扫一扫，关注官方微信

联系我们

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

亿赛通 ESAFENET

ESAFENET

亿赛通企业月刊　　中国数据安全专家　　www.esafenet.com

8 月刊

2021 年共 11 期

Esafenet
Monthly magazines

中国数据安全专家

主办：亿赛通

策划：市场部

北京亿赛通科技发展有限责任公司

地址：北京市海淀区西二旗大街 39 号 A 座四层

电话：86-10-57933600

传真：86-10-57933600

咨询热线：400-898-1617

网址：www.esafenet.com

CONTENTS 目录

刊首语 PREFACE

《亿赛通八月刊》划政策重点，分享独到见解

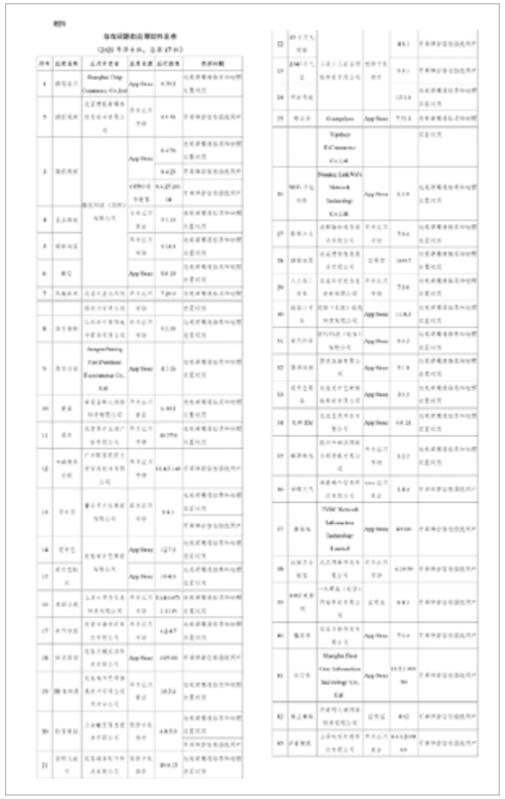
数据作为“要素”被正式提及要追溯到《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》，数据作为一种新型“生产要素”写入文件中，与土地、劳动力、资本、技术等传统要素并列为要素之一。《意见》明确，加快培育数据要素市场，推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护。

数据作为信息革命时代的基础性能源角色已经得到了明确认可，既然是新型生产要素，就必须像基础性资源一样投入市场、流动才能创造价值，要做到这一点的重要前提是要有完善、科学的数据治理规则。《数据安全法》将于 9 月 1 日正式实施，数据直接上升到了国家战略层面，身份和地位不同往日，而《亿赛通八月刊》梳理了近日公布的各项立法……

国内

1、工信部通报 43 款 APP 违规调用通信录、位置信息以及开屏弹窗骚扰用户等问题

摘要：工信部针对用户反映强烈的 APP 违规调用通信录、位置信息以及开屏弹窗骚扰用户等三方面突出问题，组织开展了“回头看”，共发现 43 款 APP 仍存在问题整改不彻底、技术手段对抗、同一问题在不同地域整改不一致的情况，腾讯视频、腾讯地图、微信、苏宁易购在列。



2、大学生贩卖自己身份信息成逃犯

摘要：近日，安徽芜湖警方发现，一名被湖北警方通缉的网上逃犯陈某在芜湖南陵县有活动轨迹。调查发现，陈某是在校大学生，因缺钱把自己的身份信息以几百元到 1 千元不等的价格卖给了别人。而这些身份信息却为诈骗分子实施犯罪提供了便利，陈某也成了网上逃犯。

3、小区业主的个人信息，竟成了这些人的香饽饽！

摘要：近期，青海西宁网安部门侦破一起房产领域侵犯公民个人信息的案件，抓获犯罪嫌疑人 22 名，查获 167 个小区的业主信息 77.8 万条。该案中的犯罪主体主要集中在房地产营销领域，部分销售人员通过购买、交换等方式获取公民个人信息，随后进行自己的营销工作，或是将手中的个人信息出售牟利。涉及的公民个人信息多为小区业主信息，内容包括业主姓名、身份证号码、联系电话、家庭住址等信息，这些信息极易被电信诈骗、敲诈勒索等犯罪利用。

4、阿里云被实锤泄露用户信息，官方回应已整改！

您好！近日您反映“阿里云计算有限公司未经用户同意擅自泄露个人信息”的投诉材料我局已收悉，经调查核实，现答复如下：

2019 年 11 月 11 日阿里云计算有限公司未经用户同意擅自将用户留存在的注册信息泄露给第三方合作公司，阿里云计算有限公司的行为违反了《中华人民共和国网络安全法》第四十二条规定，根据《中华人民共和国网络安全法》第六十四条规定，我局已责令阿里云计算有限公司改正。

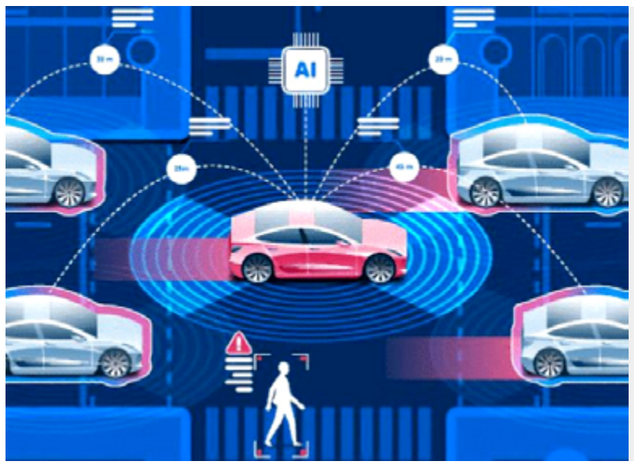
如对本答复函存异议，可在接到本函之日起 60 日内，向工业和信息化部申请行政复议，或在接到本函之日起六个月内向杭州市上城区人民法院提起行政诉讼。

浙江省通信管理局

2021 年 7 月 3 日

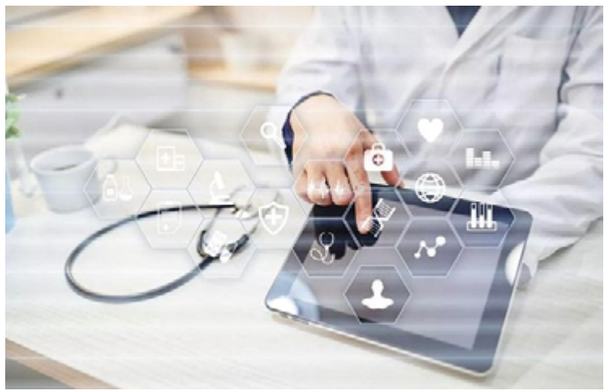
摘要：近日，网络上流传着一份答复函，这份答复函来自于浙江省通信管理局，明确指出了阿里云此前在没有得到用户允许的前提下，就将用户信息泄露给了第三方公司，在 8 月 23 日，迎来了浙江省通信管理局的实锤，表明该答复函属实。

5、你以为只是开车，其实海量个人数据可能泄露……国家出手了！



摘要：近日，国家网信办、国家发展改革委、工信部、公安部、交通运输部联合发布《汽车数据安全管理若干规定（试行）》（以下简称《规定》），自 2021 年 10 月 1 日起施行。《规定》倡导：汽车数据处理者在开展汽车数据处理活动中坚持“车内处理”“默认不收集”“精度范围适用”“脱敏处理”等数据处理原则，减少对汽车数据的无序收集和违规滥用。

6、疫后医疗数据泄露加剧！全国医疗机构网络信息安全管理办法将出台



摘要：近日，新华社主管的《经济参考报》引述消息人士报道，全国医疗机构网络信息安全管理办法正在起草中，不久将会出台。

7、孟子坤资源博发文称孟子坤个人数据被泄露

摘要：昨天孟子坤个人手机号再次被陌生号码以粉丝名义通过短信、电话等形式骚扰，已经严重影响到孟子坤的正常工作生活，并涉嫌泄露个人信息。请当事人立即停止该行为！这不是粉丝行为，私生不是粉，是自私，窥视不是爱，是伤害！在此呼吁大家，不议论、不转发个人隐私，坚决反对传播、倒卖个人信息等逾越法律底线的恶劣行为。

8、安全提示，这种“催交电费短信”不要点！

摘要：当手机收到涉及电费交纳的不明短信时，不要随意点击短信中的链接输入姓名、电话、身份证号、银行卡号等重要个人信息。如果不慎点击网址，手机可能被植入木马程序，造成个人信息泄露，存在资金被盗取的风险。

9、中纪委网站评阿里云泄露：个人信息保护安全锁不容撬动

摘要：个人信息保护之路任重道远。除立法规制外，还需多方联手协同共治。能够接触到公民个人信息的主体多元而广泛，从政府职能部门到企业，任一关口把不严、守不牢、管不住都会出现严重后果。就监管部门而言，仍需进一步加大对侵犯公民个人信息违法犯罪活动的打击力度，持续形成高压态势。企业、网络主体等信息采集方要落实主体责任，强化内部监管和自律，借助防窃密、防篡改等技术手段筑牢“防火墙”，切实解决滥用个人信息、对个人信息数据管理不力等问题，打通梗阻，平衡好公民权益保护和数字经济发展。

10、网信办规范算法推荐服务

国家互联网信息办公室关于《互联网信息服务算法推荐管理规定（征求意见稿）》公开征求意见的通知

2021年08月27日 10:09 来源：中国网信网 【打印】【转载】

为了规范互联网信息服务算法推荐活动，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，促进互联网信息服务健康发展，我办起草了《互联网信息服务算法推荐管理规定（征求意见稿）》，现向社会公开征求意见，公众可通过以下途径和方式提出反馈意见。

1. 登录中华人民共和国司法部 中国政府法制信息网（www.moj.gov.cn、www.chinalaw.gov.cn），进入首页主菜单的“立法意见征集”栏目提出意见。

2. 通过电子邮件将意见发送至：jiaxh106@cac.gov.cn。

3. 通过信函将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络法治局，邮编：100044。并请在信封上注明“互联网信息服务算法推荐管理规定征求意见”字样。

摘要：网信办发布关于《互联网信息服务算法推荐管理规定（征求意见稿）》公开征求意见的通知：参与算法推荐服务安全评估和监督检查的相关机构和人员应当对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

国外

1、英军指挥官不满游戏数据错误，怒将本国坦克机密泄给外国商家

摘要：《英国国防期刊》称，因不满某游戏中挑战者 2 主战坦克“数据错误”，英国一名游戏玩家将该坦克的机密数据上传至论坛。这名玩家声称自己是英国陆军皇家坦克团一位指挥官，并上传了《陆军装备保障出版物》上的文档截图。他表示，“结构上的复杂度很难从图片上显示出来，我只是想让开发商知道他们错了”。游戏制作公司方面表示，已收到英国国防部的书面确认，称传播该文件违反《官方保密法案》，最高可能面临 14 年监禁。

2、美国 FCC 调查 T-Mobile 美国公司数据泄露事件

摘要：美国 FCC 正在着手调查 T-Mobile 美国公司披露的数据泄露事件。该公司承认有黑客入侵服务器，取得了大量的相关数据。据悉，此次数据泄露事件影响超过 4700 万名客户，包括 780 万名现有用户。被盗的数据包括用户的姓名和出生日期等个人信息。

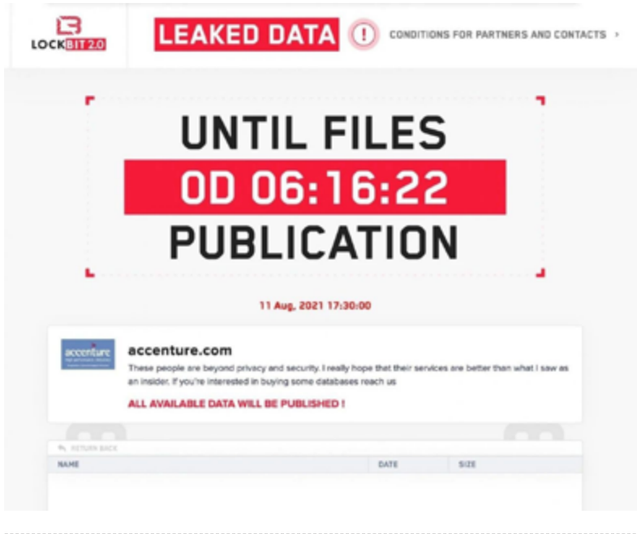
3、超 5 亿 Facebook 用户的数据被泄露，扎克伯格也中招

摘要：一个低级别的黑客论坛 3 日曝光了超过 5.33 亿 Facebook 用户数据，其中包括 3200 多万条美国用户记录，1100 万条英国用户记录和 600 多万条印度用户信息，共涉及到 106 个国家。数据显示，所泄露的信息包括个人账号、用户姓名、位置、生日、电话号码及电子邮件地址等，风险性极高。

4、未采用“零信任”方法的组织数据泄露平均成本高达 504 万美元

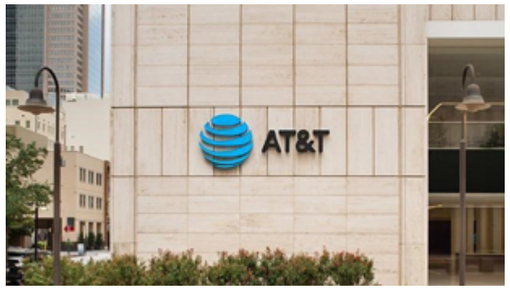
摘要：近日，《2021 年数据泄露成本报告》重磅发布，这份全球性报告已成为网络安全行业中领先的基准报告之一，综合了来自 17 个国家和地区、17 个行业的 537 个组织机构的研究结果，以展示全球平均情况。2020-2021 年间数据泄露的平均总成本增加了 10%：数据泄露成本从 386 万美元上升到 424 万美元，成为本报告有史以来最高的年度平均总成本。

5、埃森哲被黑客攻击，索要 3.2 亿元赎金：6 TB 文件被盗



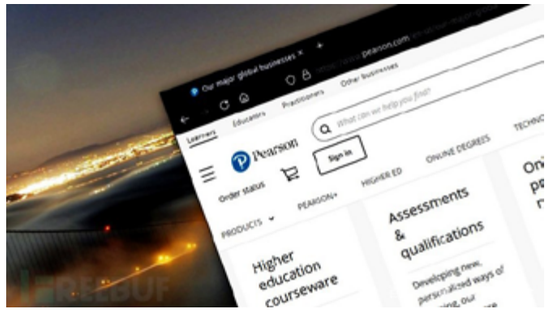
摘要：一个名为 LockBit 2.0 的勒索软件团伙扬言要发布据称在最近的一次网络攻击中从埃森哲窃取而来的文件数据。威胁分子表示，如果受害者没有支付赎金，他们将在今天晚些时候发布数据。虽然 LockBit 没有出示所窃取数据的证据，但他们声称愿意将其出售给任何感兴趣的组织或个人。LockBit 在其数据泄露网站上称：“这些人无视隐私和安全。我确实希望他们的服务比我这个内部人员看到的做得更好。如果你有兴趣购买一些数据库，请联系我们。”

6、黑客拍卖 7000 万用户数据库后 AT&T 否认数据泄露



摘要：在一个知名黑客声称要出售一个包含 7000 万用户个人信息的数据库后，ATT 表示并没有遭遇数据泄露事件。这个被称为 ShinyHunters 的黑客昨天开始在一个黑客论坛上拍卖这个数据库，起价 20 万美元，递增报价 3 万美元。该黑客表示，愿意立即以 100 万美元的价格出售。从该黑客分享的样本来看，该数据库包含客户姓名、地址、电话号码、社会安全号码和出生日期。一位不愿透露姓名的安全研究员表示，样本中的四个人中有两个被证实在 ATT 有账户。除了这几个细节之外，关于这个数据库如何获得，以及它是否是真实的，目前所知不多。

7、英国教育巨头培生因掩盖数据泄露被罚款 100 万美元



摘要：8 月 16 日，美国证券交易委员会 (SEC) 宣布，英国跨国教育出版服务公司培生（Pearson），已就 2018 年数据泄露事件中披露程序处理不当的指控达成了和解。据 SEC 宣布，Pearson 公司同意支付 100 万美元的民事罚款，以解决“不承认或否认调查结果”的指控，该指控试图掩盖和淡化 2018 年发生的数据泄露事件，此次泄露事件导致美国 1.3 万所学校的学生和管理员登录凭证信息泄露。

8、收到“白帽黑客”提醒！福特避免大规模数据泄露

摘要：近日据海外媒体报道称，在今年早些时候有“白帽黑客”提醒了福特其公司系统存在漏洞，该漏洞可能会导致福特的客户和员工记录、财务帐号等敏感信息被曝光。在收到警告后，福特公司在 24 小时内修补了相关问题。福特发言人表示：“根据提供给福特的证据和内部调查，我们认为在这种情况下没有有关员工或客户的任何敏感个人信息遭到泄露”。

9、Raccoon 黑客竟然黑了自己? 数据泄露泛滥，怎么办?

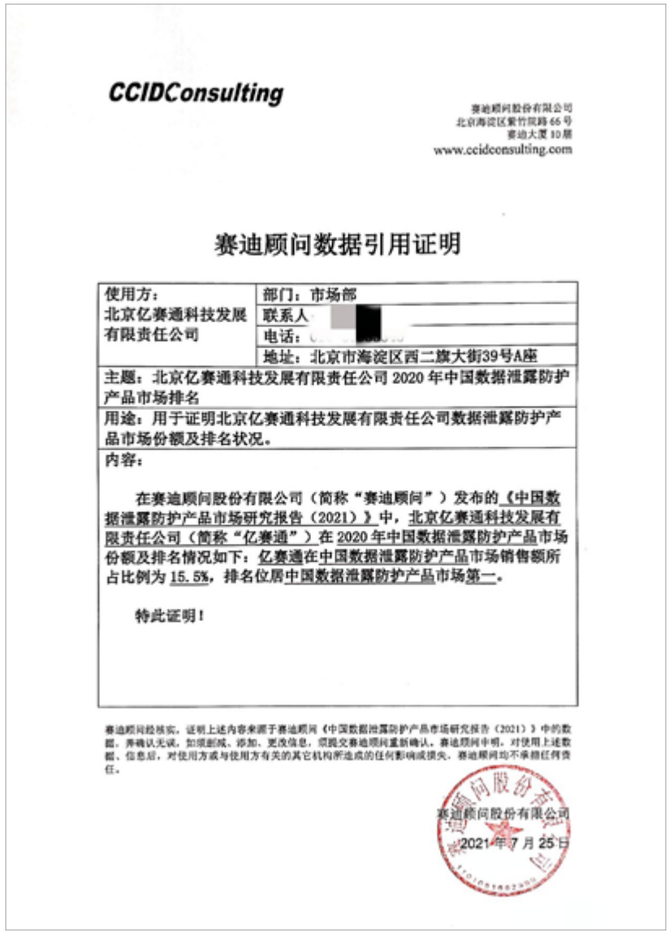
摘要：最近，恶意软件 Raccoon 的开发者测试程序时感染了自己的系统，导致数据通过 C2 服务器泄露到了黑客论坛。Raccoon 是一种信息窃取程序，可以从数十个应用程序中窃取数据。Raccoon 测试计算机中泄露的数据显示了多个电子邮件地址，以及一个名字 Benjamin Engel 等，但这些细节不足以确定开发者的身份。

10、2021 年数据泄露 & 漏洞快速浏览年中报告 - Risk Based Security

摘要：Risk Based Security 发布了两份涵盖 2021 年上半年数据泄露和漏洞的新报告，发现报告的漏洞总数有所下降，但披露的漏洞数量有所增加。该公司的数据泄露报告发现，2021 年前六个月共有 1,767 起公开报告的泄露事件，与去年同期相比下降了 24%。

报告 | 亿赛通再次入选《中国数据泄露防护产品市场研究报告》

近日，中国权威调研机构赛迪顾问 CCID 发布《中国数据泄露防护产品市场研究报告 2021》，根据 CCID 年度报告，亿赛通数据泄露防护产品在中国市场占有率保持明显优势，既意味着广大客户和业界对亿赛通数据泄露防护产品的信赖与肯定，也是对亿赛通在数据泄露防护领域的十多年专项投入和持续创新的认可。



CCIDConsulting

赛迪顾问股份有限公司
北京海淀区紫竹院路 66 号
赛迪大厦 10 层
www.ccidconsulting.com

赛迪顾问数据引用证明

使用方：北京亿赛通科技发展有限责任公司	部门：市场部 联系人 [redacted] 电话：[redacted] 地址：北京市海淀区西二旗大街39号A座
主题：北京亿赛通科技发展有限责任公司 2020 年中国数据泄露防护产品市场排名	
用途：用于证明北京亿赛通科技发展有限责任公司数据泄露防护产品市场份额及排名状况。	
内容： 在赛迪顾问股份有限公司（简称“赛迪顾问”）发布的《中国数据泄露防护产品市场研究报告（2021）》中，北京亿赛通科技发展有限责任公司（简称“亿赛通”）在 2020 年中国数据泄露防护产品市场份额及排名情况如下：亿赛通在中国数据泄露防护产品市场销售额所占比例为 15.5%，排名位居中国数据泄露防护产品市场第一。 特此证明！	

赛迪顾问股份有限公司
2021 年 7 月 25 日

创新决定企业发展

作为中国最早自主研发的数据泄露防护产品的厂商之一，亿赛通凭借丰厚的技术积累，已具备成熟的数据全生命周期能力，融合了机器学习、大数据分析、文档加密、访问控制、关联分析、数据标识等技术，帮助用户对结构化和非结构化数据进行数据治理、安全管控、态势感知，为用户的核心数据资产提供从终端、网络、存储到应用的全生命周期保护，在确保企业敏感数据安全前提下，实现安全与效率的最大平衡；同时在多场景适配上，可以不断满足用户在国产化产品的场景需求，十余年的持续积累下，累计获得数十项发明专利，多项奖项认证，从体系管理到资源投入，从技术创新到新领域开拓，均走在市场前列。

需求决定市场规模增长

CCID 报告显示，2020 年受疫情远程办公、《数据安全法》、“等保 2.0”等政策影响，中国数据泄露防护市场需求量稳步增长，2020 年达到 10.3 亿元，增长率为 8.3%，未来三年，中国数据泄露防护产品市场将保持高速增长速度，预计 2023 年将达到 15.9 亿元，三年的复合增长率为 15.6%。

厂商扩张 激烈竞争

根据 CCID 报告显示，2020 年中国数据泄露防护市场前三名合计占据了 32.5% 的市场份额，而亿赛通在前三名厂商中占据将近 50% 的份额，其背后不仅有有品牌优势的助力，更有技术创新的推动。虽然各大厂商份额较往年有所缩减，但这是由于近两年国家政策引导、国内数据泄露防护市场竞争较为激烈，在各路资本支持下不断涌现的初创公司与纷纷扩张其安全版图的传统安全公司，都在数据泄露防护领域加以布局。

市场前途不可限量面对复杂多变的应用环境，数据泄露防护不但要满足大量合规市场，更需要满足客户的价值需求，品牌优势会助力获得更大的合规市场，技术创新带动行业头部客户的青睐，以此影响合规市场的采购风向。业务场景和问题挑战的愈发多样，数据泄露防护产品也应该和一些新的数据安全技术相结合，例如去标识化数据的合规评估技术、数据匿名化、同态加密等，以期为企业提供更为全面的防护。

荣耀的成绩只是开始，只有让产品更好地服务客户，推动产品的技术进步才是一个产品持续领先的前提。作为数据泄露护领域领导者，亿赛通数据泄露防护产品将深入捕捉各行业业务场景需求，继续在诸多领域积极探索。

未来，亿赛通将继续砥砺初心，坚持自主研发创新，以用户需求为根本，紧密贴合各行业业务场景，为用户提供安全最佳实践，为我国数字经济高质量发展保驾护航。

亿赛通 & 飞腾推出电子文档安全管理联合解决方案，战略合作更进一步

在信息化水平高速发展的今天，从事高新技术研发的企业越来越多，各种研发辅助设计软件、管理软件、协同开发软件等也得到了快速发展以及广泛的应用。由于事企业单位发展以及业务的需要，各类包含大量重要信息的电子资料，如战略规划、源代码、设计图纸、计划书、技术文档等与知识产权相关的数据被高度共享，在事企业单位内部无障碍应用、传输及存储，这些核心数据关系到企事业单位的生存发展以及商业竞争力，一旦泄密，将会造成不可估量的损失。

亿赛通与飞腾融合双方核心产品，推出一套电子文档安全管理联合解决方案。亿赛通的电子文档安全管理系统通过和飞腾芯片进行国产化适配，针对数据安全性、服务器安全加固、平台易用性、系统扩展性等问题，制定完善的满足国内需求的解决方案，在企事业单位内实现数据文档安全，防止重要资源外泄，提高单位数据安全保护能力，保护单位资源和效益，同时不对日常办公、开发产生负面影响，达到安全与效率的平衡。最终实现以“保护核心数据”、“控制核心内容流通”、“规范员工访问行为”为抓手，以“带不走、打不开、读不懂”为控制目标，以平衡效率和安全为原则，基于文件过滤驱动技术实现企事业单位重要数据资产的全生命周期保护，达到合规和安全并行的目标。

图 1 亿赛通电子文档安全管理系统解决方案

此前，亿赛通的电子文档安全管理系统与飞腾旗下的 FT-1500A/4、FT-1500A/16 和 FT-2000/4 三款处理器已完成产品兼容性互认证。

方案详情

亿赛通在飞腾芯片的基础上，构建以文件保护为核心，权限管控为辅助的内网电子文档安全管理解决方案，具体实现如下：

文件保护：对文档进行高强度保护并对使用者透明使用。满足数据安全保护的同时，操作简单，应用方便；

应用灵活：与业务实际情况进行结合、实现对文档灵活的管理。达到“多方适应，技管结合，兼顾现状”的系统应用机制；

外发控制：根据业务需要，对需要与合作伙伴进行交互的外发文件进行特殊处理，在满足企业正常业务运转的情况下，最大限度的保证文件的安全性；

离线办公：充分适应企业离线应用需求，对出差人员提供离线时长限制，保证离线人员可以正常使用受保护的文件，同时防止泄密；

日志审计：提供详细的日志审计功能，对管理人员以及终端用户的操作行为进行详细计录；

系统集成：与用户的 OA、代码管理配置平台以及其它业务系统等进行无缝集成，利用动态文件保护技术实现服务器中的数据存放明文，下载到终端或离线后的文件自动保护，防止终端泄密或扩散；

分布式部署：部署方式灵活多变，采用异地部署统一管理的模式，适应企业网络环境，同时与企业已有 AD 域进行集成认证，实现单点登录。

方案实施效果

图 2 亿赛通电子文档安全管理系统实施部署图

系统通过智能动态文件保护技术，对国产终端文件进行强制保护处理，从文件创建开始即可自动保护，不同部门可按需进行，在保障用户核心数据安全情况下，兼容文档交互效率。通过对核心数据进行全生命周期保护，确保核心数据只可在企事业全域内正常、透明使用，通过任意方式将数据非法带离内部环境将无法正常使用。

配合内容安全管控，实现敏感数据文档的拷贝、粘贴、另存、内容拖拽等行为的控制，管控用户操作文件行为规范，对用户的文件操作行为进行审计记录，保障后期追溯能力。

关于亿赛通

北京亿赛通科技发展有限责任公司（以下简称“亿赛通”）成立于 2003 年，是绿盟科技（证券代码：300369）全资子公司。亿赛通作为国内数据安全行业的供应商，是一个拥有完全自主知识产权的高科技软件企业，并已取得“高新技术企业证书”、“涉密信息系统产品检测证书”、“军用信息安全产品认证证书”、“商用密码生产定点单位证书”等多项资质认定，连续多年获得 CCID 赛迪专业机构的高度认可。近二十年风雨兼程，成功打造为专业的数据安全、网络安全及安全服务三大业务的综合服务商。作为国内极具实力的、完全拥有自主知识产权的安全厂商，拥有签约用户过万家、600 余万终端用户，打造了亿赛通坚不可摧的品牌影响力。

关于飞腾

飞腾公司是国内领先的自主核心芯片提供商，致力于飞腾系列国产高性能、低功耗通用计算微处理器的设计研发和产业化推广，坚持 “核心技术自主创新，产业生态开放联合” 的发展理念，联合众多国产软硬件生态厂商，提供基于国际主流技术标准、中国自主先进的全国产信息系统整体解决方案，支撑国家信息安全和重要工业安全。

基于飞腾 CPU 的整机产品覆盖多种类型的终端（台式机、一体机、便携机、瘦客户机等）、服务器和工业控制嵌入式产品等，在国内政务办公、云计算、大数据以及金融、能源和轨道交通等行业信息系统领域已实现批量应用。

深度研究 | 隐私计算：大数据安全下的“矛”与“盾”

伴随着云计算、大数据、人工智能等新一代信息技术的落地应用，数据已成为一种基础型和战略型资源，深刻改变着全球社会的发展模式。2020 年 4 月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，将数据同土地、劳动力、资本、技术等传统生产要素并列，作为一种新型生产要素参与分配。数据要素价值的释放是通过数据资源的开放与共享、流通与交换来实现的。

全球数据量呈现指数性增长态势，但从现阶段数据的从属来看，海量数据散落于不同的组织机构和信息系统中，即使是同一区域、产业和企业，仍存在“数据孤岛”问题。多方数据协作已经成为医疗、金融、政务等领域挖掘数据价值的重要路径，聚合多方数据进行多方计算和联合建模分析是当下释放大数据价值的必然选择。但近年来数据安全事件频发，数据安全需求日益增加。《中华人民共和国数据安全法》的颁布和实施，对数据安全合规也提出了更高的要求。既要通过数据的开放与共享、流通与交换来发挥数据价值，又要保护数据安全，是当前需要解决的重要课题。在此背景下，隐私计算应运而生，以安全多方计算、联邦学习、可信执行环境等为代表的隐私计算技术为上述课题提供了解决方案。隐私计算在数据共享过程中实现数据价值挖掘与隐私保护之间的平衡，为数据确权、数据价值化、数据要素市场的发展奠定了基础。

Gartner 发布的 2021 年前沿科技战略趋势中，将隐私计算列为未来几年科技发展的九大趋势之一。隐私计算是面向隐私信息全生命周期的计算理论和方法，是隐私信息的所有权、管理权和使用权分离的前提下，面向隐私度量、隐私保护与隐私分析复杂性的可计算模型与公理化系统。隐私计算是指在保证数据提供方不泄露原始数据和保护隐私的前提下，实现数据分析计算的一系列技术，它是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。隐私计算真正做到了数据的“可用不可见”，既实现了数据价值的流通与共享，又实现了数据的隐私保护。“可用不可见”是隐私计算的精髓所在，其核心有两层含义：数据的可用性和数据的不可见性，即在充分保护数据和隐私安全的前提下，实现大数据价值的转化和提炼。

近几年来，各大互联网巨头、数据服务商、初创企业都纷纷布局隐私计算领域，推出各自的隐私计算产品。自 2003 年创立以来，亿赛通一直坚守数据安全作为公司的生命线，以数据安全为核心，从多个维度投入大量资源打造数据安全产品体系，我们认为，在隐私计算的技术体系中（如下图所示），目前主流隐私计算技术主要有三大方向：一是以安全多方计算为代表的基于密码学的隐私计算技术；二是以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术，联邦学习作为分布式机器学习框架主要面向的是联合建模的场景；三是以可信执行环境为代表的基于可信硬件的隐私计算技术。同态加密、差分隐私、秘密分享、不经意传输、混淆电路、零知识证明等基础密码技术，为上层的安全多方计算、联邦学习、可信计算等提供了密码学原语算法。不同技术组合使用，完成对数据的隐私计算。

我国在隐私计算方面布局较晚，在 2016 年后才开始出现独立的隐私计算商业项目，但国内产业化发展的速度较快。当前隐私计算应用主要集中在数据驱动的金融、互联网领域和拥有大量数据源和数据流通需求的医疗、运营商、政务等领域。从技术路线看，安全多方计算的复杂度高、开发难度大，龙头企业多致力于此，力图打造以安全多方计算为底座的数据流通基础设施。作为数据安全行业的重量级企业，亿赛通一直关注隐私计算技术的发展，在隐私计算的理论和产品研发层面积极探索，在同态加密、差分隐私、秘密分享、安全多方计算等方面的研究成果，已与公司现有数据安全和网络产品有机融合，可为用户解决数据流通、实现数据要素价值提供更高质量的解决方案。

作为解决数据共享流通、实现数据价值的关键突破口，隐私计算技术未来的发展前景空间广阔。从技术角度看，隐私计算正呈现出如下趋势，如软硬件协同提升隐私计算性能、向大规模分布式应用、与大数据平台设施的进一步整合、与区块链结合构建完整解决方案等。

随着大数据和人工智能的发展和应用的不断深入，市场各方对跨组织、跨地域、跨行业的数据共享流通需求日益增大，隐私计算在金融、医疗、政务、运营商等场景开展了应用实验。然而隐私计算要实现大规模的落地应用还尚需时日，亿赛通愿与用户一起为隐私计算在性能、技术融合、安全等方面的进一步提升共同努力。

政策 | 划重点，《关键信息基础设施安全保护条例》9 月 1 日正式实施

关键信息基础设施涉及国家安全和人民生产生活，是国之重器，历来是安全保障重中之重。8 月 17 日公布的《关键信息基础设施安全保护条例》（以下简称《条例》）是贯彻落实《网络安全法》的重要举措。围绕如何统筹设计关键信息基础设施保护工作，如何有效完善、落实《关键信息基础设施安全保护条例》，亿赛通专家积极发表观点，贡献智慧。

第一章 总则

第一条 为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条 本条例所称关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

本《条例》明确关键信息基础设施范围和保护工作原则目标。是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域。

第三条 在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

本《条例》明确监督管理体制，对国家、政府、监管部门、行业主管或监管部门、公安机关部门等核心部门确立了统筹协作、分工负责的监管机制。国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。

第四条 关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者 (以下简称运营者) 主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

第五条 国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

本《条例》明确要求对重点行业和领域的重要网络设施、信息系统属于关键信息基础设施，国家对关键信息基础设施要实行重点保护。

第六条 运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

第七条 对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

第二章 关键信息基础设施认定

第八条 本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门 (以下简称保护工作部门)。

第九条 保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

(一) 网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

(二) 网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

(三) 对其他行业和领域的关联性影响。

第十条 保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

第十一条 关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起 3 个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

本《条例》明确认定工作的组织方式和认定程序，依照行业认定规则，国家汇总并动态调整关键信息基础设施认定结果，确保重要网络设施、信息系统纳入保护范围。

第三章 运营者责任义务

第十二条 安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

第十三条 运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

第十四条 运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

第十五条 专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

(一) 建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；

(二) 组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

(三) 按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

(四) 认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

(五) 组织网络安全教育、培训；

(六) 履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

(七) 对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

(八) 按照规定报告网络安全事件和重要事项。

第十六条 运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

第十七条 运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

第十八条 关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故

障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

第十九条 运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第二十条 运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十一条 运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

本《条例》规定运营者主要负责人是本单位运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责组织落实、全面负责网络安全工作。具体职责范围包括组织制定网络安全教育和培训、规章制度、操作规程，实施开展网络安全检查和应急演练以及处置网络安全事件，向有关部门报告网络安全重要事项。

亿赛通凭借近二十年的数据安全建设方法论 + 全行业的实施经验，深入了解数据使用业务场景，基于整体数据安全防护规划，进行防护目标的差异化分析，以“数据安全流转为中心”，为用户建立综合专业的数据安全治理体系，并科学制定数据分类分级保护方法与标准，深化数据安全风险评估与监管流程，提供最新最全面的安全服务，最终实现数据安全防护价值。

第四章 保障和促进

第二十二条 保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

第二十三条 国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

第二十四条 保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

第二十五条 保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

第二十六条 保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

第二十七条 国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

第二十八条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

第二十九条 在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

第三十条 网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

第三十一条 未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

第三十二条 国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。

第三十三条 公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。

第三十四条 国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

第三十五条 国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

第三十六条 国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

第三十七条 国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

第三十八条 国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

本《条例》明确了保障和促进措施，对制定行业安全保护规划、建立信息共享机制、建立健全监测预警制度、明确网络安全事件应急处置要求、组织安全检查检测、提供技术支持和协助等作了规定。

亿赛通数据安全态势感知平台产品采用先进的大数据技术架构，通过采集分析来自于终端、网络、存储、结构化和非结构化的各类安全设备日志，通过人工智能算法，以人员和终端行为分析为主线，探测发现威胁企业的数据安全事件，并提供完整追溯取证证据链，全面保障客户数据安全。同时能将各个孤立的安全系统进行资源整合，达到数据集中和关联分析以揭示事件背后隐藏的逻辑关系从而全面监控数据安全状况，指导企业安全管理，有效预防、阻断或减少安全威胁事件的发生。

第五章 法律责任

第三十九条 运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款：

（一）在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

（二）安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

（六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

（七）专门安全管理机构未履行本条例第十五条规定的职责的；

（八）未对关键信息基础设施每年至少进行一次网络安全

检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

（九）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

（十）发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

第四十条 运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。

第四十一条 运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额 1 倍以上 10 倍以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第四十二条 运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节严重的，依法追究相应法律责任。

第四十三条 实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处 5 日以下拘留，可以并处 5 万元以上 50 万元以下罚款；情节较重的，处 5 日以上 15 日以下拘留，可以并处 10 万元以上 100 万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处 10 万元以上 100 万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5 年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第四十四条 网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十五条 公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十六条 网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第四十七条 关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第四十八条 电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

第四十九条 违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

本《条例》明确了法律责任，对关键信息基础设施运营者未履行安全保护主体责任、有关主管部门以及工作人员未能依法依规履行职责等情况，明确了处罚、处分、追究刑事责任等处理措施。对实施非法侵入、干扰、破坏关键信息基础设施，危害其安全活动的组织和个人，依法予以处罚。

第六章 附则

第五十条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

第五十一条 本条例自 2021 年 9 月 1 日起施行。

政策法规 | 《党委（党组）网络安全工作责任制实施办法》亮点解析，安全产业迎来新机遇

本月，《人民日报》头版发布《中国共产党党内法规体系》一文。与此同时，《中国共产党党内法规汇编》由法律出版社公开出版发行，该书正式解密公开了《党委（党组）网络安全工作责任制实施办法》（以下简称“《实施办法》”）。

《实施办法》作为《中国共产党党内法规体系》唯一收录的网络安全领域的党内法规，它的公开发布将对厘清网络安全责任、落实保障措施、推动网信事业发展产生巨大影响。《实施办法》从责任主体、责任范围、责任事项、问责主体、启动问责的条件、问责措施等角度对网络安全工作责任制进行了明确定义。

《实施办法》明确了责任主体

各级党委（党组）：各地区各部门各级党政机关、关键信息基础设施运营单位、重要数据和个人信息的处理者等单位的党委（党组）是网络安全工作的责任主体。《实施办法》第二条规定:“按照谁主管谁负责、属地管理的原则，各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。”此条规定明确了从中央到地方和基层的政府机关、企事业单位、人民团体中各级党委和党组，是网络安全工作的责任主体，并且进一步明确了领导班子主要负责人和相关领导班子成员的责任。

《实施办法》本身就是党内法规，体现了以习近平为核心的党中央对网络安全与数据安全工作的重视程度。

各级（各地区各部门）网络安全和信息化领导机构:《实施办法》第五条、第六条分别规定，各级（各地区各部门）网络安全和信息化领导机构具有分析研判网络安全信息、统筹协调网络安全检查、组织通报网络安全信息等职责。

行业主管监管部门：《实施办法》第四条规定：“行业主管监管部门对本行业本领域的网络安全负指导监管责任。没有主管监管部门的，由所在地区负指导监管责任。”

《实施办法》明确规定了四项网络安全责任和需要追责的七项网络安全情形，为重大网络安全事件追责提供了具体依据。

《实施办法》明确了责任范围

《实施办法》所划定的责任主体，具有各自不尽相同的责任范围，形成一张相互交织、没有死角的网络安全责任网络，严密覆盖每一个行业和领域、地区、关键信息基础设施运营单位、党政机关。

- **行业和领域：**按照《实施办法》第四条，本行业本领域的网络安全检查、事件处置，由主管监管部门负责指导监管。没有主管监管部门的行业，由所在地区负指导监管责任。电信、能源、金融等行业的网络安全工作，由相关主管监管部门负责；少数没有主管监管部门的行业、领域，由所在地区网信领导机构负责。

亿赛通针对电信、能源、金融等十大行业凭借专业的技术和丰富的解决方案，为每一位客户提供及时、全面、到位的优质服务。

- **地区：**按照《实施办法》第五条，本地区的网络安全事件汇集、分析研判、组织指导信息通报、统筹协调网络安全检查等工作，由本地区的网信领导机构负责。

亿赛通已在全国三十余个城市设立了分支机构，覆盖全国的营销及服务战略性布局基本完成。

- **关键信息基础设施运营单位：**关键信息基础设施运营单位网络安全工作，由本单位的党委（党组）负主体责任，由相关行业主管监管部门负指导监管责任，没有主管监管部门的，由所在地区网信领导机构负指导监管责任。

- **党政机关：**按照《实施办法》第三条，党政机关本单位的网络安全工作，由本单位党委（党组）负主体责任。

另外，《实施办法》第四条还对可能出现的交叉重叠责任进行了划分协调：“各地区开展网络安全检查、处置网络安全事件时，涉及重要行业的，应当会同相关主管监管部门进行。"

《实施办法》明确了国家重要基础数据以及个人信息数据应作为关键敏感数据保护，为数据安全厂商指明了数据保护的重要方向。

《实施办法》明确了责任事项

1、各级党委（党组）

1）认真贯彻落实党中央和习近平总书记关于网络安全工作的重要指示精神和决策部署，贯彻落实网络安全法律法规，明确本地区本部门网络安全的主要目标、基本要求、工作任务、保护措施；

2）建立和落实网络安全责任制，把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力的支持和保障力度；

3）统一组织领导本地区本部门网络安全保护和重大事件处置工作，研究解决重要问题；

4）采取有效措施，为公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动提供支持和保障；

5）组织开展经常性网络安全宣传教育，采取多种方式培养网络安全人才，支持网络安全技术产业发展。

2、行业主管监管部门：

《实施办法》第四条规定，行业主管监管部门对本行业本领域的网络安全负指导监管责任。没有主管监管部门的，由所在地区负指导监管责任。

主管监管部门应当依法开展网络安全检查、处置网络安全事件，并及时将情况通报网络和信息系统所在地区网络安全和信息化领导机构。各地区开展网络安全检查、处置网络安全事件时，涉及重要行业的，应当会同相关主管监管部门进行。

3、各级（各地区各部门）网络安全和信息化领导机构：

- 各级网络安全和信息化领导机构应当加强和规范本地区本部门网络安全信息汇集、分析和研判工作，要求有关单位和机构及时报告网络安全信息，组织指导网络安全通报机构开展网络安全信息通报，统筹协调开展网络安全检查。

- 各地区各部门网络安全和信息化领导机构应当向中央网络安全和信息化委员会及时报告网络安全重大事项，包括出台涉及网络安全的重要政策和制度措施等。

- 各地区各部门网络安全和信息化领导机构每年向中央网络安全和信息化委员会报告网络安全工作情况。

《实施办法》明确了网络安全责任范围，为事后追责提供重要依据。亿赛通可实现覆盖数据全生命周期全时域和网络端管云的全空域的立体防护，利用数据安全透视实现数据资产发现、数据识别、数据标签和数据分类分级，描绘数据资产及分布和数据风险评估，通过统一策略、统一流程、统一管理和统一接口实现数据安全的智能管控。

《实施办法》明确了问责条件

《实施办法》将启动问责的条件按行为及后果分为两类。

1、按行为问责：各级党委（党组）违反或者未能正确履行本办法所列职责，按照有关规定追究其相关责任。按此规定，责任主体若未履行本办法所列职责，有违反本办法的不作为或乱作为行为，则按有关规定追究相关责任。

2、按后果问责: “有下列情形之一的，各级党委（党组）应当逐级倒查，追究当事人、网络安全负责人直至主要负责人责任。协调监管不力的，还应当追究综合协调或监管部门负责人责任。

• 党政机关门户网站、重点新闻网站、大型网络平台被攻击篡改，导致反动言论或者谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

• 地市级以上党政门户网站或者重点新闻网站受到攻击后没有及时组织处置，且瘫痪 6 小时以上的；

• 发生国家秘密泄露、大面积个人信息泄露或者大量地理、人口、资源等国家基础数据泄露的；

• 关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

• 封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的；

• 阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

• 发生其他严重危害网络安全行为的。”

只要触犯上述情况均可启动问责程序。前者确认了主体在进行网络安全工作责任时不作为或乱作为行为的情况，后者确认了主体因后果及负面影响的情况。这两种情况履职尽责不到位必然导致产生严重后果。

《实施办法》明确了工作保障

1、表彰奖励措施。《实施办法》第七条规定：中央网络安全和信息化委员会办公室会同有关部门按照国家有关规定对网络安全先进集体予以表彰，对网络安全先进工作者予以表彰奖励。

2、干部考核措施。《实施办法》第十条规定: 各级党委（党组）应当建立网络安全责任制检查考核制度，完善健全考核机制，明确考核内容、方法、程序，考核结果送干部主管部门，作为对领导班子和有关领导干部综合考核评价的重要内容。

3、审计保障措施。《实施办法》第十一条规定：各级审计机关在有关部门和单位的审计中，应当将网络安全建设和绩效纳入审计范围。

《实施办法》明确网络安全纳入审计范围，不仅将网络安全与主要负责人关联，同时也将单位所有人纳入进来，统一思想和认识，全员关注和参与，可大大促进网络安全和数据安全建设工作的开展。

近年来，我国陆续出台了《中华人民共和国网络安全法》、《中华人民共和国密码法》、《关键基础设施保护条例》等多网络安全法律条文及规范性文件。

本次《党委（党组）网络安全工作责任制实施办法》的正式公布，明确了各级网络安全工作的责任，推进网络安全各项工作任务的落实，对提高国家网络安全防护能力、促进国内网络安全产业链的发展具有重要意义。

文章《实施办法》内容来源于互联网

亿赛通小贴士 ESAFENET PROMPT

政策 |《个人信息保护法》8 章 74 条，正式开启反杀熟大幕

2021 年 8 月 20 日，备受关注的《个人信息保护法》经过三次审议，在十三届全国人大常委会第三十次会议表决通过。个人信息保护法共 8 章 74 条。在有关法律的基础上，进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。

第一章 总则

第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：

• 以向境内自然人提供产品或者服务为目的；

• 分析、评估境内自然人的行为；

• 法律、行政法规规定的其他情形。

本法将符合条件的境外机构纳入管辖范围内，某些向境内自然人提供产品或服务，但却登记在海外的公司，一旦违法，也需要接受中国的处置。

第四条 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。

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。

明确了个人信息的定义，并明确了个人信息处理全过程。

第五条 处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条 处理个人信息应当具有明确、合理的目的，并应当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，应当限于实现处理目的的最小范围，不得过度收集个人信息。

第七条 处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。

第十条 任何组织、个人不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信

息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等互认。

确立了个人信息处理应遵循的原则，强调处理个人信息应当采用合法、正当的方式，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。

第二章 个人信息处理规则

第一节 一般规定

第十三条 符合下列情形之一的，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。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。

第十五条 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

处理个人信息应遵循“告知 - 同意”原则，在实现充分告知的前提下取得个人同意。用户对自己的个人信息应用状态，从头到尾都必须享有知情权和决定权。

第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：

• 个人信息处理者的名称或者姓名和联系方式；

• 个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

• 个人行使本法规定权利的方式和程序；

• 法律、行政法规规定应当告知的其他事项。

前款规定事项发生变更的，应当将变更部分告知个人。

个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。

第十八条 个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后及时告知。

第十九条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现处理目的所必要的最短时间。

第二十条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。

个人信息处理者共同处理个人信息，侵害个人信息权益造成损害的，应当依法承担连带责任。

第二十一条 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。

受托人应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息；委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

未经个人信息处理者同意，受托人不得转委托他人处理个人信息。

第二十二条 个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的，应当向个人告知接收方的名称或者姓名和联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十三条 个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。

第二十四条 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。

通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十五条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

第二十六条 在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

第二十七条 个人信息处理者可以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；个人明确拒绝的除外。个人信息处理者处理已公开的个人信息，对个人权益有重大影响的，应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十八条 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。

只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

第二十九条 处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第三十条 个人信息处理者处理敏感个人信息的，除本法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。

本法更严格限制处理敏感个人信息，若需处理敏感个人信息，需要提前向个人告知处理敏感个人信息的必要性和对个人权益的影响，并在有严格保护措施的条件下进行。

第三十一条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

个人信息处理者处理不满十四周岁未成年人个人信息的，应当制定专门的个人信息处理规则。

特别提到了对 14 岁以下未成年人实行更为严苛的信息保护，这是立法者对未成年人的特别保护。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定履行告知义务；有本法第十八条第一款规定的情形，或者告知将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：

- 依照本法第四十条的规定通过国家网信部门组织的安全评估；
- 按照国家网信部门的规定经专业机构进行个人信息保护认证；
- 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；
- 法律、行政法规或者国家网信部门规定的其他条件。

中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

第三十九条 个人信息处理者向中华人民共和国境外提供个人信息的，应当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，并取得个人的单独同意。

第四十条 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。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。

第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。

第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

对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应当将在中国境内收集和产生的个人信息存储在境内，若向境外提供的，应通过安全评估；而对于其他个人信息处理者，应满足《个人信息保护法》第 38 条规定的四种条件之一，才可向境外提供个人信息。另外，非经主管机关批准，不得向外国司法或者执法机构提供存储于境内的个人信息。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。

第四十五条 个人有权向个人信息处理者查阅、复制其个人信息；有本法第十八条第一款、第三十五条规定情形的除外。

个人请求查阅、复制其个人信息的，个人信息处理者应当及时提供。

个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

- 处理目的已实现、无法实现或者为实现处理目的不再必要；
- 个人信息处理者停止提供产品或者服务，或者保存期限已届满；
- 个人撤回同意；
- 个人信息处理者违反法律、行政法规或者违反约定处理个人信息；
- 法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条 自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。

第五十条 个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的，应当说明理由。

个人信息处理者拒绝个人行使权利的请求的，个人可以依法向人民法院提起诉讼。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

- 制定内部管理制度和操作规程；
- 对个人信息实行分类管理；
- 采取相应的加密、去标识化等安全技术措施；
- 合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；
- 制定并组织实施个人信息安全事件应急预案；
- 法律、行政法规规定的其他措施。

第五十二条 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指定个人信息保护负责人，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。

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。

第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第五十五条 有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

- 处理敏感个人信息；
- 利用个人信息进行自动化决策；
- 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；
- 向境外提供个人信息；
- 其他对个人权益有重大影响的个人信息处理活动。

第五十六条 个人信息保护影响评估应当包括下列内容：

- 个人信息的处理目的、处理方式等是否合法、正当、必要；
- 对个人权益的影响及安全风险；
- 所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年。

第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

- 发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
- 个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；
- 个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

第五十八条 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，应当履行下列义务：

按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；

遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务；

对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；

定期发布个人信息保护社会责任报告，接受社会监督。

第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。

规范了应用程序过度收集个人信息、大数据杀熟及非法买卖、泄露个人信息等情况。

第六章 履行个人信息保护职责的部门

第六十条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十一条 履行个人信息保护职责的部门履行下列个人信息保护职责：

- 开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；
- 接受、处理与个人信息保护有关的投诉、举报；
- 组织对应用程序等个人信息保护情况进行测评，并公布测评结果；
- 调查、处理违法个人信息处理活动；
- 法律、行政法规规定的其他职责。

第六十二条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

- 制定个人信息保护具体规则、标准；
- 针对小型个人信息处理者、处理敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；
- 支持研究开发和推广应用安全、方便的电子身份认证技术，推进网络身份认证公共服务建设；
- 推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务；
- 完善个人信息保护投诉、举报工作机制。

第六十三条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

- 询问有关当事人，调查与个人信息处理活动有关的情况；
- 查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；
- 实施现场检查，对涉嫌违法的个人信息处理活动进行调查；
- 检查与个人信息处理活动有关的设备、物品；对有证据证明是用于违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十四条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

履行个人信息保护职责的部门在履行职责中，发现违法处理个人信息涉嫌犯罪的，应当及时移送公安机关依法处理。

第六十五条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

对个人信息处理活动中个人的各项权利进行了明确，包括知情权、决定权、查询权、更正权、删除权等，并要求个人信息处理者建立个人行使权利的申请受理和处理机制。

明确了个人信息处理者的合规管理和保障个人信息安全等义务，要求其按照规定制定内部管理制度和操作规程，采取相应的安全技术措施，并指定负责人对其个人信息处理活动进行监督；

根据个人信息保护工作实际，明确国家网信部门负责个人信息保护工作的统筹协调，发挥其统筹协调作用。同时规定，国家网信部门和国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作。

第七章 法律责任

第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

第六十七条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十八条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

履行个人信息保护职责的部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六十九条 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。

前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

若出现涉及个人信息侵权的纠纷，如果数据处理者不能证明自己没过错，那么，就必须承担赔偿损害责任。

第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十一条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章 附则

第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

第七十三条 本法下列用语的含义：

• 个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

• 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。

• 去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

• 匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

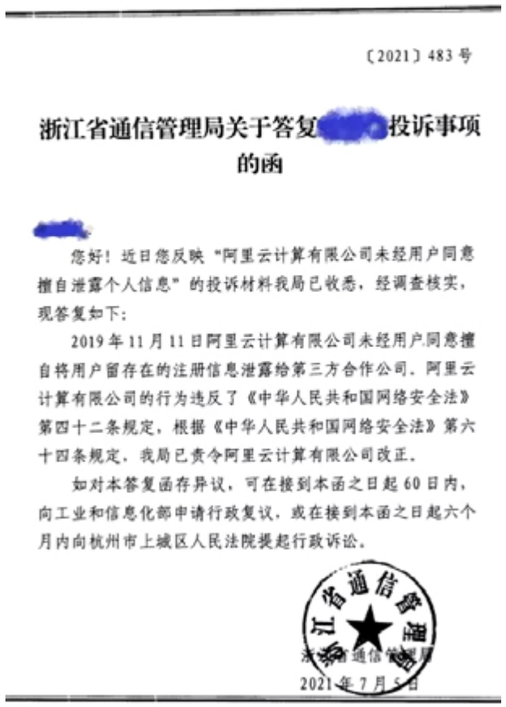
第七十四条 本法自 2021 年 11 月 1 日起施行。

此次《个人信息保护法》针对互联网中的各类个人信息数据问题给出了更明确、更清晰的解决办法，进一步加强了个人信息保护法制保障的客观要求。在其正式实施后，对信息安全将带来巨大改变。

亿赛通小贴士 ESAFENET PROMPT

实锤！阿里云数据泄露，与其亡羊补牢，不如断其根源

近期，阿里云被曝在 2019 年双 11 前后，一名电销员工违反公司纪律，利用工作便利私下获取客户联系方式，并透露给分销商员工，从而引发一名客户投诉。



浙江省通信管理局

〔2021〕483 号

浙江省通信管理局关于答复[redacted]投诉事项的函

[redacted]

您好！近日您反映“阿里云计算有限公司未经用户同意擅自泄露个人信息”的投诉材料我局已收悉，经调查核实，现答复如下：

2019 年 11 月 11 日阿里云计算有限公司未经用户同意擅自将用户留存在的注册信息泄露给第三方合作公司。阿里云计算有限公司的行为违反了《中华人民共和国网络安全法》第四十二条规定，根据《中华人民共和国网络安全法》第六十四条规定，我局已责令阿里云计算有限公司改正。

如对本答复函存异议，可在接到本函之日起 60 日内，向工业和信息化部申请行政复议，或在接到本函之日起六个月内向杭州市上城区人民法院提起行政诉讼。

浙江省通信管理局

2021 年 7 月 5 日

阿里云 V

8月23日 16:20 来自 微博 weibo.com

据自查，该投诉事件成为阿里云一电销员工违反公司纪律，利用工作便利私下获取客户联系方式，并透露给分销商员工，引发一名客户投诉。阿里云严禁员工向第三方泄露用户注册信息，已根据公司制度进行严肃处理，并遵照浙江省通信管理局要求积极整改，对人员管理层面上的不足进行改进。感谢大家的监督批评。

针对泄露问题，阿里云快速做出回应称：已根据公司制度对该事件进行严肃处理，并遵照浙江省通信管理局要求积极整改。

如果阿里云的回应属实，该涉事员工已经涉嫌侵犯公民个人信息罪。根据《刑法》第二百五十三条规定：侵犯公民个人信息罪是指违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

阿里云在强调本次事件是“个别员工违规操作”的同时，一些质疑的声音也随之出现：普通员工的权限也这么高吗？一个员工就可以轻易泄露用户信息，这么大公司管理漏洞怎么这么多？自己的用户信息都保护不了，我们放到阿里云的数据能安全吗？网友们对阿里云用户隐私保护感到失望。

不管怎样，这次事件再次暴露了，用户对上云的最大担心——数据安全。

在上云过程中阿里云是众多企业的选择，那么，阿里云是否对得起用户的信任和买单呢？对于用户而言，阿里云品牌有保障，工作流程已然可以说规范，并且符合大多数企业需求，但是这样的大品牌仍然会发生“疏忽”，并且不止一次，不论是客户隐私，还是研发代码，都应好好保护，才对得起客户和公司老板的殷切期望。

另一方面，近年来，云厂商确实经常出现数据泄露的情况，从阿里云托管平台权限设置问题，到函数计算挂掉，直接导致国内半个互联网瘫痪，以及腾讯云因为运营商光缆中断而宕机 ..... 企业是否上云，上云后的安全如何保障？成为首要解决的问题。

亿赛通在经过近二十年的技术钻研中，独家设计研发出“分放管服”数据安全建设理念。

- “分”为分层治理，制度先行，技术支撑；即需要从制度层和技术层两个维度进行分层治理；
- “放”代表在制度层面放开，使用合理的审批流程规范数据的申请及使用，明确职责后将管理放开，进行行为监察将使用放开，让数据在流转和应用中产生价值；
- “管”代表技术监管：是将数据分类分级、流程规范等管理制度落地的具体技术落地，通过端点边界、网络边界及云边界的纵深防控，形成点到面的全面技术防控。
- “服”就是数据安全高效服务，在提升生产力的同时也产生了大量的数据资产，这些资产的防护不能再按照传统的数据防护堆积设备或工具就能完成相关防护，更是需要营造及时管理环境，立体运营可持续提升数据资产的防护能力才能在新的信息化产业升级的浪潮中站稳脚跟。这就需要高效的人机结合服务来实现目标。

在这个将一切隐私数据化的时代如何保护自己的隐私成了所有人的头等大事，对用户而言，能做的也就是在使用网络服务的时候加强自我保护意识，谨慎填写个人信息，拒绝一些不必要的权限申请……

而对于企业而言，不能知法犯法，特别是大企业，更要成为引领行业的楷模，如何做好保护用户隐私这件事，还需要多多监督才是！

文章资讯来源于互联网

如何做好外包呼叫中心“关键行为”管理?

售前技术部：蒋李 / 文

呼叫中心是连接企业和企业用户之间的纽带和桥梁，是企业对外服务的窗口部门。它使相关信息能够快速地在企业和用户之间传递，能够为企业的发展提供有力的服务保障，是形成企业品牌、建立企业对外形象的坚实基础。而外包呼叫中心则是指客户方将自身的呼叫相关业务外包给第三方呼叫业务提供商，承接客服、电话营销、不良资产催收、问卷调查等业务的服务公司，属于人口密集型企业，业务来源主要有运营商、政府单位、银行、保险、互联网公司等。

随着《数据安全法》的正式颁布并在 9 月 1 日正式实行，外包呼叫中心这种第三方能够直接接触大量客户敏感信息的服务公司也必将进入纳入到《数据安全法》重点监控的范围之内，外包呼叫中心也可以明显感觉到近年来各行业甲方对外包呼叫中心信息安全的要求越来越严格，甚至是作为招投标重点考核项进行考察，那么外包呼叫中心该如何去建立属于自己的信息安全防线，降低因信息安全事件导致的经济损失，规避因信息安全事件带来的法律风险。在甲方没有任何信息安全项要求的基础上建立自己的安全底线，在此底线之上附加甲方客户的信息安全，确保敏感数据万无一失。

那么如何建立信息安全防护基线？可以参考 ISO27001 标准进行建设，结合呼叫中心实际业务情况，分布从访问控制、物理环境、主机安全、网络安全、服务器安全、数据安全等维度进行。

访问控制

访问控制分为物理环境访问控制和信息系统访问控制；物理环境访问控制即外来访客进入公司环境，需要进行登记，发放访客标识工牌并有对接人进行接待，不再此次预约访问区域禁止进入，公司核心区域没有审批禁止进入，限定访问区域；信息系统访问控制是设置信息系统访问权限，杜绝越权访问。

内部员工同样需要进行物理区域的访问控制，杜绝越权访问，同时特殊项目应禁止电子设备的带入如手机、u 盘、相机等，保障信息安全

物理环境

物理环境包含公司物理生产环境、电力生产环境、机房生产环境。公司环境大致可分为项目生产区、后台支撑区、核心信息机房、公共区，这些区域都需要进行门禁隔离，并设置相关区域的门禁访问隔离，做到项目生产分区隔离。防止项目人员间交叉导致的信息泄漏，同时物理环境需安装无死角视频监控系统，监控生产画面及员工异常行为，视频监控厂商推荐：海康威视、大华。

电力生产环境需要考虑用电故障响应，建议在物理职场建设初期就需要进行考虑，有限选择双市电接入，选择办公场地可纳入考虑范围；另一种为 USP 供电，一般要求支撑 2 小时的供电，并可进行发电机接入（发电机及 UPS 为可选项，一般运营商级别的项目需要配备），UPS 厂商推荐山特、科士达、先控等。

主机安全

电脑主机应设置锁屏密码，建议三分钟无操作进行锁屏，并开启弱密码校验；设置统一的项目软件安装套件，让软件受控；设置主机系统操作权限采用 AD 域等方式现在普通员工操作权限，主机安装杀毒软件防止病毒带来的经济损失；物理端口需进行封禁如 USB、串口、蓝牙、火线等等；目前大多数外包中心仅做到了使用注册表进行 USB 封禁，存在敏感信息通过物理端口泄密的风险，杀毒软件厂商推荐火绒、天擎。

网络安全

由于外包呼叫中心不属于关键基础设施单位故无需根据根据等保来进行网络安全防护，但可作为参考建设，基础网络防护应做到在网络边界部署网络防火墙抵御外来攻击；内网部署网络行为管理设备，限制访问其他非法网站造成带宽损耗，同时可监督员工网络行为有利于提高生产力；同时做好网络分区，一般以逻辑隔离为主，不同项目间 vlan 划分并限制访问；由于呼叫中心属于高时效性企业，在网络应急响应上存在严格要求，故出需要在互联网接入上选用双运营商接入，并在关键网络设备上做双机热备至少应保证出口防火墙、核心交换机部署双机热备，在网络层面保证业务延续性，防火墙推荐绿盟、天融信；行为管理推荐深信服、网域。

服务器安全

服务器安全主要是保障信息系统及数据安全，服务器应做好实时系统状态监控，将风险处置前移，做好数据备份及异地容灾。

数据安全

常规呼叫中心往往重视边界和人的防护，却严重忽视了数据本身的安全防护，边界和人的防护最终的服务对象还是数据本身，做好数据本身的安全防护往往比以上防护的效果更加直观和更省成本。主要防护手段为加密，推荐军攻级加密厂商亿赛通，亿赛通拥有完美的数据安全保护方案，可借助三方厂商的能力加强自身数据安全防护能力，其文档安全系统将核心数据进行加密防护，同时开启屏幕水印及截屏控制，防止不法人员进行拍照和截屏泄漏；这样即使有以上边界防护未关注到的薄弱点，也不担心重要文档泄漏后造成影响，外部人员无法打开使用；同时包含物理端口防护，涵盖 usb、串口、火线、蓝牙等等物理接口可填补主机安全的防护漏洞，在加密的同时可以做到加密文件的服务器端备份，防止员工的恶意删除核心文件；结合系统安全网关做到信息系统中的文件防护，可形成整体的数据安全防护闭环。亿赛通是数据安全厂商中的翘楚，客户覆盖运营商、互联网、金融等全行业用户，与外部呼叫中心甲方客户拥有交集，在外部呼叫中心完成此项数据安全防护时可作为与甲方投标竞谈的亮点，增加项目获取的几率。

保障信息安全的目的是让公司可持续发展，保障业务延续性，守护公司核心资产，减少因信息安全事件带来的经济损失和负面影响，规避因信息泄漏带来的法律风险。做好以上信息安全措施可全方位防护企业信息安全，法律层面合规化，为公司树立良好信息安全防护企业形象，同时可进行 ISO27001 信息安全体系认证，增加信息安全资质证明，这样的呼叫外包中心企业必将在愈发收紧的数据安全环境和竞争越发激烈的外包市场越走越稳、越走越好、越走越远。

亿赛通小贴士 ESAFENET PROMPT

浅析中外信息安全保障体系情况

售前技术部：汤智荣 / 文

信息安全保障的概念，伴随着信息技术的不断进步以及人们对信息安全内涵与外延、作用的不断深化。经历了一个由信息保密到信息安全，再到信息安全保障逐渐深化的过程。纵观各国信息安全保障的法制建设，无论英美法系还是大陆法系的国家都采取了成文法的形式，其演化历程也大致相同。

最近几年，全球信息安全监管环境趋严，全球 107 个国家和地区目前已制定数据安全和隐私保护法律。

国外信息安全保障法律制度的演化

信息安全保障法律制度的建立与完善，包括相关立法体系与实施机制两大部分。按照社会信息化的进程及信息安全的概念、立法原则的演化路径，可将国外信息安全保障法律制度建设的构建路径分为三个时期：通信及计算机安全立法时期、网络安全立法时期、国家信息安全战略下信息安全保障体系全面形成时期。

通信及计算机安全立法时期 (20 世纪 40-80 年代)

(1) 立法体系形成：分散立法

国外真正意义上的信息安全法制建设始于 20 世纪 40 年代，以计算机的问世与 1947 年美国颁布的《国家安全法》为标志，首次以立法的形式强调情报、档案以及反情报、反间谍活动对维护国家安全的重要作用。1967 年美国《信息自由法》在规定政府行政信息需向公众开放的同时。也以法律效力保护了九类豁免信息的安全。

到 20 世纪 70 和 80 年代，伴随“冷战”期间与苏联的信息战，欧美等国先后颁布了一系列保护国家信息安全、打击通信及计算机犯罪的单行法律法规。同时开始通过立法保护个人隐私 (见下表 1)。

表 1 20 世纪 40-80 年代各国颁布的信息安全法律法规

国家	时间	法律	主要内容	侧重领域
美国	1947	《国家安全法》	强调情报，档案以及反情报，反间谍活动对维护国家安全的重要作用	信息保密安全
	1967	《信息自由法》	规定了涉及秘密及隐私而受保护可豁免公开的信息	个人隐私安全
	1974	《隐私权法》	就政府机构对个人信息的采集、使用、公开和保密问题做出了详细规定	个人隐私安全
	1977	《联邦计算机系统保护法案》	对未经授权私自进入联邦计算机系统造成损害等犯罪行为做出法律规定	计算机系统安全
	1980	《隐私保护法》	除内容事关防止死亡或严重伤害或儿童色情之必需外，政府不得阻碍新闻传播	个人隐私安全
	1984	《伪装进入设施和计算机欺诈及滥用法》	对未经授权或超出授权范围情况下，故意或欺诈进入计算机获取利益或造成损害的犯罪行为做出法律规定 (美国第一部联邦计算机犯罪成文法)	计算机系统安全
	1986	《计算机欺诈及滥用法案》	明确联邦计算机犯罪中欺诈和滥用罪的定义，消除法律模糊性，扫除对计算机犯罪起诉的障碍	计算机系统安全
	1986	《电子通信隐私法》	对动态传输的有线、口头与电子通信保护及静态存储的电子通信安全保障做出规定	电子通信信息保密与安全
	1987	《计算机安全法》	规定了政府在提高联邦计算机系统安全性和隐私保护方面可采取的措施和行为 (成为美国维护计算机使用与信息安全的基本法)	计算机系统安全
英国	1984	《数据保护法》	为在计算机中存储个人信息的个体赋予了新的合法权利	个人隐私安全
	1985	《通信截收法》	对故意截收通信的犯罪行为及通信截收许可证的条件，范围，有效期等做出法律规定	个人隐私安全
	1989	《官方保密法》	缩小了国家秘密范围，修改部分违法行为处理	信息保密安全
	1990	《计算机滥用法》	重点打击未经许可而故意进入计算机的违法行为	计算机系统安全
德国	1975	《联邦议院保密规定》[44]	对国家秘密等级与范围等做出相关规定	信息保密安全
	1977	《联邦数据保护法》	对受保护数据的内容，范围及要求做出规定	信息保密安全
	1986	修正《德国刑法典》	加入资料伪造罪，资料变更罪，计算机欺诈罪，计算机破坏罪等 7 项计算机犯罪规定	计算机系统安全

(2) 立法范围与立法内容

表 l 显示，本阶段无论英美法系还是大陆法系的通信及计算机安全立法，都采取了分散式立法。即对通信系统安全、计算机系统安全、个人隐私保护分别进行了立法。即使是国家安全法也主要强调的是信息保密，且在立法范围与立法内容上呈现如下特征。

立法范围：限于政府内部系统。主要是面向政府机密、电子通信信息和单机数据的信息安全立法。通过限制获取保护信息的真实、完整、可靠，使重要信息免受侵害。

立法内容：通信与计算机系统安全 + 信息保密 + 个人隐私。欧美国家信息安全萌芽较早，信息安全立法内容较丰富，以通信与计算机系统安全为主，注重对国家机密、政府信息与个人隐私的保护。

2.2 网络安全立法时期 (20 世纪 90 年代初期至后期)

20 世纪 90 年代，计算机和通信设备快速普及，网络快速发展。“全球互联”局面逐渐形成。

为了平衡信息的开放传播与管理控制，维护网络环境下信息领域安全。各国相继制定一系列涉及信息基础设施保护、网络安全、信息技术、国防安全、个人隐私保护等已有主动防御功能的法律法规。这一时期，立法原则仍是“适度安全一最低限度”。互联网环境下的信息安全立法体系得到迅速发展。在立法体系上，英美法系与大陆法系的国家不同。

①英美法系：分散法 以美国和英国为代表的英美法系国家，在社会信息化过程中，对于计算机犯罪与个人隐私泄露等问题颁布了一系列具有针对性的法律法规，形成分散式的立法模式。“冷战”结束与国家信息基础设施计划 (National Infomation Infrastructure，NII) 的提出都对美国信息安全立法起到了极大的促进作用。1998 年时任美国总统克林顿签署第 63 号总统令《保护美国关键基础设施》，提出保护政府关键基础设施免受侵害，特别是基于网络的系统，并对各部门职能、目标、行动计划及意义等做出明确说明，成为美国信息安全的标志性事件。英国针对日益严重的计算机犯罪，于 1995 年颁布《信息安全管理实施细则》，为各机构、组织的信息安全管理提供了一套相对完整的管理框架；1998 年颁布《数据保护法案》，规定部分涉及国家安全、商业机密和个人隐私的信息受法律规范保护，可不对外公开。此外，英美两国还颁布了涉及信息基础设施、信息技术、国防安全、个人隐私的多部法律法规 (见表 2)。

表 2 20 世纪 90 年代美英两国颁布的信息安全法律法规

国家	时间	法律	主要内容	侧重领域
美国	1947	《国家安全法》	强调情报，档案以及反情报，反间谍活动对维护国家安全的重要作用	信息保密安全
	1967	《信息自由法》	规定了涉及秘密及隐私而受保护可豁免公开的信息	个人隐私安全
	1974	《隐私权法》	就政府机构对个人信息的采集、使用、公开和保密问题做出了详细规定	个人隐私安全
	1977	《联邦计算机系统保护法案》	对未经授权私自进入联邦计算机系统造成损害等犯罪行为做出法律规定	计算机系统安全
	1980	《隐私保护法》	除内容事关防止死亡或严重伤害或儿童色情之必需外，政府不得阻碍新闻传播	个人隐私安全
	1984	《伪装进入设施和计算机欺诈及滥用法》	对未经授权或超出授权范围情况下，故意或欺诈进入计算机获取利益或造成损害的犯罪行为做出法律规定 (美国第一部联邦计算机犯罪成文法)	计算机系统安全
	1986	《计算机欺诈及滥用法案》	明确联邦计算机犯罪中欺诈和滥用罪的定义，消除法律模糊性，扫除对计算机犯罪起诉的障碍	计算机系统安全
	1986	《电子通信隐私法》	对动态传输的有线、口头与电子通信保护及静态存储的电子通信安全保障做出规定	电子通信信息保密与安全
	1987	《计算机安全法》	规定了政府在提高联邦计算机系统安全性和隐私保护方面可采取的措施和行为 (成为美国维护计算机使用与信息安全的基本法)	计算机系统安全
英国	1984	《数据保护法》	为在计算机中存储个人信息的个体赋予了新的合法权利	个人隐私安全
	1985	《通信截收法》	对故意截收通信的犯罪行为及通信截收许可证的条件，范围，有效期等做出法律规定	个人隐私安全
	1989	《官方保密法》	缩小了国家秘密范围，修改部分违法行为处理	信息保密安全
	1990	《计算机滥用法》	重点打击未经许可而故意进入计算机的违法行为	计算机系统安全
德国	1975	《联邦议院保密规定》[44]	对国家秘密等级与范围等做出相关规定	信息保密安全
	1977	《联邦数据保护法》	对受保护数据的内容，范围及要求做出规定	信息保密安全
	1986	修正《德国刑法典》	加入资料伪造罪，资料变更罪，计算机欺诈罪，计算机破坏罪等 7 项计算机犯罪规定	计算机系统安全

②大陆法系：基本法 + 单行法

以德国、俄罗斯、日本为代表的大陆法系国家，在国家基本法框架下。针对国内信息安全问题与信息安全法制建设需要。颁布多项单行法规，形成“基本法 + 单行法”的立法模式，以德国和俄罗斯为代表的信息安全综合法开始出现。

德国 1997 年颁布的《信息和通信服务规范》(《多媒体法》)，被认为是国际上第一部规范的信息安全法律，涉及网络犯罪、数字签名、个人隐私等多项内容，是一部较全面的综合性法律，后来成为德国信息安全的统一法、基本法。苏联解体后，1993 年《俄罗斯联邦宪法》 作为俄罗斯的基本法，首次对信息安全做出明确规定，并纳入国家安全管理范围，并在此基础上颁布《信息、信息化和信息保护法》(1995)，对信息资源的所有、使用以及保障手段进行了规定，成为俄罗斯信息安全立法的根本依据 1995 年颁布《信息安全纲要》(草案)"，提出了信息安全保护的任务、目的、政策以及要解决的关键问题; 1997 年发布《国家安全构想》，强调网络信息安全的重要性；1999 年又颁布《网络立法构想》(草案)，提出加强网络安全立法和个人信息保护的必要性。日本于 1999 年颁布《信息公开法》《禁止非法接入法》和《保护商业机密法律修正案》”，通过管理和维护信息安全。规范和促进信息化发展。

(2) 立法范围与立法内容

表 2 显示。本阶段英美法系国家对网络安全立法继续采取分散式的立法模式。而大陆法系国家则采取基本法 + 单行法或综合法立法模式。在立法范围与立法内容上呈现以下特征。

立法范围：这一时期。各国立法范围主要涉及网络犯罪、数字签名、个人隐私、信息基础设施、信息技术、国防安全等领域。计算机系统安全防护由原先的政府系统扩展到普通用户计算机的使用。

立法内容：重视对信息技术安全的保护：个 人隐私安全重点由传统资料及通信隐私安全向网络隐私安全转变；国家安全由反情报、反间谍到开始重点关注国防信息安全。总体来看。信息安全立法由保护信息本身向保护信息体裁、传播、监管的全过程转变，信息安全保障由被动保护向主动防御转变。

国家安全战略下的信息安全保障体系健全完善时期 (21 世纪初至今)

(1) 国家安全战略框架: 基本法 + 实施机制 (行动计划) 进入 2l 世纪，网络的数字化、互联化、智能化，在方便信息传播的同时，也给信息安全提出了更大的挑战。特别是近年来，物联网、云计算、大数据等概念活跃于人们的视野中，世界范围内的信息化建设步人新的阶段。新型媒体与通信方式层出不穷。“9.1l”“棱镜门”“2017 勒索病毒”等新型网络攻击技术下的恶性犯罪事件频发，一次次给各国的信息安全保障敲响了警钟。自 2003 年以来，美国、日本、英国、俄罗斯等国先后颁布了“信息安全战略”，各国开始采取更加积极的政策来应对国家信息安全问题。

立法原则从“适度安全”转向“大安全”原则。颁布专门的信息安全基本法，并将信息安全特别是网络安全提升至国家战略高度。提出战略行动计划，做到前瞻性布局 (见图 1)。信息安全保障体系进入国家安全战略下的健全完善时期。

图 1 各国信息安全基本法及战略

此外。各国还针对不同阶段的发展情况及信息安全问题颁布了多部政策框架与行动计划 (见表 3)。这些政策法律的颁布说明各国信息安全法制建设逐渐走向信息基本法框架下的各信息活动全过程的立法，法律规范中有关计划 的实施、监管及评价的实施机制出现，立法模式由分散的单行法规向统一立法转变。

表 3 2000 年至今各国信息安全政策框架与行动计划

国家	时间	法律	国家	时间	法律
美国	2000	《信息系统保护国家计划》	德国	2002	《联邦数据保护法》
	2002	《信息网络安全研究与发展法》		2015	《德国网络安全法》
	2002	《联邦信息安全管理法案》	俄罗斯	2000	《国家信息安全学说》
	2003	《保护网络空间的国家战略》		2000	《国家信息安全构想》
	2006	《联邦网络空间安全及信息保护研究与发展计划》		2000	《国际间发展和利用之国家政策法》
	2008	《国家网络安全综合计划》		2013	《2020 年前俄罗斯联邦国际信息安全领域国家政策框架》
	2011	《网络空间可信身份国家战略》		2014	《俄罗斯联邦网络安全战略构想》草案
	2011	《网络空间国际战略》			
	2011	《网络空间行动战略》	日本	2001	《e-Japan 战略》
	2014	《网络安全框架》		2006	《第一国家信息安全战略》
	2015	《网络安全法案》		2009	《第二国家信息安全战略》
	2016	《网络安全国家行动计划》		2010	《保护国民信息安全战略》
				2013	《网络安全战略》

其中，美国《网络安全法案》(2015) 是目前美国规制网络安全信息共享方面一部较为完备的法律。德国《德国网络安全法》(2015) 标志着德国信息安全立法由分散走向统一，堪称系统完备的关键信息基础设施保护制度体系。俄罗斯《2020 年前俄罗斯联邦国际信息安全领域国家政策框架》(2013) 明确了俄罗斯在国际信息安全领域的主要威胁、政策目标及实施机制，体现了信息安全正在由国家安全走向国际安全。

(2) 立法范围与立法内容

表 3 显示，进入 21 世纪，以美国、日本、英国、俄罗斯等国为代表的发达国家，其国家安全战略下的信息安全保障体系，在立法范围及立法内容方面呈现以下特征。

立法范围: 立法层次由国家立法上升到国家战略高度。发达国家信息安全立法与实施机制逐渐健全与完善；立法范围涉及信息内容安全、数据安全、物理安全、网络空间安全、信息基础设施安全、国际信息安全等领域。网络空间安全由国家战略走向国际战略。

立法内容：各国信息安全法律体系不仅包括网络安全的国家战略与行动计划，还包括网络安全的法律法规，以及信息安全的管理、技术标准，立法内容空前丰富，以维护网络空间安全为主的综合性主动防御型信息安全保障体系全这一时期，在大安全观下，国际安全、国家安全和社会安全紧密相连，信息质量、信息设施、信息环境和信息管理有机结合，是新时期构建信息安全保障体系一体化的理论基础。

国内信息安全体系现状

我国近年信息安全法律法规现状

我国目前已确立了“总体国家安全观” 的立法原则，即以人民安全为宗旨，以政治安全经济安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托。兼顾外部安全与内部安全、国土安全与国民安全，兼顾传统安全与非传统安全、发展问题与安全问题，以及自身安全与共同安全，体现中国特色国家安全保障体系全新的指导思想。

图 2 我国国家信息安全保障体系整体框架

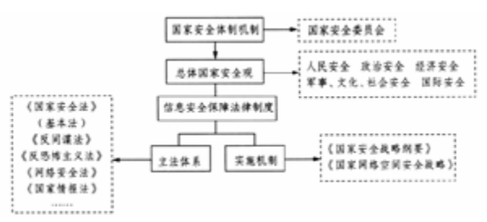


表 4 21 世纪初至今我国颁布的信息安全法律法规

级别	时间	部门	名称	意义	领域
法律	2014. 11	全国人大常委会	《反间谍法》	首次对具体间谍行为进行法律认定，起到基础性法律保障作用	国家安全，人民安全
	2015. 7	全国人大常委会	《国家安全法》	综合性、全局性、基础性的国家安全立法	11 个领域的全面安全
	2015. 12	全国人民代表大会	《反恐怖主义法》	构建了反恐怖主义情报信息工作机制	国家安全，国际安全，人民财产安全
	2016. 11	全国人大常委会	《网络安全法》	成为我国网络安全的基本法，我国网络安全工作有了基础性的法律框架	网络安全
	2017. 6	全国人大常委会	《国家情报法》	加强和保障国家情报工作	国家安全，人民安全，情报安全
行政规章	2003. 8	国家信息化领导小组	《关于加强信息安全保障工作的意见》	我国信息安全保障工作有了总体纲领	基础信息网络、重要信息系统
	2016. 12	国家互联网信息办公室	《国家网络空间安全战略》	从国家安全战略高度部署网络空间安全的具体措施与目标	网络空间安全

我国数据安全相关法律法规

2021 年，我国《数据安全法》《个人信息保护法》已被列入人大常委会表决通过。数据安全国家标准定位如下：

《网络安全法》：国家建立和完善网络安全标准体系

《数据安全法》：国家推进数据开发利用技术和数据安全标准体系建设

支撑法规政策：数据安全国家标准是对国家法律法规和政策规章的细化支撑

规范引导行业：基于问题导向原则，及时发现数据安全典型问题和安全风险，为组织数据安全事件提供参考。

图 3 我国数据安全相关法律法规

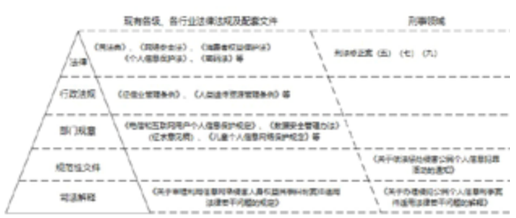


图 4 数据安全国家标准体系

总结

中国在信息安全保障概念、立法原则及法律制度建设的演化路径方面与国外基本一致，但在发展起点与发展阶段上却存在滞后性，在立法内容上也存在一定的差异。随着《数据安全法》、《个人信息法》和《关键信息基础设施安全保护条例》的实施，我国在总体安全观下新型信息安全保障体系将逐步建立。

引用资料：

[1]、相丽玲 陈梦婕 : 试析中外信息安全保障体系的演化路径

[2]、中国电子技术标准化研究院 程多福 数据安全法规及标准建设

[3]、复旦发展研究院 重点国家网络安全法洞察报告

[4]、刘志诚 隐私与数据安全趋势与实践

《数据安全法》中的数据安全治理分类分级要求

售前技术部：曾云杰 / 文

《数据安全法》马上将于 9 月 1 日正式实施，这是我国历史上第一部针对数据安全所制定的法律，表明生活中我们必不可缺的数据已经获得立法上的认可。

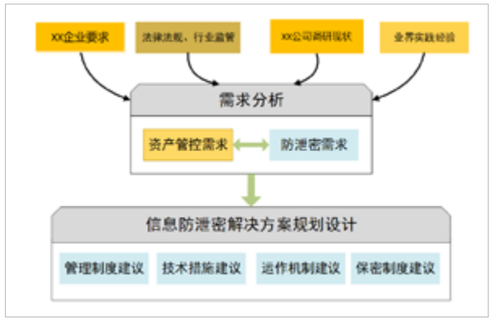
随着数据安全法的实行，确立了数据在我们使用过程中的高地位，也确立了数据的主体，同时为企业和个人规定了相应的义务和责任，在法律层面上确立处罚的标准等等。

针对第三章数据安全制度第二十一条规定：国家需要建立数据分类分级保护制度。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。“

延申到企业，更要进行数据分级分类的保护并按要求执行，不仅是对于以数据为主要营收手段的企业，针对我们各行各业也是需要进行数据分类分级保护。

某些企业虽然已经安装加密产品，但缺乏数据分类分级的保护，解密权限随意发放，企业资产没有分类分级处理，导致重要文件被泄露，使用加密产品形同虚设。亿赛通具备专业的数据安全建设能力，10 余年数据安全建设方法论 + 九大行业实施经验，为企业推出全工作场景、全业务流程、全生命周期的数据安全防护方案。

数据分级分类整体思路：



目前已服务过包括华润置地、东风汽车、泉州银行、山东城商联盟等知名客户，其中泉州银行与亿赛通共同完成的《城商行数据安全管理平台的研究及实践》获得 2018 年度银行业信息科技风险管理课题研究成果二类奖项。

典型案例 TYPICAL CASES

互联网行业数据安全治理解决方案

一、行业背景

在互联网时代发展浪潮中，涌现了越来越多的新型互联网产业。其中大量的数据在互联网中飞速传播流转，由于互联网信息传播的即时性、开放性、互动性也使我们的数据安全造成了极大的泄露风险，互联网科技型公司以研发技术实力为根本，一旦核心商业资料和客户信息泄露将引发极大的经济和声誉的损失。

从国家层面，《网络安全法》的颁布以及《个人信息安全规范》的重新制定，规范了个人信息的主体权益和互联网运营者所营业务的范围标准、达到保护民众在使用互联网产品时保护个人隐私，各企业也能有效的保护自己的商业核心。

二、互联网泄密风险分析

1. 关键的技术资料没有有效的防护措施，容易被内部人员窃取；

2. 数据库的访问权限没有做到细粒度控制；

3. 数据库的日志操作行为没有详细的审计工具；

4. 个别高层管理者数据访问权限过高，没有有效的检测审计手段。

5. 出现安全事件后，没有相关审计溯源措施，无法确定相关责任人。

三、解决方案

互联网企业要在激烈的竞争脱颖而出，就必须稳中求发展，商业机密资料的安全是第一位，提升安全管理意识的同时，增加有效的技术手段是信息防泄露的必要条件。亿赛通提供如下三个层面的解决方案；

1．结构化数据安全防护

亿赛通的数据库防护技术是基于数据库协议分析与控制技术的数据库安全防护系统。通过主动防御机制，实现数据库的访问行为控制、危险操作阻断、可疑行为审计。

2．非结构化数据安全防护

亿赛通文档安全管理系统是国内早期基于文件过滤驱动技术的文档加解密产品，系统包括透明加密、权限管理、外发管理、应用安全网关、安全中间件、智能移动终端、U 盘客户端等核心组件。用于对用户电脑终端、移动办公、各类应用系统上的数据，从生产、存储、流程、外发到销毁进行全生命周期保护。

3．用户行为检测与分析

以企业数据为核心，通过大数据技术和数据收集等技术，为用户提供企业数据资产分布、企业数据关系、应用使用分析等。帮助用户了解企业内部数据分布、数据业务、数据拓扑关系等，可以帮助企业清晰了解数据整体使用和流动情况。

四、方案收益

1. 细粒度数据库访问控制保证数据库访问安全；

2. 数据库三层关联审计模式对运维开发者的操作过程进行端到端的用户行为审计，达到数据库的审计溯源；

3. 对核心资料加密存储、加密传输有效的防止重要信息的泄露；

4. 通过用户行为分析可以快递精准定位数据位置、展示用户活动、分析数据历史。完整展示数据生命周期，协助用户快速定位泄密风险。

通讯行业数据安全治理解决方案

一、行业背景

随着云计算、大数据、移动物联网等新技术的全面覆盖，运营商与通讯研发行业在互联网的飞速发展下产生了庞大的、多样化的数据。数据的采集、存储、处理的效率不断提高，也促使数据体量变化越来越大，其中包含这大量的敏感信息和用户个人信息，所以如何合理的利用这些数据的同时还能保护数据安全是我们面临的严重挑战。

此时，国家发布了国家标准《个人信息安全规范》对个人信息的分类分级和安全技术要求做了明确要求。针对通讯行业也发布了《基础电信企业信息安全责任管理办法 (试行)》《电信网和互联网信息服务业务系统安全防护要求》对通讯行业相关安全技术要求也做出了详细指引。

二、通讯数据安全风险分析

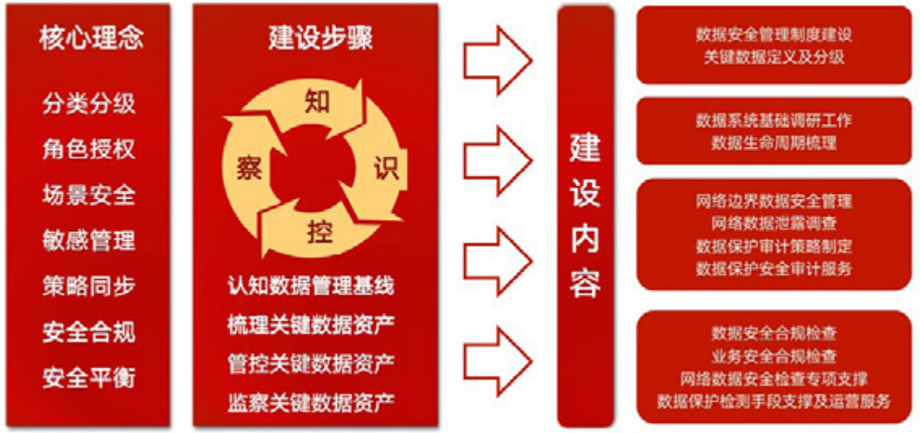
数据安全的整体需求

1) 系统数据量大，数据关系复杂，难以进行梳理；

2) 个人信息数据没有明确的分级分类；

3) 大量的结构化、非结构化数据没有标准化、规范化；

4) 保护措施无法分级分类管理，保护效能和效率较低。



三、解决方案

数据安全体系化标准

1) 数据安全的人员职责明确化；

2) 数据安全的管理制度需要规范化；

3) 根据数据生命周期不同阶段建立不同的管控手段；

4) 建立数据资产的审计和溯源。

四、方案收益

1. 管理型收益

符合国家信息安全相关标准，对组织、人员、制度整体性管理的建设，独立组织、明确职责、规范流程的可持续优化，全面的帮助通讯行业在庞大的体系管理中达到可持续发展。

2. 安全性收益

结合相关业务应用的运行现状来建立数据安全体系，数据安全全生命周期技术防护策略配合标准化的管理制度及流程；即可满足现有环境的数据分级安全管理又能保证业务的连续性。

数据安全建设从来不是一蹴而就的，而需要长期不断 PDCA 进行管理和技术的调整优化。随着管理制度的不断完善，数据安全管控策略也要随之完善优化，通过数据安全工具的日志分析和趋势分析，有针对性地加强各部门安全建设，防控安全风险，也要进行各部门的自查和监督部门的结果性审计检查，同时要做好公司内的培训宣贯，规避常见办公安全风险，贯彻数据安全管理规定。