万+	4.3亿+	150家+	3118万次	100亿+	99.99%
服务企业客户数（家）	平台个人用户数（人次）	500强企业客户（家）	单日合同签署峰值（次）	合同总量（份）	服务可用性

THANKS

CSA GCR cloud security alliance GREATER CHINA REGION ® × 上上签 —电子签约云平台—