CAICT 中国信通院

移动互联网数据安全蓝皮报告

（2021 年）

中国信息通信研究院泰尔终端实验室

2021 年 6 月

版权声明

编制说明

本报告编写参与单位：中国信息通信研究院、北京全时信安科技有限公司、北京爱奇艺科技有限公司、北京天眼查科技有限公司、好大夫在线、北京融世纪信息技术有限公司 、北京默契破冰科技有限公司、北京蓝城兄弟信息技术有限公司、北京点众科技股份有限公司、度小满科技（北京）有限公司、北京每日优鲜电子商务有限公司、北京思维造物信息科技股份有限公司、北京植德(深圳)律师事务所、北京米连科技有限公司、北京一起教育科技有限责任公司、同道猎聘集团、北京酷得少年科技有限公司、深圳平安智汇企业信息管理有限公司、北京自如信息科技有限公司、北京东大正保科技有限公司、满帮集团、北京中安国发信息技术研究院、北京斯尔教育科技有限公司、广州数融互联网小额贷款有限公司、北京畅行信息技术有限公司。

前　言

数据安全是通过采取必要措施，保障数据得到有效保护和合法利用，并使数据持续处于安全状态的能力。数据作为新型生产要素，正深刻影响着国家经济社会的发展，促进了数字基础设施的发展与产业的迭代升级。

从国家宏观政策角度来看，围绕数据安全保障能力建设，“十三五”规划中明确提出了要强化信息安全保障，加快数据资源安全保护布局。如建立大数据管理制度、实行数据分类分级管理，加强数据资源在采集、存储、应用和开放等各环节的安全保护，加强公共数据资源和个人数据保护等。中共中央关于“十四五”规划和二〇三五年远景目标建议明确提出建设网络强国、数字中国，发展数字经济，建立数据安全保护基础制度和标准规范，保障国家数据安全。

从行业微观应用角度来看，我国数字经济获得了新的发展空间，并深刻融入到了国民经济的各个领域。如，直播带货、在线游戏、在线教育和在线办公等新业态迅速成长，数字经济显示了拉动内需、扩大消费的强大带动效应，促进了我国经济的复苏与增长。在数字经济蓬勃发展的过程中，数据安全是关键所在。除了数据本身的安全，对数据的合法合规使用也是数据安全的重要组成部分。滥用数据或进行数据垄断，不合法合规地使用数据，将大大削弱数字经济的发展活力与动力。

本报告全面梳理移动互联网数据安全发展现状与趋势，深入探

讨移动应用在数据安全全周期面临的问题和挑战，并从数据安全管理要求，技术防范能力等多方面进行梳理，以期为移动互联网行业企业提供支撑和帮助。

目 录

图 目 录

表 目 录

一、移动应用数据安全发展现状与趋势

（一）国内移动应用数据安全发展现状

随着移动通信技术的飞速发展，移动应用成为了经济活动和民生需求必不可少的工具，全面覆盖到金融、医疗、教育、办公、交通等各个领域，移动应用种类和数量呈爆发式增长，对社会经济发展的基础性服务作用日益突显。

新时代下，数据作为生产要素参与市场分配，已成为企业发展乃至国家发展的重要战略资产。然而，移动应用前端的过度、强制索权，以及中后端粗放式的安全漏洞管理、数据管理、权限管理，甚至内外勾结陷入数据黑灰产等暗藏隐患，使得数据安全面临严峻挑战，而国内现有安全标准和企业安全管理及技术水平尚不足以攻克这一道难题。

近年来，移动应用数据安全问题越来越得到社会各界的广泛关注，国家、行业、企业积极开展多方共治，协同推进移动应用数据保护工作。国家层面加快立法及标准制定步伐、提供检测工具、加强执法；重点行业先行先试、加强行业自律；企业积极借助安全标准和检测工具，逐步探索最佳安全管理实践。

1.数据安全立法和标准陆续出台

随着移动应用数据安全领域的快速发展，数据合规立法和标准进入井喷期。《中华人民共和国网络安全法》作为我国第一部全面规范网络空间安全管理方面问题的基础性法律，对国家安全、社会

公共利益，保护公民、法人和其他组织的合法权益等做了要求；《民法典》之人格权编规定了隐私权和个人信息保护；《个人信息保护法（草案）》、《数据安全法（草案）》、国家互联网信息办公室关于《常见类型移动互联网应用程序（App）必要个人信息范围》层出不穷。

同时，信息安全技术系列标准不断迭出，《信息安全技术 个人信息安全规范》、《信息安全技术 个人信息安全影响评估指南》均已发布。工业和信息化部日前组织中国信息通信研究院、电信终端产业协会制定发布了《App 用户权益保护测评规范》10 项标准和《App 收集使用个人信息最小必要评估规范》8 项系列标准。

进一步，未来可预期的顶层的《个人信息保护法》、《数据安全法》均可能会发布，并与《民法典》、《网络安全法》共同成为个人信息保护和数据合规法律体系中的“骨架”，同时进一步通过制订行业标准、国家标准，以及司法案例的丰富，我国的数据法体系将进一步有“血”有“肉”。

2.数据安全治理和行动持续推进

2021 年 1 月 29 日，银保监会开出 2021 年第一张罚单，某银行因涉及发生数据安全管理粗放存在数据泄露风险、互联网门户网站泄露敏感信息等六项问题，被罚 420 万人民币。类似处罚不是个案事件，执法已经关注到了后端的数据安全治理情况。2020 年 5 月 9 日，中国银保监会披露一批罚单，包括 6 家国有大行，2 家股份制银

行在内的 8 家银行被罚了 1770 万元。被罚原因是，监管标准化数据（EAST）系统数据质量及数据报送存在违法违规行为，比如理财产品数量漏报、资金交易信息漏报严重等。这是中国银保监会首次就监管标准化数据报送等问题向银行业开出罚单。同时，工信部数据安全能力专项治理仍在持续推进。

3.数据安全共治模式稳步探索

一是鼓励企业开展自愿性 App 个人信息安全认证工作。2019 年 3 月，中央网信办、市场监管总局正式发布《移动互联网应用程序（App） 安全认证实施规则》，明确认证依据、认证模式、认证流程、认证规则、时限等要求。认证需按照 App 运营商自愿申请的原则，由具备资质的认证机构依据相关国家标准对 App 收集、存储、传输、处理、使用个人信息等活动进行评估，符合要求后颁发安全认证证书并允许认证标识。通过鼓励搜索引擎和应用商店优先推荐获证 App 等方式，引导消费者选用安全的 App 产品，提升个人信息保护意识和能力。

二是第三方机构、安全企业探索 App 检测评估服务。相关单位积极开展 App 数据安全与个人信息保护检测能力建设。如已建设的相关平台，可实现应用商店及 App 市场发展和接入情况监测、数据安全和诱骗欺诈风险检测， 强化对应用商店及 App 巡查监测能力，为行业主管部门开展 App 数据安全监管提供技术支撑。部分安全服务企业也建立 App 测试平台，通过静态检测、动态检测、源码扫描

等技术，为企业提供本地数据存储、数据传输、加密安全、第三方 SDK 等方面的安全检测服务。

三是重点地区和业务领域发布 App 行业自律公约。2014 年，为规范 App 发布虚假信息、窃取用户隐私、非法营销等行为，促进行业健康有序发展，北京市互联网协会组织新浪、网易、搜狗、今日头条等 50 余家互联网企业签署《北京市移动互联网应用程序公众信息服务自律公约》，这是国内首个移动互联网应用行业自律公约。2019 年， 一起教育科技、科大讯飞、极课大数据、思骏科技等企业共同签署学习类 App 行业自律倡议，在内容审核、商业模式、学生信息安全等方面明确了行业准则，承诺不断提升技术防护能力，及时总结推广成功经验，逐步建立学习类 App 使用管理的长效机制。

（二）国外移动应用数据安全发展现状与趋势

不仅国内数据安全面临严峻挑战，在移动应用发展较早的欧美国家，移动应用数据安全问题也日益猖獗。根据 2020 年 Verizon 数据泄露调查报告（The 2020 Verizon Data Breach Investigations Report），43%的数据泄露都与应用程序漏洞相关。尤其是 2020 年 COVID-19 疫情的爆发，通过应用程序非法调用个人位置数据和联系人信息等数据安全事件频发。基于此，欧美主要国家在构建基础性法律框架的基础之上，通过出台一系列行业规范、针对性指南并通过严格执法的方式对应用程序数据安全进行管控。

欧盟

2018 年 5 月 25 日，《通用数据保护条例》（下称“，《通用数）正式在全球生效。GDPR 旨在提升对欧盟居民个人隐私的保护与可控程度。GDPR 给予了欧盟居民对其个人数据的控制权，并对企业如何处理客户数据提出了要求。

根据 GDPR 的规定，处理欧盟境内居民个人数据的企业（包括移动应用，下称 APP）将需要遵守一系列隐私规则，不遵守相应的规则将会导致高额罚款。这些强制性规则包括：（1）必要性原则；（2）征得用户的知情同意；（3）数据处理透明清晰；（4）回应用户请求；（5）给予用户被遗忘权；（6）与第三方处理服务提供方或 SDK 服务方签署义务完备的协议；（7）准备数据安全预案并在发生数据泄露时通知用户；（8）指派数据安全保护官（即 DPO）；（9）数据加密处理；及（10）记录数据处理活动等。

除统一法律 GDPR 外，欧盟数据保护委员会（EDPB）还通过发布一系列指南指导各企业的行为规范。指南涵盖 GDPR 适用范围的界定、数据控制者和处理者的分类、如何获得用户的有效同意等，明确企业对个人数据的保护义务。

2021 年 1 月 5 日，欧盟理事会发布了新的电子隐私条例草案（即“，欧盟理事）。该草案一经通过将正式取代 2009 年的电子隐私指令，并对企业处理终端用户设备上元数据的方式施加了更多限制。

美国

与欧盟自上而下严格立法保护个人数据安全所不同的是，美国

基于促进经济发展的考量，暂无联邦层面生效的统一保护个人隐私/数据的法案[1]。其对个人隐私的保护依托于联邦贸易委员会的执法（即 FTC），散落在各专门立法及少数州的立法之中。如 1970 年的《公平信用报告法》（Fair Credit Reporting Act）、1974 年的《隐私法》（Privacy Act of 1974）、1986 年的《电子通信隐私法》（Electronic Communications Privacy Act of 1986）、1996 年《健康保险流通与责任法案》（Health Insurance Portability and Accountability Act ）、1998 年的《儿童在线隐私保护法》（Children's Online Privacy Protection Act ）；1999 年的《金融服务现代化法》（Gramm 服务现代化法》（line Priva）等，仅针对征信、金融、医疗、教育等特殊领域，或儿童、学生等特殊群体的个人数据收集、使用等问题做出了规定。2018 年美国发布《应用程序隐私保护和安全法草案》(即 APPs Act of 2018)[2]，这是第一部全国性的专门规范 App 收集使用用户隐私信息的法案，试图实现用户隐私保护与 App 功能正常之间的动态平衡[3]。

除联邦各专门立法之外，在州层面，2020 年 1 月 1 日，《加州消费者隐私法案》（即 CCPA）正式生效。CCPA 给予每位加州居民可强制执行的法定隐私权利。与 GDPR 不同的是，CCPA 要求 APP 允许用户选择退出（即 opt-out 机制），而不是要求 APP 在收集用户个人信息之前获得用户的明确同意。

值得注意的是，2020 年 11 月，加州通过第 24 号提案（即 CPRA），

[1] 见《后 GDPR 时代的美国数据隐私保护走向》，链接：https://www.secrss.com/articles/16618
[2] 见 https://www.congress.gov/bill/115th-congress/house-bill/6547
[3] 见《2019 版数据安全蓝皮书》

该提案有效地扩大了加州的数据隐私立法，将于 2023 年 1 月 1 日正式取代 CCPA。CPRA 借鉴了 GDPR 的经验，成立了新的数据保护执法机构—加州隐私保护机构（即 California Privacy Protection Agency，下称 CPPA）。同时，CPRA 扩大了针对数据泄露的行权方式，除以州检察长的名义提起民事诉讼外，CPPA 也可自行调查企业可能的数据泄露行为，并作出行政处罚，内容包括禁止令及罚款[4]。相比目前号称全美最严数据保护法案的 CCPA，CPRA 针对数据保护的要求更加严格，致力于保护个人消费者的隐私与防范数据泄露。

数据安全执法层面

欧盟与美国保护消费者隐私与用户个人信息最主要的手段就是采取强制执法措施来制止违法行为，并要求企业采取积极整改措施。

以欧盟为例，针对企业违反 GDPR 的行为，由欧盟各国监管部门作出相应惩罚。如，2020 年 10 月 30 日，英国信息专员办公室（ICO）就万豪集团泄露顾客个人信息一事对其开出 1840 万英镑的罚单。遭到泄露的个人信息种类因人而异，但可能包含姓名、电子邮件地址、电话号码、未加密的护照 ID，起飞/降落信息，以及顾客的 VIP 信息和会员号码。而 ICO 经过调查发现，万豪未能依照 GDPR 的要求，履行其系统的安全保障义务。

以美国为例，美国联邦贸易委员会（FTC）已建立两年一次的独立专家评估制度，并针对一系列移动互联网应用隐私问题开展执法行动，通过高罚款、禁止销售运营等强力处罚手段，震慑移动应

[4] 见 Sec 24 Establishement of California Privacy Protection Agency of CPRA

用提供者[5]如，2020 年 11 月 13 日，针对视频会议平台 Zoom 就其安全性的“误导性声明”，FTC 表示，当 Zoom 错误地声称其视频通话受到端到端加密保护时，该公司从事了“破坏用户安全的欺骗行为和不公平做法”。根据与联邦贸易委员会达成的协议条款， Zoom 必须采取具体措施解决投诉中的问题，并审查软件更新中的安全漏洞。该公司还被“禁止对其隐私和安全做法做出不当解读”，包括该公司如何收集和使用客户的个人数据，以及“用户能够在多大程度上控制其个人信息的隐私或安全”户。FTC 还要求 Zoom 必须让独立的第三方每隔一年评估其安全性，并在数据泄露的情况下通知 FTC。

综上所述，在移动应用数据安全方面，欧美等先行发展国家采取了构建保护数据安全专门法规、辅以高压执法的方式，用强力处罚推动企业落实法律法规要求，履行数据安全保护义务。

二、 移动应用数据安全问题

截至 2020 年第三季度末，我国国内市场上监测到的移动应用数量超过 350 万款，我国第三方应用商店在架应用分发总量达到 14723 亿次，免费的商业模式加剧了用户权益侵害的风险，我国互联网产业普遍采用前端免费、后端获利的模式，随着技术演进，盈利的模式也从在线广告向基于大数据的定向推送，精准营销转型，用户个人信息正在成为企业角力的核心。移动应用的数据安全问题可从监管执法行动和几大典型民事案例中一以窥见。

自 2019 年以来，中央网信办、工信部、公安部、市场监管总局、

[5] 见《2019 版数据安全蓝皮书》

中国人民银行、银监会开展多次专项行动。其中工信部连续两年的专项行动中责令 1336 款违规移动应用进行了整改，公开通报 377 款整改不到位的移动应用，下架 94 款拒不整改的移动应用，监管部门将会加强对移动应用程序信息服务的监督检查，及时清理处置违法违规移动应用程序和应用商店，营造出清朗的网络空间。

在“微博诉脉脉”案[6]中，淘友天下技术有限公司、淘友天下科技发展有限公司（以下简称“被告”）并没有基于《开发者协议》在取得用户同意的情况下读取非脉脉用户的新浪微博信息，因此获取新浪微博信息的行为存在主观过错，违背了在 OpenAPI 开发合作模式中，第三方通过 OpenAPI 获取用户信息时应坚持“用户授权”户授平台授权”台授用户授权”的三重授权原则。被告未经新浪微博用户的同意及北京微梦创科网络技术有限公司（以下简称“原告”）的授权，获取、使用脉脉用户手机通讯录中非脉脉用户联系人与新浪微博用户对应关系的行为，违反了诚实信用原则和互联网中的商业道德，故判决维持原判，被告赔偿原告经济损失二百万元及合理费用二十万八千九百九十八元。

“微信群控”案[7]，系首例涉及微信数据权益认定的不正当竞争案，原告为腾讯公司，被告开发运营的“某群控软件”，利用外挂技术将该软件中的“个人号”功能模块嵌套于个人微信产品中运行，为购买该软件服务的微信用户在微信平台中开展商业营销、管理活动提供

[6] 来源于北京知识产权法院（2016）京 73 民终 588 号判决书。
[7] 来源于《中国对外贸易》2021 年第 1 期“2020 年数据竞争与个人信息司法案例盘点”，作者：刘晓春、李梦雪。

帮助，功能包括监测、抓取微信用户账号信息、好友关系链信息以及用户操作信息（含朋友圈点赞评论、支付等）存储于其服务器。擅自使用他人控制的数据资源是否构成不正当竞争，还需要重点考察是否属于破坏性利用，只要不是破坏性利用或有违法律规定，且能够给消费者带来全新体验的，一般不应被认定为不正当竞争。但本案中，被告行为势必导致微信用户丧失对微信产品的应有安全感，减损用户关注度，损害原告商业利益和竞争优势，属于损人自肥，有违商业道德，构成不正当竞争行为。

2020 年 3 月 20 日[8]，北京市第一中级人民法院对汪某某非法获取计算机信息系统数据案二审宣判。本案中，被告人汪某某使用专门用于侵入计算机信息系统的程序及包含大量用户名密码的样本数据，对抖音公司的计算机信息系统实施撞库攻击，非法获取了抖音公司储存的用户身份认证信息 177 万余组。海淀法院一审法院认定：被告人汪某某违反国家规定，侵入计算机信息系统，获取计算机信息系统中储存的数据，情节特别严重，其行为已构成非法获取计算机信息系统数据罪，应予惩处。二审法院驳回上诉，维持原判。

数据安全问题具体可从数据采集、数据传输、数据存储、数据使用、数据开放共享、数据销毁六个方面对数据全生命周期安全问题进行分析梳理。

（一） 数据采集环节中的安全问题

[8] 来源于《中国对外贸易》2021 年第 1 期“2020 年数据竞争与个人信息司法案例盘点”，作者：刘晓春、李梦雪

1.移动应用违规手机个人信息

隐私政策是移动应用运营者告知用户个人信息收集规则的主要途径。移动应用应在用户首次注册、登录移动应用时以弹窗、超链接等明显方式提醒用户阅读隐私政策，明示告知用户收集使用个人信息的目的、方式、范围，使用户充分了解其个人信息如何被收集、存储、使用、传输、共享、销毁。部分移动应用存在用户首次登录时要求用户默示“打勾”同意隐私政策（即未要求用户主动打勾同意），导致隐私政策难以起到告知和真正具有法律效力的“同意”作用，存在违规收集个人数据行为。除了前面的默认打勾的违规行为，还包括如：通过“登录/注册即表示同意隐私政策”的方式强制用户同意，且未提供拒绝选项； 移动应用仅展示隐私政策但未征询用户同意。

2.移动应用过度索取个人权限

移动应用因业务功能需要向移动终端操作系统申请权限，收集使用用户个人信息。移动应用应当遵循最小够用原则，仅收集使用业务功能必需的最少类型和数量的个人信息。但部分移动应用申请权限数量多，所收集的个人信息远远超出全国信息安全标准化技术委员会发布的《网络安全实践指南——移动互联网应用基本业务功能必要信息范围》中规定的必要信息，存在超范围获取权限现象。其中包含违规申请“拍摄”、“访问粗略定位”、“访问精确定位”、“读取外置存储器”、“录音”等危险权限。移动应用过度索权现象成常态，

为违规收集用户个人信息提供了渠道，一旦这些个人信息被不法分子获取滥用，将严重危害用户权益。

3.第三方 SDK 引发安全风险

为了满足移动应用的快速迭代，解决成本效率问题，移动应用中嵌入大量第三方 SDK。随着国家对个人信息专项治理行动的深入推进，第三方 SDK 存在的安全风险随之浮出水面。第三方 SDK 自身存在大量安全漏洞，包括 http 误用、SSL/TLS 不正确配置、敏感权限滥用、通过日志造成信息泄露、远程任意文件读取漏洞、越权调用未导出组件等。第三方 SDK 成为病毒传播新途径，不法分子通过制作、发布、吸引 App 嵌入含有恶意代码的第三方 SDK，造成短时间、大范围的病毒传播和感染。第三方 SDK 隐蔽收集个人信息问题逐步显现，第三方 SDK 具备收集个人信息的能力。第三方 SDK 收集了哪些个人信息，用户往往难以感知，移动应用开发者也未必完全知悉，因而导致多起第三方 SDK 隐蔽收集个人信息的安全事件。

（二） 数据传输环节中的安全问题

移动应用客户端与服务器间进行个人敏感信息传输的过程中，如果没有采取有效的保护措施，存在用户个人敏感信息泄露和篡改的风险。使用 HTTP 协议进行明文个人敏感信息的传输，个人敏感信息在嗅探或者抓包等攻击中会被泄露。使用 HTTPS 请求时以 URL 的方式传递包含明文个人敏感信息的参数，URL 被转发或存储时存

在泄露场景。使用 HTTPS 传输明文个人敏感信息，如 SSL 版本错误、使用不安全的密码算法、非合法 CA 证书等场景下，存在中间人攻击、降级攻击、协议版本漏洞等攻击场景，导致用户个人敏感信息的泄露和篡改。

（三） 数据存储环节中的安全问题

1.明文存储个人敏感信息

数据存储是移动应用运营过程中的关键环节，移动应用应优先在用户个人终端内加密存储所收集的个人信息，确保用户数据即使泄露也难以被破解。移动应用会在用户终端内存储运行日志、设备信息、用户信息等数据，存在明文存储用户个人信息的问题。移动应用的服务端同样会存储个人敏感信息，包含：密码、姓名、手机号码、邮箱、身份证号、银行卡号等，这些个人敏感信息存储在数据库中，很容易受到外部 Web 攻击以及内部员工越权违规操作，需要对个人敏感信息进行加密存储。发生数据安全事件时，若未对个人敏感信息采取加密等保护措施，会对移动应用运营者和个人产生极大的风险。

2.移动应用数据备份缺失

数据备份是移动应用运营者日常运维过程非常重要的一环，数据的丢失，对于移动应用运营者是灾难性打击。数据备份包含数据备份流程、数据备份策略、数据备份恢复等，必须严格执行到位。部分移动应用运营者存在数据备份策略执行不到位情况，如：微盟

“删库”事件，导致微盟的 SaaS 业务服务突然宕机，商铺后台的所有数据被清零。

（四） 数据使用环节中的安全问题

1.数据未进行分类分级保护

由于移动应用各行业属性及标准的不同，没有形成统一的数据分类分级方法或指引，对应数据分类分级的安全技术要求尚不完善。不同行业、不同场景的数据的差异化保护要求存在落实困难，难以全面覆盖。因此，移动应用企业在执行数据分类分级和安全防护实际工作中多停留在纸面和理论层面，部门数据缺乏有效的安全防护措施，造成数据的非授权访问、数据泄露等风险发生。

2.敏感数据未脱敏处理

移动应用运营者使用海量数据来支撑业务和辅助决策，这些数据在创造着巨大的商业价值。但是，诸如身份信息、银行帐户信息、位置信息、医疗信息等重要的敏感信息在使用的过程中存在严重的安全风险。移动应用运营者需要减少敏感隐私数据被非法使用和获得的可能性，消除对敏感数据不必要的访问和复制。

3.移动应用权限管理混乱

对数据的访问操作授权机制是保障数据安全的重要防线。操作用户通过身份认证即可进入授权环节，此环节会根据权限控制表判断操作用户是否有权进行数据访问操作。企业内数据源众多，数据

开放接口繁多，不可避免存在着数据授权粒度粗、数据访问权限过大、内部操作权限滥用等诸多问题。同时，企业缺乏有效的敏感数据的控制保护机制，如果不及时解决，数据的安全性难以充分保证。

4.数据操作缺乏审计告警

移动应用运营过程中，需要对敏感数据的使用操作、运行维护、开放共享进行定期审计和异常行为告警规则，及时发现数据使用过程中的隐患和风险。目前移动应用运营者对数据的不当授权和第三方滥用，缺乏有效的监管审计机制。在数据应用过程中，无法得知某个用户对数据具体做了什么操作、是否有违规和误操作，难以及时预警和追溯审计定责。

（五） 数据开放共享环节中的安全问题

1.移动应用数据开放存在数据泄露风险

数据开放共享扩大了数据访问的范围，移动应用数据资源跨领域、企业共享使用十分频繁。如：互联网电商平台完成一次购物环节，订单信息需要共享给商家、仓库、物流、快递查询平台、短信供应商等多家企业。数据被各方调取、使用、或存储到本地，存在共享管理责任不明确、数据超范围共享、扩大数据暴露面等安全风险和隐患。相关企业仅从业务出发，未针对应用场景充分识别、评估影响，未对照法律法规和技术标准注意梳理共享开发要求的情况，任何一个数据使用方未按照要求共享数据、未严格控制数据空闲范围、或防护措施不到位，都可能导致数据被未授权访问、使用，进

而引发数据泄露或滥用事件。

2.数据平台 API 接口安全问题

数据开放共享为企业带来商机与便利，另一方面也为数据安全保障工作带来压力。特别在开放场景下，数据平台 API 接口的应用部署面向外部用户群体庞大、性质复杂、需求不一等诸多挑战，需时刻警惕安全外部威胁。包含：API 漏洞导致数据被非法获取、网络爬虫通过 API 爬取大量数据、合作第三方非法留存接口数据、API 请求参数易被非法篡改。应对外部威胁的同时，API 接口也面临许多来自内部的风险挑战。API 类型和数量随着业务发展而扩张，通常在设计初 期未进行整体规划，缺乏统一规范，尚未形成体系化的安全管理机制。在身份验证、访问控制、数据脱敏、审计监控等方面存在安全缺陷。

（六）数据销毁环节中的安全问题

1.移动应用账户注销难，数据过度留存

账号注销功能是用户自主注销权的重要保障，也是民众关注的热点。移动应用账号常与用户银行卡、身份证等敏感信息相关联，若账号无法注销将导致用户个人敏感信息长期被运营者留存，增大数据泄露风险。部分 App 虽然提供了注销功能，但注销耗时长、流程繁琐，还需比注册时多提交额外非必要的个人敏感信息，如用户真实姓名、住址、邮箱、身份证照片等，且移动应用运营者并未明确额外信息在注销后是否会删除。相比简单的注册流程，为用户注

销账号设置了大量不合理条件，阻碍用户行使注销权。无法注销账户或者为完成注销流程需要用户额外提交个人信息的行为，均存在数据过度留存风险。

2.云端数据销毁存在残留风险

部分移动应用使用云服务供应商，为了优化资源分配、实现定期备份，提高可用性，服务供应商会移动或复制数据，这样才能在多租户环境中优化资源的使用情况。且数据会在多个数据中心间共享，数据被数据所有者移动，或者是在公共云里被服务供应商移动，原本位置的数据应该要销毁，如果有任何数据残留，就有可能产生安全问题，也可能出现未经授权访问残留数据的问题。

三、 移动应用数据安全管理要求

移动应用数据安全管理的基本要求包括机构人员、制度保障、分类分级、合规评估、权限管理、安全审计、合作方管理、应急响应、投诉处理、教育培训等方面。

（一）机构人员

通过明确数据安全管理责任部门，明确职责范围，有助于具体工作的落地和实施。即通过高屋建瓴的方式，由顶层设计开始，逐步向下，落实到实处。不同行业，不同企业，可以根据自身条件，划定符合企业自身发展需要的数据安全责任管理部门。为了更明晰的说明，这里列举某互联网企业的做法，以供参考。例如某互联网

企业内部设立数据资产管理委员会，牵头企业内的数据安全管理工作；该委员会的成员由企业负责人如 CEO 或 CTO 牵头，各业务和职能部门数据负责人组成；同时定义和明确了该委员会的具体职责：一是制定公司重要数据安全规章制度，二是对公司数据安全技术能力提出明确要求，三是对公司数据安全相关制度落实情况进行定期合规性评估和检查，四是应急处置有关数据安全方面的重大事件。

明确了数据安全管理责任部门的职责，这些职责的实施和落地需要企业内各个部门分别执行。同样，不同行业，不同企业，可根据自身条件，将管理责任和执行责任划分给不同的部门。这里，继续列举某互联网企业的做法，进行说明。

例如，数据资产管理委员会的具体数据安全管理工作由安全部，法规内控部等承担。各项工作的执行部门包括，但不限于：数据管理业务部门，数据使用部门，系统运维部等。

安全部的职责，建设企业数据安全防护体系，在数据安全各项活动中提供技术支持。法规内控部的职责，对业务部门在数据生命周期各环节的操作行为进行合规性检查，依据法律法规及公司制定，对违规操作进行问责。其他部门将公司相关数据安全规范在日常工作中实施落地，积极配合数据审计及合规工作。

在明确了部门职责的分工后，具体的数据安全管理工作需要由具体的责任人负责执行，企业可以在责任部门和执行部门设立数据安全工作岗位，由该岗位的人员承担相应的工作。同样的，不同行业，不同企业，可根据自身条件，将职责指定或划分给不同的人员。

（二）制度保障

企业应建立完备的数据安全管理制度体系，涵盖数据安全策略、管理制度、操作规程、记录表单等。指导企业管理人员和操作人员执行各类数据安全活动，使数据安全管理工作在企业内有章可循。

数据安全管理制度包括但不限于：数据分类分级管理、数据访问权限管理、数据安全合规性评估、数据全生命周期管理、数据合作方管理、数据备份与恢复、数据安全应急响应等。

（三）分类分级

定期梳理企业数据资产清单，包括通过合法方式收集、产生的，存储在计算机信息系统或其他存储介质中用户个人信息，包括但不限于用户相关数据、生物识别信息等。

在《金融数据安全 数据安全分级指南》中对数据安全的定级目标、数据安全定级原则、数据安全定级范围等做做出了说明，并对如何进行数据安全定级做出了详细说明，各企业可结合企业自身情况进行参考。

围绕数据全生命周期的各环节，采取有针对性的安全保障措施，下面对各环节的安全保障措施，提供一些安全建议，供企业结合自身实际，做出适合的安全保障。

数据采集需要获得用户充分授权,数据传输和存储需要确保数据加密，数据使用过程进行最小授权，大量或高危操作需进行审批，数据交换需法规内控部进行合规审核，数据销毁应按公司制度进行

执行。

对于数据特殊需求，如数据出境，需上报主管部门进行审批。

所有数据相关操作，都需要进行留痕进行记录，方便日后进行审计。

（四）合规评估

企业应依据《网络安全法》，《网络安全等级保护基本要求》、《电信和互联网用户个人信息保护规范》、《信息安全技术 个人信息安全规范 》等法律法规开展数据安全合规评估工作。

（1）企业应将数据安全合规性评估作为数据安全管理的重要内容和抓手，按照“谁运营、谁主管、谁负责”的原则，从组织建设、制度流程、技术工具、人员能力等方面开展企业整体数据安全保护水平评估并形成评估报告。评估报告中应包括评估对象基本情况、评估流程、评估要点对标情况、保障措施配备情况与佐证材料说明、问题分析和改进措施等。

（2）数据安全合规性评估内容包括但不限于数据安全制度建设情况、数据分类分级情况、数据安全事件应急响应水平，以及重点业务与系统数据合规处理情况、数据安全保障措施配备情况、合作方数据安全保护水平等。

（3）企业按照数据安全制度规范，按年度开展重点业务数据安全合规性评估并形成评估报告。重点评估业务数据处理活动中相关制度规范执行落实情况、数据安全保护措施配备情况等。实现对新

上线业务、重点存量业务的评估全覆盖，业务数据处理模式变化时应动态跟踪评估。

（4）企业按照数据安全制度规范，按年度开展核心数据处理活动平台系统数据安全合规性评估并形成评估报告。重点评估企业内部管理措施执行落实情况、平台建设运维部门及合作方数据安全保护措施配备情况等。。

（五）权限管理

需要对数据使用过程中的权限进行管理，确保数据使用过程中安全，权限管理基本要求:

一是，明确企业数据处理活动平台系统的用户账号分配、开通、使用、 变更、 注销等安全保障要求， 及账号操作审批要求和操作流程， 形成并定期更新平台系统权限分配表， 重点关注离职人员账号回收、 账号权限变更、 沉默账号安全等问题。

二是，按照业务需求、 安全策略及最小授权原则等，合理配置系统访问权限，避免非授权用户或业务访问数据。 严格控制超级管理员权限账号数量。

三是，对数据安全管理、 数据使用、 安全审计等人员角色进行分离设置。 涉及授权特定人员超权限处理数据的， 由数据安全管理责任部门进行审批并记录; 涉及数据重大操作的（如数据批量复制、 传输、 处理、 开放共享和销毁等）， 采取多人审批授权或操作监督， 并实施日志审计。

（六）安全审计

数据所面临的安全风险是动态变化的，企业需要通过实施数据安全审计掌握安全措施有效性，进而补足薄弱点，优化安全防御策略，真正实现数据安全。

（1）企业应对数据安全操作访问等日志留存，包含：授权访问、批量复制、开放共享、销毁、数据接口调用等重点环节。日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等。定期对日志进行备份，防止数据安全事件导致的日志被删除。

（2）企业应对数据安全操作访问等日志进行安全审计具备，及时发现攻击行为、违规操作、事后溯源等能力。重点审计分析内容：数据安全攻击事件、数据流动安全分析、数据访问行为分析。

（3）企业应对数据操作相关权限进行定期审计。对所有账号及权限进行变化监控，及时发现权限违规变化及权限蔓延情况。

（4）企业应加强数据安全审计管理，明确审计对象、审计内容、实施周期、结果规范、问题改进跟踪等要求。企业数据安全管理责任部门或核心数据处理活动相关平台系统负责部门应配备日志安全审计员，加强日志访问和安全审计管理，至少每半年形成一份数据安全审计报告。

（七）合作方管理

随着技术进步，社会分工合作越来越精细，不同主体间数据共

享、流通、交易需求越来越频繁。企业应该对为提供数据建模、数据挖掘、数据分析、系统集成开发、系统维护和技术支撑的合作方进行管理，确保合作方具有数据安全能力，可以从以下几方面对合作方进行管理:

一是，建立第三方数据合作管理制度，明确在数据合作过程中企业内部各部门的职责、联动机制，明确合作方管理规范和监督流程，明确合作方数据安全监督管理部门和执行配合部门，明确企业对外合作中数据安全保护方式和合作方责任落实要求;

二是，合作方监督管理部门建立合作方台账管理机制，牵头梳理形成并定期更新合作方清单（含合作方企业名称、合作业务或系统、合作形式、合作期限、合作方联系人等），加强对合作方数据使用情况的监督管理

三是，与合作方签订服务合同和安全保密协议中，应根据实际合作项目明确具体条款，包含但不限于下述内容：合作方及项目参与员工可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围及用途（应符合最小化原则），合作方数据安全责任、保障措施配备情况（保障措施不得低于本企业），合作结束后数据删除要求，合作方违约责任和处罚等。

（八）应急响应

移动应用的数据安全管理过程中应急响应是关键的一环节。如果处理不当，会导致业务运营及企业声誉遭受严重打击。

（1）企业应制定数据安全应急响应体系，制定应急响应管理制度、安全事件管理制度，开展应急响应培训、应急演练。保障数据泄露（丢失）、滥用、被篡改、被损毁、违规使用等突发事件发生时，进行有效应对和写作，保障数据安全。

（2）企业应参照《公共互联网网络安全突发事件应急预案》制定数据安全应急预案，包括应急处理流程、系统恢复流程等内容。数据安全事件对企业和个人信息主体合法权益影响等因素划分事件等级。结合事件场景和等级制定应急预案并开展演练，典型场景至少每年开展一次演练。每个核心数据处理活动有关平台系统至少两年开展一次演练。

（3）发生数据安全事件时及时采取补救措施，并向相关主管部门报告。发生大规模用户个人信息泄露、毁损和丢失时，采取合理、有效方式告知用户。及时总结数据安全事件情况，分析原因、查找问题，调整企业数据安全策略，形成事件调查记录和总结报告，避免再次发生类似情况。

（九）举报投诉处理

近年来，国家在数据安全和个人信息保护方面已逐步完善顶层立法设计，陆续出台多项规范性文件、行业标准，如《民法典》、《数据安全法（草案）》、《个人信息保护法（草案）》、《个人信息安全规范》等都对举报投诉进行了规范和要求，对企业数据安全和隐私安全合规已经产生显著影响，企业也需不断完善数据安全

用户举报与受理机制，建立用户数据安全举报投诉渠道，将举报投诉制度落到实处，包括但不限于:

完善数据安全用户举报与受理机制，建立用户数据安全举报投诉渠道，如电子邮件、电话、传真、在线客服、在线表格等;

明确举报投诉处理部门和人员、处理流程、处理要求等;

针对有效举报线索，及时核查处理并在接到投诉之日起十五日内答复投诉人;

（十）教育培训

数据安全培训教育是数据安全管理的重要部分，通过教育培训等投入，持续提高员工知识、技能和素质水平，更好地保障企业数据安全目标。

（1）制定数据安全教育培训相关制度，将培训要求以制度规范的形式，纳入到日常安全管理中来。明确培训目标、对象、时间、形式以及奖惩机制等。

（2）明确数据安全培训计划，针对组织范围内不同员工类型有针对性制定培训计划，区分培训内容、培训形式和考核要求。如:区分高层领导、数据操作人员、技术人员、新员工等。

（3）拟定数据安全培训内容大纲。数据安全培训内容分布应包括法律法规、政策标准、合规性评估、防护措施、应急响应流程、知识技能、安全意识等方面。

（4）构想多样的培训形式。教育培训应在确保培训人员与内容

合理的情况下，采取多种的方式结合培训。如：线上直播与线下培训相结合、内训与外训相结合、专项与日常相结合、图文与视频相结合等形式。

（5）制定数据安全培训考核奖惩机制。对未达到考核目标的人员进行相关处罚如：强制培训、绑定绩效等；对于有效完成培训的人员给予一定程度的鼓励。

四、数据安全生命周期管理

（一）数据采集

数据采集是指信息控制者在提供服务、开展经营管理等活动中，直接或者间接从个人信息主体、其他企业以及第三方数据供应方收集数据的过程。包括但不限于，由个人信息主体主动提供、通过与个人信息主体交互或者记录个人信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取信息行为。利用外部数源采集数据的，应对数据源的合法性进行确认。涉及到个人信息，应要求提供方说明个人信息来源与个人信息主体授权同意的范围。

1.1 直接从个人信息主体获取时，信息控制者需要

a)明确数据源、数据采集范围和频率，开展数据安全影响评估;

b)规范数据采集渠道、数据格式、采集流程和采集方式,定期开展数据采集合规性审查。

注：数据采集渠道包括但不限于手机 APP、SDK、纸质(电子)表单、电子摄像头、指纹信息采集器、体感信息采集等。严禁以非

法方式采集个人信息。

c)利用外部数据源采集数据的,应对数据源的合法性进行确认,涉及个人信息的,应要求提供方说明个人信息来源与个人信息主体授权同意的范围。

d)在进行个人信息采集前,以通俗易懂、简单明了的方式向个人信息主体明示采集规则,如收集、使用个人信息的目的、方式和范围等,并获得个人信息主体的授权同意。收集个人信息遵循最小必要原则,收集的个人信息类型应与实现产品或服务的业务功能有直接关联。

e)采集个人敏感信息时(包括但不限于个人头像、身份证、指纹等)需要严格遵国家相关法律法规。己方产品中嵌入的第三方程序、代码(比如 SDK)采集个人敏感信息时，必须由个人信息主体明确的授权同意方可采集。

f)数据采集的过程中需要针对数据做加密处理后上报,防止数据泄露以及被第三方通过技术手段非法获取。

1.2 从第三方数据供应方获取数据时，信息控制者需要

a)采取自动化手段从网站或其他公开数据库间接收集数据时，应考虑网站和其他公开数据库的数据处理能力和网络承载能力，不能影响网站和公开数据库的正常运行。

b)从第三方企业采集数据时，应采用合同协议等方式，明确数据采集的范围、频度、类型、用途等，并确保数据的合法合规性和真实性。

c)基于不同业务目的所收集的企业客户信息，根据所用于的目的，开展数据安全影响评估，并采取相应的有效保护措施。

d)从第三方企业采集数据时，应核查对方数据来源是否符合相关法律规范，不得使用非法采集数据。

（二）数据传输

数据传输是指数据从一个实体传输到另一个实体的过程，存在传输中断、篡改、伪 造及窃取等安全风险，应采取数据传输加密、身份认证等技术措施加强数据传输过程的安全防护。数据传输过程包括数据控制实体内部数据传输以及数据控制实体之间传输等场景。

2.1 数据控制实体内部传输，应满足以下要求:

a) 局域网内部应加强无线网络安全，生产网不应使用 WLAN，办公网使用 WLAN 应采用足够强度的安全防护措施，包括但不限于:

应通过绑定设备序列号或 MAC 地址(硬件地址)等硬件特征信息对无线接入点进行准入控制，合理设置传输功率，控制无线信号的覆盖范围;

SSID 应采用规范的命名规则，且不应泄露机构、网络特性、物理位置等信息;

不应使用缺省 SSID，应进行信号隐藏，并禁用 SSID 广播，避免攻击者通过扫描直接获取无线网络信息;

应加强无线网络设备的管理帐号和口令安全，不应使用弱口令;

应采用双因素认证方式对接入用户进行身份校验;

接入端设备不应安装和使用无线网络密码分享等对数据安全有危害性的程序;

应控制移动智能终端在内网和互联网间的交叉使用;

短期使用和临时搭建的无线网络应及时拆除或关闭。

b）对于跨部门跨业务的数据传输，需要进行严格的数据需求评审以及必要的鉴权，核心数据对外部业务暴露需要遵循最小化、必要等原则。非业务必须不得直接暴露用户敏感信息，需要进行去标志化、匿名化处理后使用。

c)传输通道建立前，应对通信双方进行身份鉴别和认证，确保数据传输双方是可信任的;

d)对客户端应采取准入控制、身份认证等技术措施，防止非法或未授权终端接入网络;

e)根据业务流程、职责界面、网络部署、安全风险等情况,合理划分企业网络系统安全域,区分域内、域间等不同数据传输场景,明确数据传输安全策略和操作规程。

f）梳理企业存在数据出境情况的业务,对涉及个人信息和重要数据出境的场景、类别、数量级、频率、接收方情况等进行梳理汇总。

2.2 数据控制实体之间传输，应满足以下要求:

a)与外部实体之间的数据传输应优先选择专线、VPN 等技术。使用公共网络进行通信的，应采取技术手段防范恶意第三方通过获

得网络操控能力，避免发生 APT 攻击、DDOS、Worm 恶意软件攻击等网络攻击;

b)采取虚拟专网技术的传输链路，应对 VPN 用户和权限进行严格管理，采取适当强度的用户认证方式，并应按照“最小权限”原则对用户访问权限进行管控，防范非法接入行为。

c)原则上涉及中国公民的个人信息数据，不得跨公司出境。

d)对外提供公共数据服务、以及第三方大数据公司在对外传输数据功能模块需要加强数据安全管理，防止撞库、恶意爬虫等可能危及数据安全的危险。

（三）数据存储

数据存储是指数据以某种格式记录在计算机内部或外部存储介质上。数据存储安全是数据中心安全和组织安全的一部分，同时数据完整性、保密性和可用性三个方面都有涉及。

3.1 为了能够合保证数据的安全性,要对数据存储介质的安全做好管理建设，相关要求如下:

明确组织机构对数据存储介质进行访问和使用的场景，建立存储介质安全管理规定/规范，明确存储介质和分类的定义，常见存储介质为磁带、磁盘、光盘、内存等，依据数据分类分级内容确定数据存储介质的要求。

明确存储介质的采购和和审批要求，建立可信任的渠道，保证存储介质的可靠。

对存储介质进行标记，如分类（可按照类型、材质等分类）、标签（对存储介质进行打标签处理，明确存储数据的内容、归属、大小、存储期限、保密程度等）。

明确介质的存放环境管理要求，主要包括存储的区域位置、防尘、防潮、防静电、防盗、分类标识、出入库登记等内容。

明确存储介质的使用规范，包括申请单、登记表等一系列访问控制要求及数据清理（永久删除、暂时删除等）和销毁报废（销毁方式、销毁记录）要求。

明确存储介质测试和维修规范，包括测试存储硬件的性能、可靠性和容量等以及如何返厂、操作人、时间和场地等内容。

明确常规和随机审查要求，定期对存储介质进行检查，以防信息丢失。

3.2 针对数据存储介质管控要做到符合安全要求,同时要对数据下载做好的严格的审核和日志记录，相关要求如下:

明确数据安全管理的岗位和人员，负责明确整体的数据存储系统安全管理要求，并推进相关要求的落地实施。

明确各类数据存储系统的账号管理、认证鉴权、权限管理、日志管理、加密管理、版本升级等安全要求

对数据存储系统的日志记录进行采集和分析，识别账号和访问权限，监测数据使用规范性和合理性，同时可对发生的安全事件进行分析和溯源。

3.3 备份和恢复是为了提高信息系统的高可用行和灾难可恢复

性，在数据库系统崩溃的时候，没有数据库备份就没法找到数据，保证数据可用性是数据安全的基础。相关要求如下:

建立数据备份与恢复的策略和管理制度，以保证数据服务的可靠性和可用性。

建立数据备份与恢复的操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、日志记录规范、数据保存时长等。

明确数据备份和恢复的定期检查和更新工作要求，如数据副本的更新频率、保存期限等，确保数据副本或备份数据的有效性等。

建立备份数据的压缩、完整性校验和加密策略要求，确保备份数据存储空间的有效利用和安全访问。

识别组织适用的国内外法律法规要求，结合自身业务需求，确保按照法律规定和监管部门要求对相关数据予以记录和保存及满足备份保存周期要求。

建立统一的、自动化执行的备份和恢复工具。

对备份数据采取安全管理数据手段，包括但不限于对备份数据的访问控制、压缩或加密管理、完整性和可用性管理。

（四）数据使用

数据使用是指对数据进行操作、加工、分析等过程，此阶段对数据接触的最深入，所以安全风险也比较大。因此要降低该阶段的安全风险，4.1 从数据脱敏、数据分析安全等方面着手，相关要求如下:

应结合数据分类分级表对敏感数据进行识别和定义，明确需要脱敏的数据信息，一般包括个人信息数据、组织敏感信息、国家重要数据（非涉密信息）等。

应定义不同等级的敏感数据的脱敏处理场景、流程、方法和涉及的部门及人员分工，根据数据使用者的职责、权限及业务范围采取不同的数据脱敏方式，如对开发人员使用的数据，可采用扰乱技术在脱敏后保留数据属性特征等；对投屏展示用的数据，可以选择掩码方式隐藏敏感的信息。

应配置统一的数据脱敏工具，提供静态脱敏和基于场景需求的自定义脱敏规则的动态脱敏功能，满足不同业务需求。

应在数据脱敏的各阶段加入安全审计机制，对数据脱敏过程的操作行为进行记录，用于后续问题排查分析和安全事件取证溯源。

应明确哪些人员可以使用数据分析工具，开展哪些分析业务，限制数据分析工具的使用范围，根据最少够用原则，允许其获取完成业务所需的最少数据集。

应制定数据分析结果审核机制，采取必要的技术手段和管控措施，保证分析结果不泄露敏感信息。如规定数据分析的结果需经过二次评估后才允许导出，重点评估分析结果是否与使用者所申报的使用范围一致。应明确规定数据分析者不能将分析结果数据用于授权范围外的其他业务。

应对分析算法的变更重新进行风险评估，以确保算法的变更不会导致敏感信息和个人隐私的泄露。

4.2 使用用户数据做分析时，应该是消除具体的用户身份特，并且数据使用范围应该是已经在用户征求范围内，相关要求如下:

应建立组织的数据权限授权管理制度，明确授权审批的整个流程以及关键节点的人员职责。

基于国家相关的法律法规（《网络安全法》、《个人信息保护法》等）要求及组织数据分类分级标准和处置方式等，对数据使用进行严格规范管理。如，当使用个人信息时，必须征得个人信息主体的明示同意。

数据授权过程应遵循最少够用原则，即给与使用者完成业务处理活动的最小数据集。

应定期审核当前的数据资源访问权限是否合理。如，当人员岗位调动或者数据密级变更后是否对访问权限及时进行了调整，避免数据不正当使用。

应建立数据使用的违规处罚制度和惩罚措施，对个人信息、重要数据的违规使用等行为进行处罚，强调数据使用者安全责任。

应配置成熟的数据权限管理平台，限定使用者可访问的数据范围。

应配置成熟的数据使用日志记录或审计产品，对数据使用操作进行记录审计以备责任识别和追责。

（五）数据开放共享

数据对外开放共享指企业在经营过程中，自身采集(含生成)的数

据分发共享至外部合作单位的过程。 企业按照国家法律法规与行业主管部门规章要求，向行业主管与监管部门等有关机构履行数据报送义务的情况，也属于数据外部共享范畴。与外部机构共享数据时，应充分重视信息安全风险。具体要求如下:

a) 数据共享行为不得超过数据交换需求评审中确定的数据范围，应建立规范的数据共享审核流程，由数据共享的业务方、共享数据在组织机构内部的管理方、数据共享的安全管理团队，以及数据共享具体风险判定的相关方，如法律团队、对外公关团队、财务数据对外管理团队等其他重要的与数据价值保护相关的团队，共同确认共享的数据未超出需求和授权范围。具体标准需参照已发布的《信息安全技术数据安全能力成熟度模型（DSMM)》制定。

b) 通过图片、PDF、EXCEL 文件等线下方式进行数据共享电子数据时，应采用文件加密、文件水印、补充法律声明等形式保障数据的安全性，安全责任落实到人;

c) 通过接口等线上方式进行数据共享时，应具备有效验证调用者身份的技术手段，如添加个性化标识，并通过传输加密、安全性监控和攻击防护等手段保障数据传输的安全性和可靠性，防范网络监听、数据泄露等安全风险;

d) 如共享数据涉及个人身份信息时，依据业务需求应采用去标识化(含加密技术)等方式进行数据脱敏;

e) 应将数据对外共享纳入企业的应急响应机制，在发生数据外部共享相关的数据泄露事件或违规违约行为时，应及时采取相应的

缓解措施，并执行安全事件应急处置流程。应定期对数据接收方进行现场检查，检查数据使用、数据存储以及数据使用后销毁等环节，保证协议的有效执行;

f)对共享的数据进行安全审计和日志审计，对传递数据的内容、用途、量级，数据接收方(细化至法人机构数据安全负责人)情况、使用时长、数据是否收回(或由对方进行销毁)等情况进行说明与审批，有关记录留档备查;

g)建立基于溯源数据的数据业务与法律法规合规性审核机制，并依据审核结果，增强或改进数据服务相关的访问控制与合规性保障机制和策略;

（六）数据销毁

数据销毁是指组织在停止服务、数据运行以及存储从而终止或释放再分配场景下，对数据存储设备、服务器和介质中的剩余数据采用数据擦除或者物理销毁从而确保数据无法复原的过程的过程。数据销毁的方式分为数据擦除和物理销毁。其中，数据擦除是指使用预先定义的无意义、无规律的信息多次反复写入存储介质的存储数据区域；物理销毁是指采用消磁设备、粉碎工具等设备以物理方式使存储介质彻底失效。

6.1 在数据销毁过程中，组织应授权至少 2 个不同部门开展销毁工作，并做好相应书面记录，具体要求如下:

a)应制定数据存储介质销毁操作流程，明确数据存储介质销毁

场景和技术措施，以及销毁过程所应遵循的安全管理要求，并对已共享或者已被组织内部使用的数据提出有针对性的数据存储介质销毁管控流程;

b)存储数据的介质如不再使用，应采用不可恢复的方式（可读写介质采用反复覆盖的方式处理、对磁介质执行消磁操作等。对于纸质文档、只读光盘等无法执行清除操作的介质，须使用碎纸机等专业工具进行粉碎处理。）对介质进行销毁处理;

c)存储介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行信息销毁，应通过多次覆写等方式安全地擦除数据，确保介质中的数据不可再被恢复或者以其他形式加以利用，具体措施包括但不限于:

d)采用数据擦除方式销毁数据时，应明确定义数据填充方式与擦除次数（如全零、全一以及随机零一最少填写 7 次），并保证数据擦除所填充的字符完全覆盖存储数据区域;

e)数据擦除后的存储介质应通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除结果;

f)针对数据擦除后擦除失败的存储介质，应进一步采用物理方式进行销毁;

g)数据销毁全过程应被有效记录，并由销毁部门针对销毁结果进行详细记录，同时应由另一部门开展定期检查和审计，以确保销毁真实性;

h)针对存储个人敏感信息或涉密数据的存储介质的销毁，应采

取物理方式直接将其销毁;

6.2 针对由于相应法规要求，对应留存的数据开展数据销毁时，应针对数据进行不可逆的去标识化存储后，销毁原始数据。并遵循以下原则:

a)个人信息匿名化处理，应确保数据被处理后不能被复原，且个人信息主体无法被识别或者关联;

b)应依据国家法律法规与行业主管部门规章，针对不同类型的数据设定其数据保存期，对于多不同保存期数据的集合，其保存期限选择其最长时限为该数据集合的保存期;

c)针对超过保存期限的数据，应在产品和服务所涉及的系统中去除待删除的数据，使其不可被检索和访问;

d)开发测试、数据分析等内部数据使用需求执行完毕后，应由数据使用部门依据数据销毁有关规定，对其使用的有关数据进行销毁处理;

e)针对个人隐私数据等敏感数据，应建立数据删除的有效性复核机制，定期检查能否通过业务入口与管理后台访问或检索已被删除数据。

五、数据安全技术能力

（一）数据识别

企业应该采用数据识别技术，对企业数据资产自动数据识别及标识，并定期进行敏感数据扫描，识别未标识的数据，实现数据的

分类分级管理。

建立及维护脱敏规则，对数据进行分类分级管理，如：敏感数据为 L4 默认脱敏展示及导出；（平台实现脱敏的敏感数据包括：手机号、固定电话、证件号、邮箱、通讯地址、身份证、银行卡号等。）

接收到用户进行业务数据下载请求后，脱敏模块根据脱敏策略自动化识别文件中的数据，如果与数据的特征与脱敏策略中的规则相匹配，则对数据进行脱敏处理，脱敏完成后将数据文件发送给数据使用者。

定期对数据库进行敏感数据扫描，针对未标识的数据进行确认并手工更新数据标签等级，对数据的使用进行监控，实现对敏感数据使用的审计，并根据国家对数据保护的合规要求、企业的业务拓展、公司安全合规的要求，持续优化及扩大脱敏数据的范围，通过新建或编辑脱敏规则，以实现对脱敏规则的维护，保证企业敏感数据的安全防护，降低敏感数据外泄后的风险。对企业业务系统敏感接口进行实时扫描，自动识别接口传输中的敏感数据，将扫描结果同步至溯源系统，实现敏感接口调用数据溯源管理。

对业务系统进行敏感数据统一加解密服务，自动对敏感数据进行加密，并进行权限控制及调用日志审计，确保敏感数据的调用得到有效保证及可追溯。（敏感数据包括：手机号、固定电话、证件号、邮箱、通讯地址、身份证、银行卡号等。）定期查验业务系统的数据场景，确保各类数据处理场景中数据脱敏的有效性和合规性，并根据国家对数据保护的合规要求、企业的业务拓展及安全合规的

要求，持续优化及扩大脱敏数据的范围，保证企业敏感数据的安全防护，降低敏感数据外泄后的风险。

（二）操作审计

国内外很多研究表明大部分的网络安全事故是由企业员工造成的，《2020 Securonix 内部威胁报告》调查则显示 62%的内部威胁涉及敏感数据的泄露，内部人员通过无意或恶意的操作造成的数据安全风险的问题，受企业对内部安全监控能力限制，以及属于单一场景下的授权可信操作，或以内部设施为跳板的攻击，通常难以被及时发现和有效处置，在此情境下对来自内部员工或系统的操作行为进行有效审计，将成为对内部安全风险的预警、处置、追责、威慑的必要手段。

操作审计,监控并记录系统账户的活动，包含控制台、API 接口、技术人员工具对操作系统服务和应用的访问和使用行为。可以将以上行为数据以日志或录像等多种形式保存到存储空间中进行事件记录、安全分析、资源配置变更追踪及行为合规性审计等操作。

应当跟踪记录当前到预定一定期限内的操作记录；应当可以通过特定的应用将操作记录转换为日志服务可解析的形式，以便分析、检索、查询、管理；应支持从操作时间、用户名称、资源类型、资源、操作指令等多维度查询分析操作历史。

（三）数据防泄漏

数据作为信息系统中的核心资产，需要符合安全 CIA 原则，即

机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）。随着互联网、大数据、AI 等应用的爆发，数据本身成为可以产生价值的资源，其资源属性不仅会给企业主体造成较大的经济损失、信用损失，甚至可能引发恶性的社会影响。数据防泄露技术主要用于保护数据机密性和完整性，确保数据不会被非法获取，不会被非法篡改。

1.数据泄漏的途径

一是内部人员利用职权之便有意或无意行为造成的数据暴漏在外部环境或脱离管理

离职人员泄密：权限管理疏忽造成人员离职时带走用户数据。

内部人员泄密：由于权限管理不到位、安全意识薄弱或因为利益关系内部员工有意或无意的泄漏了用户数据。

二是通过网络攻击等非法手段窃取企业数据

攻击者通过漏洞链接到目标服务器并获得操作相关数据的权限，造成数据泄露。

通过网络攻击获取数据，如：xss 攻击、csrf 攻击、sql 注入、第三方软件漏洞等。

网络传输安全措施不到位导致数据泄漏：通过 HTTP、FTP、SMTP、POP3、IMAP 等明文协议发数据时被截获。

三是失密

权限划分不合理或审核不严格，导致低权限账号能够查看高权

限数据。

使用明文存储数据或者使用了不安全的加密方式。

员工误将数据安全信息上传到公共网络中或在 qq、微信、邮件、网盘等软件中传播。

有权限的设备丢失或被盗窃。

2.防止数据泄漏的技术方案

在数据泄露防护方面，传统方式倾向于认为内网是相对安全的，所以重点会放在对黑客及外部攻击的威胁防护上，内部则通过 OA 系统、审批流、DLP 等技术手段对数据进行管理。传统领域的技术解决方案相对比较成熟，主要有如下几种:

一是网络隔离技术。通过虚拟专有网络（Virtual Private Network, VPN）等网络隔离技术，配合防火墙、安全组、网络流量分析等综合手段，将数据库等核心资产保护在可信任网络区域内。外发流量则通过白名单等方式对目标 IP 地址及端口进行控制。对生产环境与开发测试环境进行有效隔离，开发、测试环境不应使用真实的生产环境数据。

二是数据加密技术。数据加密作为数据泄露防护的基本技术之一，包含磁盘加密、文件加密、传输加密等技术方案。可以从数据泄露的源头对数据进行保护，在数据离开企业内部之后也能有效防止数据泄露，但对加密所使用的秘钥管理要求较高，一旦秘钥丢失或加密数据损坏将使原始数据无法恢复。

三是权限控制。权限控制技术按照黄金法则对数据进行管理，即认证（Authentication）、授权（Authorization）、审计（Audit），有时还会加上问责（Accounting）、身份识别（Identification），组成“，组成“if 法则”，权限控制技术一般会通过设置安全策略、安全主体及客体，在受保护数据生成、存储、访问时实现控制，防止数据被非法复制和扩散。

四是基于数据内容的防泄露保护。基于数据内容的防泄漏保护(Data Loss Prevention,DLP)，主要用于对企业内部敏感数据外发进行防护。DLP 以内容识别为核心，基于敏感数据内容策略定义，监控数据的外发通道，对敏感数据传输进行审计或控制。通过灵活的策略配置，可以实现阻断式、审计式等不同防护等级。

3.数据防泄漏的新技术

传统的数据防泄露技术在应对外部威胁时效果比较理想，大部分企业对外部威胁也会比较重视，尤其网络隔离、数据加密、权限控制等防护技术，其普及程度相对较高，基本成为企业安全体系建设的必选项。但在应对内部威胁时，传统数据防泄露技术则面临诸多挑战，而内部威胁已经成为数据泄露的主要途径，且呈现出手段多样化、隐蔽化的趋势。以传统 DLP 产品为例，其使用场景是防止内部人员有意或无意识的造成数据泄露，解决了快速响应、及时阻止的问题。但在应对新型数据泄露手段时则存在不足，不能达到准确溯源和提前预防的效果。为应对上述挑战，目前数据防泄露技术

已经开始跳出固有框架，寻找新的技术路线，综合来看，呈现如下发展趋势:

一是数据分类分级。对数据进行分类分级已逐渐成为合规落地的最佳实践，并被各行业监管规范与合规指南广泛采用。传统方式虽然也会对数据进行分类，并赋予不同的密级，但依靠人的经验，或是关键字、指纹、正则表达式等简单逻辑描述。新的技术路线则倾向于使用人工智能、自然语言处理技术对数据进行梳理，训练模型并生成机器学习规则，实时感知关键数据的分布和使用情况，为数据治理提供基础支撑。

二是数据生命周期安全防护。解决数据分类分级之后，配合不同部署方式和技术路线，可以覆盖整个数据生命周期的各个环节。尤其是以人为中心的内部威胁防护，如对用户行为的分析与意图预测、风险用户象限图等。分析模型实现流程一般如下：1）利用 DLP 技术对敏感数据进行追踪；2）为用户建立行为基线，采集用户行为信息，依据策略对用户行为进行加权打分；3）分析引擎对用户行为进行关联分析与意图预测；4）结合数据风险等级，利用机器学习算法对威胁等级进行综合计算。

通过上述分析模型，常见风险场景可被提前预知并进行监测，例如频繁打开大量敏感数据、突然下载共享服务器大量数据、用户终端短时间积累大量数据等。

三是数据云化。通过桌面云等技术手段，实现数据不落地、终端零数据的数据架构，通过桌面管理平台自身的多重认证、外设管

控、录屏审计、拷贝控制、防截屏、屏幕水印等技术和策略设置，实现涵盖终端、接入、网络、数据、平台多层面的安全设计，从而有效防范通过网络、邮件、FTP、USB 等渠道的数据泄露。

数据防泄漏技术属于数据安全中一个细分领域，目前基于深度内容识别、自然语音处理的数据防泄漏技术已经日趋成熟，并发展出一些适应国内市场的特色方向，但是也应注重传统数据防泄漏技术的运用，通过渐进式发展来构建立体化的企业数据防护体系。

（四）接口安全管理

面向互联网及合作方开放的数据接口，应当具备以下能力:

认证鉴权能力：鉴定接口调用方身份;

安全监控能力：限制违规设备接入，对接口调用进行必要的自动监控和处理;

数据安全加密能力：对涉及个人信息和重要数据进行加密;

调用审批能力：实施调用审批;

日志审计能力：定期开展接口日志审计。

应制定完善的接口上线、下线的相关制度和步骤，以便接口调用方有序处理相关服务;

接口上线前，接口提供方需要进行源代码安全审计、渗透测试等技术检查，及时处理安全漏洞，有效控制安全风险;

接口下线后，相关数据归档、数据删除（或销毁）、个人信息保护、消费者权益保护等问题充分达成一致，明确相关责任，并充

分履行用户告知义务。

数据保留期限应按照国家与行业主管部门相关规定与规则执行。

一是认证鉴权能力

接口需要有身份验证机制，如基于表单的认证（Cookie & Session）、基于 JWT(Json Web Token)的认证、基于 Http Basic 的认证、基于 Http Digest 的认证、基于 AccessKey 和 SecretKey 的认证、基于 Token 和 AppKey 的认证等。必要时需设置限流或黑白名单机制，防止非法访问。比较典型的使用场景，如开放平台中的 AccessKey 和 SecretKey 的认证，APP 平台中的 Token 和 AppKey 的认证。

1、开放平台接口场景中，接口提供方应为接口调用方分配唯一的开发者标识和密钥，用于接口加密，确保不易被穷举，生成算法不易被猜测。

接口调用方的请求参数中不能明文提交开发者标识，需要对该开发者标识进行防篡改和防重放攻击设计，如将开发者标识拼接到请求的参数中进行算法排序，并且添加随机字符串，进行加密处理，如 MD5 等；将生成的字符串，加入必要的唯一标识（如时间戳和随机字符串组合）作为最终 sign 值访问应用接口，同时接口服务端在指定的时间内记录该随机字符串，防止二次使用。

2、在 APP 开放 API 接口的设计中，由于大多数接口涉及到用户的个人信息以及产品的敏感数据，所以要对这些接口进行身份验证。

由于调用方（客户端）与接口提供方（服务端）接口的交互在请求之间是无状态的，当涉及到客户端状态时，每次请求都要带上身份验证信息，且需要将关键信息加密处理。客户端向服务端接口提供认证信息（如账号和密码、第三方 cookie 等），服务端接口验证成功后返回 Token 给客户端；客户端将 Token 保存在本地，后续发起请求时，携带此 Token；服务端接口检查 Token 的有效性，判断允许或者拒绝。

与开放平台的验证方式类似，服务端为客户端分配 AppKey（即密钥，用于接口加密，不参与传输），将 AppKey 和所有请求参数组合成源串，根据签名算法生成认证签名值，客户端发送请求时将签名值一起发送给服务端接口验证。这样，即使 Token 被劫持，劫持者不知道 AppKey 和签名算法的情况下，依然无法伪造请求和篡改参数。再结合上述的重放攻击解决方案，即使请求参数被劫持也无法伪造二次重复请求。

二是安全监控能力

接口安全监控应具备状态监控、故障隔离、黑白名单控制等接口调用控制能力。

监控报警能力：监控接口服务状态（包括状态码、成功率、耗时、时间戳等参数）并建立告警机制。

流控能力：控制规则包括最大允许接口调用并发数、流量、单位时间错误数等。

流控处理措施：包括告警、限流、拒绝、暂停等。

滥用避免机制：建立未授权和冒用接口的监测机制，发现问题及时处理。

同时还要具备黑白名单管理能力与故障监测和恢复能力。

三是数据安全加密能力

加密和签名应该分配不同的密钥，且相互分离。

不能以编码的方式将私钥明文（或密文）写在接口的相关代码中，SecretKey、AppKey 等密钥信息不应存储于调用方本地配置文件中，防止因代码泄露引发密钥泄露。

接口开发者应依据接口等级设置不同的密钥有效期，并对密钥进行定期更新。

未经用户授权，不应该采集或存储用户的敏感信息，如地里位置、IP 地址、身份证、手机号、银行卡号等。

对于必须采集的用户的密钥信息（如 SecretKey、Token、密码等）和私人敏感信息（如手机号、身份证），需要加密传输和存储。

采取必要的技术或组织措施确保用户数据的安全，包括防止未授权或非法处理用户数据、数据丢失或意外毁损(完整性和机密性)。

四是调用审批能力

接口提供方应对接口调用方进行审核，并制定和签署相关合作协议（包括但不限于接口调用频率，敏感数据保护），必要时应对调用方的安全保护能力进行技术评估。

应通过线上或线下手段，对调用方提交资料的有效性、完整性、真实性进行审核，对调用方身份进行合规性核验。

应对调用方的唯一标识（如 AccessKey、Token 等）进行存储与统一管理，并根据用户唯一标识进行应用身份认证、状态校验和权限控制等。

应按调用方的唯一标识（如 AccessKey、Token 等）、接口、用户等维度，依据最小授权原则进行授权，对于未授权的资源禁止访问。

接口开发者，需要能够控制接口调用方的频率。

五是日志审计能力

接口日志应按照国家要求和行业主管部门相关规定与规则予以保存，保存期限不少于 6 个月（180 天）。

应完整记录接口访问日志，相关日志应至少包括调用方唯一标识、接口唯一标识、调用耗时、时间戳、返回结果（成功或失败）等。

应对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。

用户的密钥信息（如 SecretKey、Token、密码等）和私人敏感信息（如手机号、身份证）不应在接口日志中进行明文记录。

应对日志进行定期审计，并对异常或敏感信息进行监控报警。

（五）个人信息保护

1.个人信息保护的重要性

个人信息被誉为 21 世纪最富有价值的资源。具体而言，个人信

息对自然人具有社会交往价值，对公权力主体具有管理价值，对企业等私主体具有商业价值。然而，在信息商业化过程中，信息失控已成为不争的事实。伴随着移动互联网的快速发展，各类 APP、网站平台的用户成为个人信息泄露的主要受害群体。伴随信息泄露而至的垃圾短信、骚扰电话、精准诈骗日益威胁着人们的隐私、财产甚至生命安全；同时，用户个人信息泄露还容易破坏市场秩序、制约经济发展，滋长各类犯罪、危害社会稳定，甚至引发公共安全及国家安全危机。因此，保护个人信息安全对于更好协调个人信息保护与信息自由流通，推动我国信息化进程，保护个人隐私，维护国家安全，促进和保障人权具有重大意义。

2.数据安全领域常见的个人信息和敏感信息

数据安全领域常见的个人信息和敏感信息见表 1。

表 1　APP 常见操作的个人信息和敏感信息

数据来源常见操作	具体的个人一般信息和个人敏感信息
注册或创建账号	昵称、头像、出生日期、手机号码、邮箱地址、身份证信息、面部特征、身高体重、照片、社会关系等
使用 APP 或网络平台时	设备存储权限、设备电话权限、设备型号、操作系统、唯一标识符、登录 IP 地址、GPS 位置、浏览记录、操作日志、服务日志信息等
使用地图找人功能	行踪轨迹、地理位置、登录 IP 地址信息等
使用动态 feed 流功能	浏览及搜索记录、位置信息、交易信息、行为习惯等

使用语音输入、文字输入	语音内容、文字信息、待翻译的文本信息等
使用各类认证功能	银行卡信息、实名认证信息等
使用支付功能	交易记录、消费记录、流水记录、虚拟交易信息、游戏类兑换码、虚拟财产信息等

来源：参编企业访谈

3.个人信息保护的具体内容

一是安全准则

收集准则：需要在 APP 应用或者网络平台上明确给出，会按照何种方式收集个人信息，以及在使用服务时主动提供或因为使用服务而产生的信息。例如：在创建 Blued 账号或者 ID 的时候，需要明确说明收集的昵称、头像、出生日期、手机号码、邮箱地址等这些信息的具体原因是因为帮助完成注册，保护您的账安全并完成网络实名制的需要等。在使用 Blued 软件时，需要申请设备存储权限和设备电话权限等操作权限的时候，必须明确弹出权限选择框，提供给用户进行确认和选择，不能默认开启敏感权限，严禁未经用户同意收集敏感信息。

存储准则：收集的个人信息必须存储在中华人民共和国境内，以下情形除外（法律法规有明确规定的、获得用户明确授权的、通过互联网进行跨境直播和发布动态等个人主动行为）。收集和存储的个人信息，其存储期限均为符合法律法规最短期限为佳，对于超期的个人信息，必须进行物理删除。

使用准则：使用用户个人信息必须征得用户同意并授权，例如在重要的产品或服务通知的时候，通过邮箱告知；参与抽奖等类似的推广活动，用提供的信息用于管理此类活动；关于购买相关信息以及条款、条件和政策变更等对用户个人至关重要时候，用提供的信息进行告知；用于防丢失和防诈骗目的等使用个人信息。同时，根据相关法律法规及国家标准，依法使用并使用用户个人信息的可以不经过用户同意。

二是安全策略

个人信息安全制度体系建立与发布：需要建立安全管理体系并发布，为后续的安全管理给予明确的权限和实施主体。以 Blued 为例，在 2019 年就建立了信息安全管理政策并发布。

组织架构岗位设置：在个人信息安全制度建立之后，需要建立相应的组织架构来承接对应的任务。应该设立个人信息安全保护委员会以及个人信息安全保护工作组。常见的岗位需要纳入个人信息安全保护工作组，例如：信息安全部负责人、系统架构师、运维负责人、安全管理员、安全审计员、业务系统管理员、风控人员、法务人员。

三是技术安全保障

最小授权：个人一般信息和个人敏感信息保护，需要做到最小授权，一般常见的个人信息均可在各类 APP 和平台的后台系统中进行查询和存储，这里需要注意，需要严格控制可以查询、展示、处理、使用、共享的个人信息的范围、数量，做到最小授权，严格管

理。同时在后台系统中需要对用户敏感信息进行进一步保护，例如用户手机号，在后台页面展示中，需要做脱敏处理；存储时，需采用相应强度的加密算法进行加密处理。

个人信息数据收集：个人信息数据收集和获取必须通过合法、正当的方式，明确处理目的，并获得用户的授权同意，如可在 APP 内或者网络平台内通过弹出采集告知同意框向用户明示和获得用户授权同意。为防止网页表单数据提交时被窃取，表单提交时，需要对表单内容进行加密处理，但对于登录时的密码，不仅要进行加密处理，最好可以保证每次提示登录请求时，密码的密文不一致。APP 数据传输的时候需要参考 https 安全传输机制，同时采用对称加密和非对称加密算法使用，可以防止数据传输对称密钥在客户端存储，也可能避免非对称加密带来的性能影响。

个人信息数据存储：敏感数据在存入数据库，应当采用当前安全算法进行数据加密，为便于公司系统内部流通使用，可以使用一个内部的密钥对进入数据库的数据进行统一加密。这种加密的数据可以在内部的多个系统之间流通，同时也可以被数仓同步。此处加密可以使用对称加密算法，内部系统与数仓均持有密钥可以解锁，内部密钥的持有应当进行权限控制，保障只有可信的人和系统才能对数据进行解密处理，数据可以在哪些内部系统、应用间流通以及哪些人员可以访问，需要通过预先评估和审批，对于不同安全等级或不同防护能力的系统，原则上重要数据不允许流转。

附录：移动互联网企业实践

优秀案例集 1：好大夫在线

好大夫合作业务处理中涉及到患者身份、病情、处方等个人敏感数据，要对开放平台开展数据安全管理。

1.合作方安全管理制度

制定《合作方安全管理制度》明确在合作业务开展过程中业务部门、法务部、安全部的职责。业务部门负责接入合作方生命周期管理，包含合作方审核、开通、登记等。法务部通过商务合同和安全保密协议，明确合作方数据安全责任、义务落实要求。安全部负责接入合作方技术对接过程安全评估、安全测试、安全验收及后续安全监控工作。

2.合作方信息管理

资产管理平台创建合作方信息管理，业务部门更新维护合作方清单信息，安全部门定期审计。包含：合作方、合作业务、IP 地址或域名、负责人等信息）。

来源：好大夫在线

图 1 好大夫在线合作方信息管理平台

3.开放平台安全评估

制定《OPEN API 接口安全设计规范》，包含：机密性、完整性、

可用性及身份鉴别等内容。开放平台 API 接口的方案设计、开发过程、功能变更，都要开展安全评估。按照安全设计规范实现安全功能和功能的安全性。面向服务合作方提供完整规范的 API 技术对接文档，要求合作方安全规范接入服务。以下为《OPEN API 接口安全设计规范》

表 2 好大夫在线 OPEN API 接口安全设计规范

序号	要求
1	传输加密：接口通讯使用HTTPS协议，对敏感信息的传输和存储应采用对称加密算法加密。
2	身份认证鉴权：面向互联网及合作方开放的数据接口具备接口认证鉴权。
3	数据校验：服务端要验证接受到数据与客户端发送的数据的完整性。
4	对象级越权访问控制：通过授权机制检查该用户是否在该条记录上执行所请求的操作。使用不可预测的GUID作为信息记录的ID。
5	接口过载保护：服务端接口防止被攻击者恶意访问，需要对接口访问频率设置一定阈值，对超过阈值的请求进行屏蔽限制。
6	日志记录：对身份认证、重要操作行为做日志记录，定期进行日志审计。
7	安全监控能力：对接口调用进行必要的自动监控和处理，具备发现违规接入和异常操作行为发现能力。

来源：好大夫在线

4.开放平台安全测试

开放平台 API 接口开发上线前进行安全验证测试。参考接口安全设计规范及《OWASP API 安全 Top 10》编写安全测试用例。包含:身份验证、水平越权、数据加密措施等。OPEN API 接口安全测试推荐使用 POSTMAN 工具进行测试。

5.数据安全监控

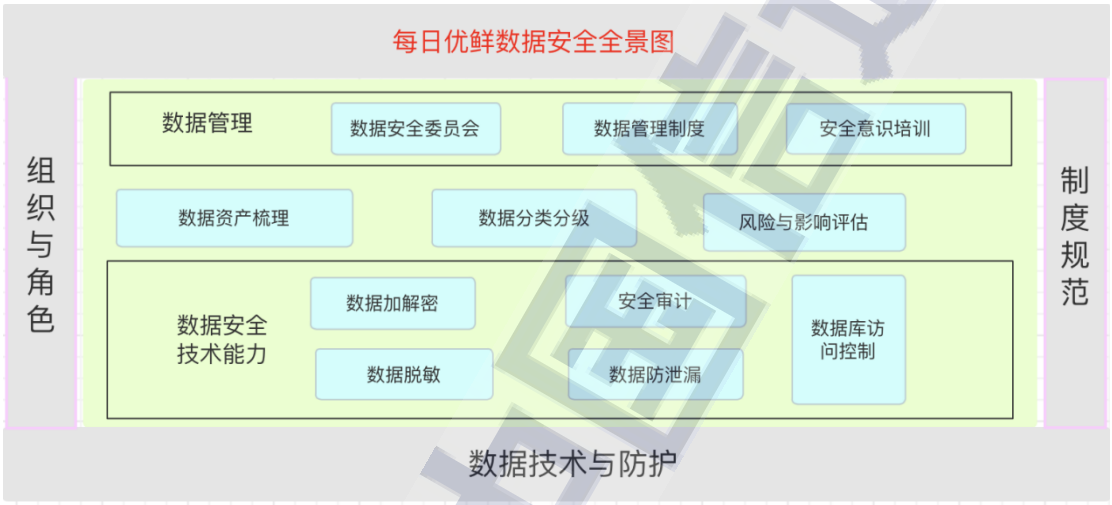
对开放平台 API 接口监控并记录日志，通过流量分析系统和 ELK 系统对接口传输日志进行记录和统计分析，及时发现数据接口异常流量、用户异常操作行为、异常调用等行为。对敏感数据进行传输情况统计分析，形成敏感数据的外部数据地图。

6. 引入权威机构评估

好大夫积极引入第三方权威机构对公司数据安全方面的体系、政策、技术等进行全方位评估。是工业和信息化部中国信通院“卓信大数据”计划首批成员单位，并通过多项“卓信大数据”计划专项。

优秀案例集 2：每日优鲜

每日优鲜公司高度重视数据安全工作，不断打造更完善的信息安全管理体系，已经通过了信息系统等级保护三级认证，以及 ISO27001 体系认证，首批通过信通院测评并被授予“卓信大数据”证书，获得过国家计算机病毒应急处理中心颁发的安全与检测最高等级认证。



来源：每日优鲜

图 2 每日优鲜公司数据安全全景图

公司成立了技术委员会，作为公司的数据安全规划指导组织，统一协调管理数据安全工作，技术委员会下设数据安全管理小组来推动执行各项数据安全活动，安全团队负责数据安全规范在日常工作中落实执行。

公司建立了数据分类分级管理、数据访问权限管理、数据安全合规性评估、数据全生命周期管理、数据合作方管理、数据安全应急响应等机制。基于数据的类别属性、使用目的等，明确了数据分类策略。在数据分类的基础上，对每一类数据，结合数据的重要及敏感程度以及一旦泄露、丢失、破坏造成的危害程度等，制定了相

应的数据分级策略。针对不同级别的数据，围绕数据全生命周期各环节规划了相应的安全保障措施。

公司具有明确的数据处理系统的用户账号分配、开通、使用、变更、注销等安全保障要求，及账号操作审批要求和操作流程，按照业务需求、安全策略及最小授权原则等，合理配置系统访问权限，避免非授权用户或业务访问数据。严格控制超级管理员权限账号数量。对数据安全管理、数据使用、安全审计等人员角色进行权限分离设置。

对数据授权访问、批量复制、开放共享、销毁、数据接口调用等重点环节实施日志留存管理，日志记录至少包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等，能够对识别和追溯数据操作和访问行为提供支撑。定期对日志进行了备份，防止数据安全事件导致的日志被删除。

对数据合作方安全管理，明确合作方数据安全监督管理部门和执行配合部门，明确公司对外合作中数据安全保护方式和合作方责任落实要求。并且在合作协议中明确了具体条款，建立合作方台账管理机制，更好的做好合作方的管理。

具有完善数据安全用户举报与受理机制，建立电子邮件、电话、传真、在线客服、互联网网站投诉受理、在线表格等举报投诉处理渠道。

此外公司在数据防护层面也有完善的机制，公司上线了基于 NTA 全流量分析技术，镜像核心交换机流量，对各种协议层面进行安全分析、监控及防范。公司上线了外网威胁监控系统，对公司主域名及子域名的解析的变动、公网 IP 安全监控、端口安全、钓鱼监

控、黑产暗网监控、IS 安全监控、GITHUB 信息泄露等进行全面感知和监控告警;接入了云 WAF 和网关做联动，进行了联防联控，防止 SQL 注入，XSS、远程命令执行等 WEB 层面入侵；二次开发了每日优鲜漏洞管理系统，对漏洞全生命周期进行综合管理，对漏洞分类分级，漏洞的产生，处理，修复，复测等全链路进行闭环，对常见的漏洞的产生如何去避免进行安全技术普及和安全加固。

这些技术措施和管理措施显著提高了数据安全能力，能够有效保护公司数据安全。

优秀案例集 3：爱奇艺

爱奇艺在数据安全治理上面临着诸多挑战：

（1）用户信息基数较大：围绕视频媒资衍生了游戏、主播、阅读等诸多业务线，日活用户达数亿人，随着移动端、TV 端、车辆网等智能设备的普及，进一步扩大了用户个人信息收集的边界；

（2）安全防护边界扩大：多种类型的网络系统以及多个数据中心的搭建和维护，海量数据的传输和存储为公司在数据安全管理方面带来了新的挑战；

（3）新技术、新应用引发新风险：爱奇艺一直关注科技创新，随着大数据、人工智能等技术的广泛应用，不可避免的为数据的处理和使用带来了更多的合规和安全风险；

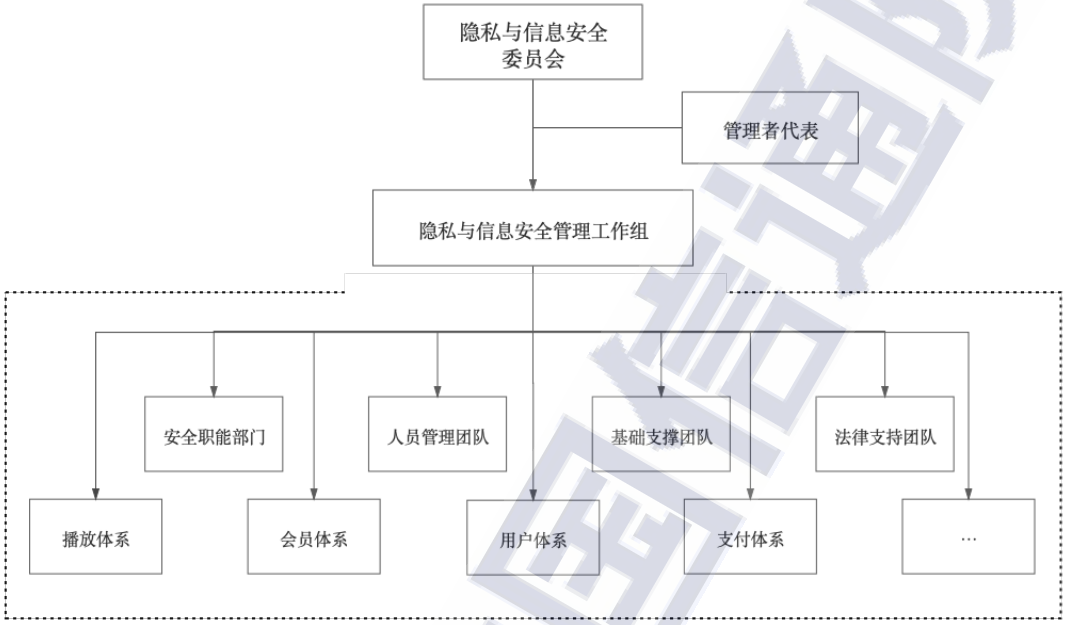
（4）数据类型多样性保护：除用户数据、公司数据和传统的业务数据之外，音视频等媒资数据作为爱奇艺核心数据资产，在数字版权保护方面具有特殊需求，对防盗版、防盗链、防泄漏、防篡改、可追溯等技术能力要求苛刻。

爱奇艺一直都极为重视数据安全治理工作，经过几年的努力，依据法律法规规范、业务自身需求和行业最佳实践，构建了一套完善的数据安全防护体系，下面从工作过程中一些好的实践和成果抽取部分做简要介绍：

1.组织结构升级——隐私与信息安全管理委员会

2020 年，爱奇艺全面升级隐私和信息安全管理体系，将信息安全委员会及信息安全管理工作组升级为隐私与信息安全委员会以及隐私与信息安全管理工作组，重新规划制定了组织的职责，重点纳入了隐私安全的相关要求。爱奇艺搭建了跨部门、跨业务、跨系统

的数据安全治理团队，安全、法律、内控、公共事务部、职业道德部、大数据中台、战略规划部、各事业部业务线等部门紧密协作，推动数据安全治理工作。



来源：爱奇艺

图 3 爱奇艺隐私与信息安全组织架构

2.国内外第三方权威认证

2019 年,爱奇艺通过了 ISO/IEC 27001 29151 认证，2020 年通过了 PCI DSS 认证和 ISO/IEC 27701 认证，成为国内视频行业中首批获得此类认证的平台。一系列国际安全认证的获得，体现了爱奇艺高层非常重视数据安全体系建设，以最高标准实施各项安全策略和法律法规、政策标准要求，并在实践数据全生命周期安全防护方面，达到国际标准水平。

同时，爱奇艺首批加入了中国信通院发起的“卓信大数据”计划，成为首批成员单位，并通过了“卓信大数据”计划数据安全方面的多项评估。

3.制定完善的管理制度体系

爱奇艺建立了完善的数据安全管理制度，从安全策略到评估文档，从数据分类分级标准到数据泄漏应急管理规范，全面覆盖数据安全治理各项工作。结合公司实际情况，公司紧紧围绕《爱奇艺隐私红线》，详细规范从数据收集、存储、访问、处理、共享到删除的全生命周期的数据安全管理要求，配套的行动指南为业务提供的具体指导，结合安全合规管理、业务/产品/项目隐私风险评审、数据安全专项培训等多维度的数据安全保护机制，积极推动数据安全制度落地。

4.全面的技术能力支撑

爱奇艺从事前管控、事中监控和评估、事后应急响应的角度，自研了合规风险管理平台（GRC）、移动安全分析平台（MSEC)、绿盾数据异常风险识别与管控平台等工具，囊括了数据分类分级、敏感文件识别和流转监控、数据库安全审计、大数据平台安全加固、敏感运营后台安全审计、合规项目安全管理、第三方安全管理等内容，采用“安全运营+风险管理”相结合的模式，在数据安全的重要环节投入更多资源进行加固。通过提升自动化能力，降低人力成本，在事前、事中、事后各个环节支撑公司数据保护治理能力。以用户个人数据保护为例:

事前:通过产品 SDL 服务及 MSEC 平台,对第三方 SDK 和 APP 中敏感权限调用、超前采集、高频采集、安全漏洞等情况进行代码分析和审核，通过 GRC 对第三方 SDK、APP 应用、对外数据合作实施数据安全风险评估，最后通过 APP 安全加固服务，保障 APP 在“事前”上线时处于一个安全、合规的状态;

事中：通过 GRC 项目管理跟踪 APP 合规态势，实施“隐私红线”季度全业务线 APP 隐私合规巡检，通过绿盾监控 APP 用户个人数据在公司内各系统间及与外部第三方系统间的安全、合规流动，保障用户个人信息在“事中”的合法合规使用；

事后：通过“安全吹哨人”机制和爱奇艺应急响应团队，第一时间了解到舆情动态、安全合规需求和数据安全事件，及时组织力量开展“事后”的应急响应。

5.创新合规管理和应急机制

爱奇艺建立了“安全吹哨人”机制，持续关注监管部门和社会事件中的隐私合规要求、合规事件，提升对隐私合规事件的反应敏感度和主动程度，建立预警信息的征集与评级流程，变“被动合规”为“主动合规”，减少或减轻舆情影响，并为业务争取更多合理的整改空间。

急响应团队，不定期组织外网渗透测试，及时发现和修复暴漏的安全漏洞和数据泄露风险问题；与行业内白帽子、威胁情报机构建立紧密的合作关系，及时有效妥善地处置各类安全漏洞和突发事件，联合相关部门进行安全事件溯源和打击。

6.参与标准制定、试点、加强交流与分享

进入数字经济时代，在国家安全和个人信息保护的大背景下，爱奇艺将业务发展与数据安全保护看成“多赢游戏”，在遵守国家法律法规对隐私合规的要求的同时，将数据安全保护作为新的增长机遇，积极寻求产品和技术创新，让“隐私和安全”成为产品亮点，赢得用户的信赖。

爱奇艺积极参与国家和行业数据安全保护标准的制定、试点、

推广等工作，如在监管部门指导下牵头制定国家标准《信息安全技术 网络音视频数据安全指南》，参与《APP 收集个人信息基本规范》等规范的编写等，并在各类数据安全与个人信息保护会议中分享爱奇艺的实践经验，为共同提升国家数据安全治理和行业数据安全保护贡献力量。

保护数据安全是企业生存的生命线，需要管理层的高度重视、完善的制度流程保障、不断优化的技术能力和全体人员的共同努力。爱奇艺通过科学高效的组织、管理和技术措施，构建了完善的数据安全管理体系，采用“安全运营+风险管理”相结合的模式，对数据全生命周期实施有效的安全管理。

承担应尽的网络安全义务，用心守护用户信任，是我们的重要使命，爱奇艺人通过创新不断的实践着这一切。

中国信息通信研究院 泰尔终端实验室

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300325

传真：010-62300325

网址：www.caict.ac.cn