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

7 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

守护产业数字化转型，《亿赛通七月刊》重拳出击

随着各项新兴技术的迅速发展应用，并与实体经济深度融合，数据已成为我国经济社会发展的基础性、战略性资源和重要生产力，带动着信息数据相关的新业态、新模式迅速崛起，成为我国经济高质量发展的新引擎。鉴于其重要性，国务院把信息数据以新型生产要素写入文件，纳入到与土地、劳动力、资本、技术等传统要素同等重要的要素之列。当前，我国数字技术覆盖面广、渗透力强，与各行业融合发展，已成为关键的生产要素。数据要素推动我国经济高质量发展和数字化转型。

亿赛通作为国内专业的综合数据安全厂商，守护企业数字化转型是我们的义不容辞的责任，本月，亿赛通针对数据安全法进行专业系列解析，拓展战略合作，增强国产化产品适配，积极响应国家政策，《亿赛通七月刊》为您精彩呈现……

国内

1、八成多网民因信息泄露添烦恼 调查发现平台猫腻多多

摘要：据中国互联网协会《中国网民权益保护调查报告（2021）》显示，63.4% 的网民个人网上活动信息被泄露 (如通话记录、网购记录、网站浏览痕迹、ip 地址、软件使用痕迹及地理位置等)，82.3% 的网民亲身感受到了由于个人信息泄露对日常生活造成的影响，49.7% 的网民认为个人信息泄露情况严重或非常严重。

某些 App 是如何侵犯个人数据隐私的？近期，深晚记者也从多方面对部分涉嫌侵权的 App 进行调查，揭露平台猫腻。法律界人士提醒，平台泄露信息将面临行政处罚，情节严重的还可能被追究刑事责任。

2、泛海置业等 20 家房企收集人脸信息被罚 203 万 浙江“亮剑”个人信息泄露与买卖

摘要：7 月 19 日，浙江省市场监督管理局微信公众号发文，浙江省“亮剑 2021”消费安全综合执法行动于 6 月底收官，消费信息安全成为重点执法领域。十大典型案例中有三例与侵犯消费者个人信息相关，涉及房地产、网络教育培训、家装业等领域的非法收集、使用及贩卖消费者信息等行为。其中，宁波 20 家房地产公司合计被罚 203 万，非法收集人脸信息行为被叫停。即便展示采集人脸信息标识，但未经消费者同意仍不能免罚。

3、20 多万条个人信息遭泄露，竟是多家培训机构“共享资源”

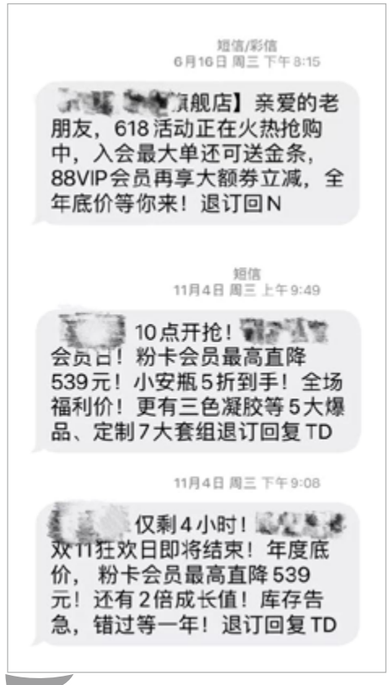
摘要：近日，盐城市盐南高新区警方陆续接到家长举报。现代快报记者了解到，经过民警深入调查，发现 4 家教育培训机构，非法获取学生及家长个人信息 20 余万条，警方抓获了 3 名犯罪嫌疑人。

4、青海一男子贩卖个人信息，多人信息已遭泄露…

摘要：7 月 15 日，西宁市公安局城北公安分局发布消息，西宁一男子售卖个人信息，涉嫌帮助十余起信息网络犯罪活动罪，被警方采取刑事强制措施。

5、滴滴出行 App 突然被下架，信息泄露会有什么严重后果？

摘要：7 月 4 日晚，网信办发出《关于下架 " 滴滴出行 "App 的通告》。根据公告，其下架原因是：" 滴滴出行 "App 存在严重违法违规收集使用个人信息。目前，" 滴滴出行 "App 已在 App Store、华为、小米等各大应用商店全面下架。



6、个人信息保护新规将出台 消费者被短信轰炸将成为历史

摘要：上海证券报记者近日获悉，工业和信息化部将会同相关部门尽快发布实施《移动互联网应用程序个人信息保护管理的暂行规定》（简称《规定》）。《规定》将为个人信息保护提供更加坚实的政策保障。在新规的引导下，多个电商平台已经主动加强了对客户信息的保护力度。

7、家长群又出幺蛾子，老师让在线登记学生信息，家长不满信息被泄露

摘要：家长群让老师方便与家长沟通的同时，也存在一些隐患，比如广州南沙一位班主任和学生家长在家长群吵起来了，家长要投诉班主任泄露个人信息！由于广州中学生要开始打疫苗，所以需要登记个人信息和家庭信息，这位班主任就弄了一个在线文档在群里面让大家填。

大家都能互相看到其他家庭的个人信息，全班各学生的姓名、身份证号码、联系方式、家长姓名和联系方式一览无余，家长群所有人都可以看得到。所以这位家长就觉得自己的信息被暴露了，很不满，于是将个人信息私发给老师，让老师自己整理，防止孩子信息泄露，但该班主任并不想给自己增加麻烦，拒绝自己整理。当学校老师再次提醒家长填写信息时，家长表示已经将个人信息发给了班主任，是班主任没有填上去，没有做到应有的责任。然而该老师与班主任持同样看法，认准了只能让家长自己填写，还说：“是学校要求老师这样做的，我们只是执行，不满意你可以换学校”！

8、央行出手，这些银行，因泄露个人不良信息被罚，揭开征信修复骗局

摘要：近日， 友利银行（中国）有限公司因为三项违规案由被人民银行营业管理部开出罚单，其中一项违法事实是“由于提供个人不良信息未事先告知等违法行为”，这个就是侵犯了客户的隐私权 . 银行是没有权利私自将客户的不良信息提供给第三方的，至少也得经过本人同意。友利银行为自己的违法行为付出了代价，被罚款 198.5 万元。

9、身份信息泄露？芜湖一大学生因为“刷单”卷入诈骗案！

摘要：近日，特警三大队民警接 110 指令称，一名犯罪嫌疑人在芜湖有活动轨迹，民警立即对其进行研判。7 月 16 日晚，该嫌疑人来到芜湖市公安局投案自首。得知自己违法后，嫌疑人十分后悔，几次痛哭，表示自己并不知情，以为只是单纯的刷单获取报酬。

10、宁夏银川对泄露消费者信息和预付式消费“开刀”

摘要：为保障群众交易安全，使消费者免受骚扰信息侵害，宁夏银川市将严厉打击部分重点领域泄露消费者信息的违法行为，并着力整治预付式消费问题。重点打击投资、理财、贷款、房产中介、寿险、车险、医疗险等领域 3 类泄露消费者信息的违法行为：未经消费者同意，收集、使用消费者个人信息；泄露、出售或者非法向他人提供所收集的消费者个人信息；未经消费者同意，或消费者明确表示拒绝，但仍向其发送商业性信息。

国外

1、日媒：东京奥运会、残奥会门票购买者和志愿者个人信息遭泄露

摘要：据共同社报道，东京奥运会、残奥会门票购买者和志愿者的 ID 及密码被盗，并在网络上泄露。东京奥组委正在进行调查，并已经采取措施防止影响扩大。日本政府的有关人士解释说，规模“不是很大”，但并未透露具体数量。

2、赎金 5000 万美金，沙特阿美数据泄漏

摘要：据美联社报道，沙特阿拉伯国家石油公司（沙特阿美）21 日承认公司有数据泄露。此前，有黑客向该公司勒索 5000 万美元赎金。沙特阿美表示，被泄露数据原先掌握在第三方承包商手中，公司自身系统未被入侵。该公司称，“我们证实这起数据泄露并非由于我公司系统遭到入侵，不影响公司运营。”

3、美国保险巨头 Humana 客户医疗数据被泄露

摘要：在一个出名的黑客论坛上有攻击者泄露了美国超过 6000 名患者高度敏感的健康保险数据的数据库。攻击者声称这些数据是从美国保险巨头 Humana 处窃取的，包括该公司健康计划内客户可追溯到 2019 年的详细医疗记录。被泄露的信息包括患者姓名、ID、电子邮件地址、密码哈希、医疗数据等信息。

4、费城一医院癌症患者数据遭泄露！8 月起用户可收到高危风暴预警短信

摘要：费城托马斯·杰斐逊医院（Jefferson Health）说，今年 4 月，一个包含了 1769 名在西德尼金梅尔癌症中心（Sidney Kimmel Cancer Center）患者信息的云数据库，遭到了针对软件供应商的黑客攻击，部分癌症患者的数据被窃取。

5、美国前情报分析员因泄露美军用无人机数据获刑

摘要：据多家美国媒体报道，当地时间 27 日，美国前情报分析员丹尼尔·埃弗里特·黑尔因向媒体披露美军用无人机信息而被判处 45 个月监禁。

6、2020 年全球数据泄露的数量超过过去 15 年的总和

摘要：有研究机构统计，2020 年全球数据泄露的数量超过过去 15 年的总和。这些数据安全的风险影响范围已经从个人、企业逐步辐射到产业甚至是国家，数据安全风险隐患非常突出。

7、黑客暗网售卖 7 亿用户数据 领英拒承认数据泄露 会员面临巨大风险

摘要：有黑客在暗网平台售卖领英 7 亿条的用户数据，数据中包含用户邮箱、姓名、电话号码、家庭住址、个人和职业背景信息等内容。据悉，领英有 7.56 亿用户，此次事件为领英历史以来最大规模的数据“泄漏”。领英官方发表声明表示，“这不是数据泄漏，也没有泄漏任何 Linkedin 成员的私人数据。调查发现，这些数据是从 Linkedin 和其他各种网站上抓去的，其中包括今年早些时候在 4 月事件的相同数据”。

8、PHP 站点的用户数据库在最近的源代码后门攻击中遭到黑客攻击

摘要：PHP 编程语言的维护人员发布了关于上月底曝光的安全事件的更新，指出攻击者可能已经掌握了包含其密码的用户数据库，以便对存储库进行未经授权的更改。“我们不再相信 服务器已被入侵。但是， 用户数据库有可能泄露，”在 4 月 6 日发布在其邮件列表上的消息中说。3 月 28 日，身份不明的攻击者使用 Rasmus Lerdorf 和 Popov 的名字将恶意提交推送到托管在 GIT.PHO.NET 服务器上的“php-src”存储库，其中涉及在一个实例中向 PHP 源代码添加后门。软件供应链攻击。

行业聚焦 INDUSTRY FOCUS

9、厄瓜多尔 150 万名患者身份信息遭泄漏

摘要：厄瓜多尔公共卫生部长加尔松表示，该部已经要求检察院调查包括接受新冠病毒感染检测人员在内的 150 万名患者身份信息泄露事件。报道称，该国卫生部采集疫情统计信息的平台上 7 月 25 日发布了 150 多万名人员的私密信息，包括姓名、职业、身份证号码、医保卡号码、电话等项。据悉，这些数据曾在数小时内可以随意浏览。

10、英国枪支销售网站超 11 万名用户信息遭泄露

摘要：近日，犯罪分子侵入了一个用于买卖枪支的网站，窃取了一个 111000 个条目的数据库，其中包含来自英国各地枪支商店使用的 CRM 产品的部分信息。本周早些时候，Guntrader 泄露事件导致 Guntrader.uk 买卖网站及其电子枪支商店注册产品的 SQL 数据库被盗，该数据库包括约 111000 名用户的姓名、手机号码、电子邮件地址、用户地理位置数据，以及包括 bcrypt 哈希密码在内的更多信息。

亿赛通亮相首届数字安全大会，独家分享亿赛通的“夺宝秘笈”

数字世界 安全共生

数字世界，安全是千行百业的“地基”。万物互联构筑了新的世界体系，安全问题不再禁锢在本行业活动领域内，数字安全成为千行百业共同关注的话题。数字经济离不开数字安全的保驾护航，确保数字安全，推动行业变革，是维护数字世界安全运行的保障。

7 月 16 日，由中国信息协会信息安全专业委员会，中国关键信息基础设施技术创新联盟指导，数世咨询和 CIO 时代主办的“首届数字安全大会”成功举办。亿赛通于分论坛发表《数据安全的数据安全的大势与小节》主题演讲，同现场的行业学者、专家领导，分享了从理念、建设、实施等多个维度进行数据安全体系防护经验和突出效果。

本届大会，以“数字世界 安全共生”为主题，分为上午主论坛和下午分论坛，来自企业 CSO、CIO、CISO 和专家以及研究机构负责人等行业内外的学者大咖 400 余人齐聚一堂，共论数字经济健康发展策略，引领行业变革，推动数字安全发展。

大胆创新 理念升级

数字时代下，传统的数据安全防护模式遭遇全新挑战，亿赛通数据安全建设理念的出现为数字安全防护带来新的可能，是当前应对数字化挑战的最佳思路。

数据安全建设理念包括“分 • 放 • 管 • 服”四步。亿赛通“分 • 放 • 管 • 服”引自国务院总理李克强提出的全国深化“放管服”改革优化营商环境指导，亿赛通把其引入到数据安全创新理念之中，是因为二者理论思路相同。在数字化转型的驱动下，数据安全已经成为企业运行和发展的核心资源，整合自身内、外优势，将其作为有利的工具，更好的服务于客户，准确识别和抵御安全威胁，化解各种安全风险，构建数字化发展的安全可信环境。

亿赛通安全专家讲解到：“分”是从整体架构的层面来规划数据安全，是数据安全综合解决方案的基础，没有准确合理的“分”就没有有效安全的数据应用和管控。

“放”的含义是指数据的流动与应用，“管”则是指保障数据的安全。高效的数据应用给机构带来巨大的业务价值，但如果没有数据安全的保障，则时刻面临着巨大的运营风险，两者之间是一个需要动态精准把握的平衡关系。

但无论如何，这些企业都会将数据安全放在第一位，数据一定要为使用者而服务，因此这一理念映射出亿赛通具有针对和规划性的将客户需求放在第一位。同时意味着，亿赛通更贴近客户需求，也为营销端提出了新的挑战，面对不同客户对数据不同需求，能更了解客户的管控环境。

总结而言，亿赛通“分 • 放 • 管 • 服”的数据安全理念，是为了更好的将服务贯穿到大客户、行业客户之中，为客户提供更好的服务而进行的战略升级。

未来，亿赛通将顺应时代发展，基于“分 • 放 • 管 • 服”数据安全建设理念，全面融合行业解决方案，以发展的视角持续推动数据安全体系的普及与落地，联合生态伙伴共促行业演进，合力构筑我国数据安全基石。

亿赛通助力爱数 SMART 大会，深化双方战略合作

7 月 8 日 -9 日，爱数 SMART 大会在上海开幕，会议以共绘数据新丝路为主题，探讨面对即将到来的智能世界，如何通过技术的创新与连结释放新的生产力。亿赛通作为爱数的战略合作伙伴，受邀进行合作方案展示。

随着企业用户安全防范意识的提高以及对数据安全法、等级保护的深入理解，安全需求个性化、安全方案整体化、安全产品服务化的需求越加强烈。爱数为政府、公共事业及企业的数字化转型赋能，帮助各行各业的客户在数字化浪潮中充分释放数据价值。其面临着安全创新与业务发展的双重压力，如何抓住用户的安全需求并提供整体性的安全服务解决方案迫在眉睫。亿赛通作为国内早期从事数据安全业务的企业之一，始终致力于数据安全产业的发展，特别是数据安全体系的建设和创新应用。

亿赛通与爱数的强强联合，就内容安全管控方面深化进一步的战略合作，借安全之力为产品增值，保障非结构化数据管理过程中的安全合规。通过亿赛通安全产品对本地终端文件进行管控，爱数的 AnyShare 实现云端文件的管理，做到线上线下全方位管控。同时，基于策略驱动的安全管控体系能支持更多的安全管控场景，满足客户不同的安全管控需求，从而维系企业相关业务工作的正常运转，为企业的数据安全与业务的正常运转保驾护航。

本次战略合作依托爱数在行业内的深厚积淀，以及亿赛通在安全技术及能力方面的优势。双方将通过共建内容安全防护能力，创新安全业务增值模式等多种方式，加强安全研究成果的转化，促进安全能力与内容安全深度融合。

近年来，亿赛通始终致力于研究国内外最新数据安全动向，聚焦安全技术以及安全模式的创新。通过与爱数合作，将推动数据安全研究紧贴内容安全需求，带动数据安全能力紧跟新的业务安全场景，加速数据安全紧随行业用户安全应用转变。

除本次大会外，亿赛通将与爱数不断深入合作，加强探索。在新技术新威胁不断涌现的复杂安全环境之下，提升安全管控能力，安全服务能力，并在这些能力的基础上建立协同运营体系，构建符合爱数业务需求的安全能力，为安全赋能。

行业全景图 | 亿赛通数据安全领域专业领跑，全景图入围再下一城

近日，数说安全正式发布《2021 年中国网络安全市场全景图》（以下简称 “全景图”）。凭借数据安全领域专业产品技术，亿赛通入选数据泄漏防护、电子文档管理与加密、数据库安全、数据安全治理与隐私保护四大细分领域代表厂商。

数说安全通过对产品、能力、场景、服务、解决方案这 5 个维度做进一步细分和梳理，最终统计得出，我国网络安全产品与服务市场共计包括 13 类一级版块、81 类二级版块，并以此作为基础，绘制了《2021 年中国网络安全市场全景图》。

与往年一致，此次全景图入围仍然以国家权威机构与行业主管部门颁发的产品和服务资质作为主要考量标准：

- **产品领域：** 主要参考公安部颁发的计算机信息系统安全专用产品销售许可证，优选具有增强级、三级等高级别资质的品牌。

- **服务领域：** 主要参考中国信息安全测评中心、中国网络安全审查技术与认证中心、国家互联网应急中心（CNCERT）颁发的服务资质证书，优选具有高级别服务资质的厂商。

- **通用安全能力和行业解决方案领域：** 主要结合企业核心业务方向、产品成熟度、产品资质级别、市场表现力、品牌知名度等多方面因素进行综合考量。

2021 年上半年，亿赛通基于技术创新优势和行业领先地位，已多次入选行业权威调研机构榜单及相关评选———

• 3 月，亿赛通入选安全牛《第八版中国网络安全行业全景图》；

• 4 月，亿赛通入选 Freebuf《CCSIP2021 中国网络安全产业全景图》；

• 4 月，亿赛通获评“2020 年度商密产业优秀解决方案”奖”；

• 5 月，亿赛通入选 IDC2021《中国数据安全市场研究》报告；

• 6 月，亿赛通 入选嘶吼《2021 年网络安全产业链图谱》；

数说安全发布的“中国网络安全市场全景图”，结合甲方的需求痛点和网络安全市场的趋势热点，站在业务角度看安全，以公平、科学的角度，对中国网络安全市场的产品和服务进行梳理和聚合。

亿赛通专业领域再度上榜，印证了公司近年来研发实力不断增强，自主研发的技术优势和长期以来的客户服务口碑不断提升，是安全行业专业机构对亿赛通综合实力的高度认可。

新时代的安全新思路，亿赛通携全新理念亮相首届数字安全与信任高峰论坛

7 月 24 日，由中关村科学城管委会、CCF 计算机安全专委会、中国保密协会指导，中关村网络安全与信息化产业联盟主办，北京指掌易科技有限公司及北京亿赛通科技发展有限责任公司联合承办的首届数字安全与信任高峰论坛顺利召开。亿赛通作为数据安全安全产品方案提供商，受邀出席并发表主题演讲，同与会领导、行业专家等分享了数字化背景下的数据安全方案及落地实践。

近年来，新一代信息技术与实体经济加速融合，为各产业提质降本增效带来活水，产业数字化转型迎来发展浪潮。企业融合大数据、人工智能、区块链等数字技术构建数字基础设施，进而依托数字基础设施推进客户服务、供应链等业务模块数字化转型。

当前，我国正处于数字化发展的关键时期。随着数字化进程的迅猛推进，数字技术加速向经济社会各领域渗透，业务系统拥抱互联网逐步实现业务线上化，全球的数据爆发增长、聚集，因内部应用系统增多、网络环境愈加开放、用户角色复杂等问题，以及黑灰产针对核心业务的勒索攻击，信息泄露等事件与日俱增，企业的数据安全防控面临巨大的挑战。如何更有效的保障数字资产与业务的安全可信，成为企业数字化转型中的难点。

亿赛通技术专家表示：我司在数据防泄露领域深耕多年，通过不断的技术积累和用户实践，持续对产品的稳定性、易用性、安全性研究完善，始终围绕用户的实际业务需求，创新升级产品和解决方案。并全新提出“分•放•管•服”的数据安全建设理念，并配合设计咨询服务、产品方案、工程交付及售后服务四大体系，根据云、网、端三类应用场景对产品线进行扩充，实现数据安全理念建设的可落地执行，从不同维度为用户提供产品和服务，形成一体化智能管理，打造数据安全领域真正意义上的综合解决方案。

亿赛通提出了自己独具特色的数据安全能力模型，作为数据安全的抓手，从终端、存储、网络和云等几个方面对数据安全进行防控。基于数据安全智能管控平台，利用大数据存储、分析和建模技术，实现数据全生命周期（采集 - 存储 - 传输 - 处理 - 交换 - 销毁）的安全能力，形成包括数据资产梳理、数据安全监控识别、数据风险防控和数据智能分析四大能力集。再结合各行业的数据及业务特征，打造具有行业特色的数据安全解决方案，满足各种行业数据安全防护和治理需要。

数据的时代已经到来，未来人类的生产生活将与数据联系得越来越紧密，保障数据安全可以说是维护社会健康发展必不可少的条件之一。频发的网络安全事件、黑客攻击、以及即将实施的《数据安全法》、《个人信息保护法》等，不论是事件的驱动，还是相关法律法规的促进作用，未来，数据安全领域将会有很多工作要做，数据安全市场必将迎来爆发式增长。亿赛通一直以来积极顺应时代环境和用户需求的变化，找准自身定位，持续创新升级产品和技术，探索制定战略规划。期待亿赛通未来在数据安全领域有更好的表现，为行业带来更多惊喜！

亿赛通亮相中国工业设计软件创新峰会北京站，与众大咖共话数据安全新风向

7月30日，由中望软件主办，亿赛通协办的中国工业设计软件创新峰会北京站正式开幕。峰会邀请了国内工业软件用户、商务技术合作伙伴、行业专家等，旨为搭建深入交流与研讨的互动平台，分享最新的技术成果和行业应用经验。亿赛通作为数据安全领域骨干企业受邀在会中进行独家方案展示。

当前，在加速数字化的大背景下，企业致力于通过推进数字化设计体系建设、提升企业信息化水平，促进转型升级及实现高质量发展。设计行业普遍面临着图纸电子化的新挑战。

面对这一现状，在设计图纸的产生、传递、保存、使用过程中，如何避免设计图纸被窃取、泄露、非法使用，成为企业需要面临的新一轮安全挑战。尽管对数据安全具有强烈需求，但不少企业无法对此投入大量人力物力潜心研究，与专业的数据安全服务商合作，便成为性价比较高的选择。

亿赛通与中望共建安全新生态

亿赛通与中望在双方专业领域中强强联手，优势互补，打造成最强王牌。通过双方共同打造的设计图纸安全一体化产品解决方案，解决企业内部图纸设计中的便捷性和安全性问题。

联合方案在设计平台的基础上，结合亿赛通安全产品，满足不同专业、不同复杂应用场景的需求，实现设计经验的有效传承及设计成果的数字化管理。

• 对文档进行高强度加密并对使用者透明解密，满足数据安全保护的同时，操作简单，应用方便。

• 根据业务需要，对需要与合作伙伴进行交互的外发图纸进行特殊处理，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。

• 显示水印，对截屏、拍照、录屏、打印等敏感操作进行警示，同时方便进行追踪溯源。

作为国内数据安全专业厂商，近二十年来，亿赛通主要涉及数据安全、网络安全及安全服务三大业务，以数据资产防泄密为核心，以网络安全为基本框架，以协议识别解析为技术支撑，对数据进行智能识别、智能分类和智能加密，保障政企单位核心数据资产安全无泄露，打造数据安全领域的综合解决方案。与此同时，亿赛通在业内首提“分•放•管•服”的数据安全建设理念，通过制度主建，技术主战，分放管服，将数据实现分权分责分风险，放管结合，做到要素服务保支撑，持续安全可运营，确保数据有价值的安全流转，共赢数据安全大生态。

迈入数字经济时代，产业升级，威胁也在加剧，面对不断变化的安全挑战，亿赛通提供可靠有效的解决方案的同时，会同行业伙伴和客户积极探索数据安全的产业价值，助推数字经济安全腾飞。活动现场诸多参会人员均反馈，此次参会为企业提供了建设性的思路与实践方向，不虚此行。而亿赛通也凭借深厚的实力积淀，丰富的产品解决方案体系及广泛的客户支撑，成为活动现场最亮的星。未来，亿赛通与中望将全渠道广泛渗透触及更多客户，双方充分发挥各自优势，实现优势互补，共同探索更广泛的合作机会，共同深化双方产业链价值的发展，推动数据安全系统与服务在更多行业落地，保障客户数据安全的同时促使其业务发展与创新。

严惩 APP“一键授权”，深圳政府先行先试

不知从何时起，买个东西，要查看我的手机通讯录；看个电影，要允许录制音频；安装软件，要允许打开定位设置……长久以来，应该有很多人跟小亿一样，对于使用 APP 时被要求“全面授权”的霸王条款，深恶痛绝。

近日，深圳市成为全国首个对这类 APP 下狠手的城市。7 月 6 日，《深圳经济特区数据条例》在深圳市人大常委会网站公布，并将于明年 1 月 1 日起实施，这是国内数据领域首部基础性、综合性立法。

《条例》坚持个人信息保护与促进数字经济发展并重，对市民深恶痛绝的 APP“不全面授权就不让用”、大数据“杀熟”、个人信息收集任性、强制个性化广告推荐等问题说“不”，并给予重罚。

此规定公布后，相关话题立即登上央视新闻。

网友纷纷表示：建议全国推广！

个人数据处理规则以“告知—同意”为前提

我国互联网用户量已达 9 亿，应用程序数量数百万个。长期以来，一些 APP 过度收集个人信息、强制索要用户授权令人深恶痛绝。针对这一问题，《条例》确立以“告知 - 同意”为前提的个人数据处理规则，即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，数据处理者应当提供撤回同意的途径，不得对撤回同意进行不合理限制或者附加不合理条件。

用户有权拒绝被画像和被推荐

《条例》规定，数据处理者基于提升产品或者服务质量的目的，对自然人进行用户画像的，应当向其明示用户画像的具体用途和主要规则。自然人有权拒绝对其进行的用户画像或者基本用户画像推荐个性化产品或者服务，数据处理者应当以易获取的方式向其提供拒绝的有效途径。

不得向未满 14 周岁未成年人进行个性化推荐

《条例》将未满十四岁未成年人的个人数据视作敏感个人数据，首次在国内立法中明确，除为了维护未满十四周岁未成年人的合法权益且征得其监护人明示同意外，不得向其进行个性化推荐。

“人脸识别”不能强制使用

为了在拓展生物识别技术应用的同时，避免生物识别数据的滥用，《条例》对处理生物识别数据作出更严格的规定——除了该生物识别数据为处理个人数据目的所必需且不能替代外，应当同时提供处理其他非生物识别数据的替代方案。

公共数据应当最大限度免费开放

《条例》设计了公共数据治理的顶层框架，要求政府建立城市大数据中心，实现对全市公共数据资源统一、集约管理。明确公共数据以共享为原则，不共享为例外，建立以公共数据资源目录体系为基础的公共数据共享需求对接机制。

《条例》明确将提供教育、卫生、社会福利、供水、供电、供水、环保、公交等公共服务的组织纳入公共管理和服务机构范围，其在提供服务过程中产生、处理的数据均属公共数据。公共数据应当在法律、法规允许范围内最大限度地开放，不得收取任何费用。

大数据“杀熟”最高可罚五千万元

《条例》明确规定，市场主体不得使用非法手段获取其他市场主体数据，不得非法收集其他市场主体数据提供替代性产品或者服务，不得通过数据分析无正当理由对交易条件相同的交易相对人实施差别待遇。违反上述规定拒不改正的，处五万元以上五十万元以下罚款，情节严重的，处上一年度营业额百分之五以下罚款，最高不超过五千万元。

数据立法必不可少

数据安全尽管表面看来似乎不会为企业 / 国家创造直接效益。但是当发生了重大事故时才想起数据安全防护的重要性？对现代社会来说，数据安全已经渗透到生活的方方面面，安全管理早已上升到国家战略层面，成为关系国家命脉的重要组成部分，由此可见，数据立法必不可少。亿赛通也时刻以保护国家、企业、个人的信息安全为己任，坚持做好中国数据安全专家。

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。

重点点名 Uber，数据安全就是国家安全

从近期种种合规行动中可以发现，网安行业的舆论漩涡中心依旧是数据安全。而交通出行行业由于其涉及庞大的用户数据、地图数据，成为数据安全的又一焦点聚集地。

我们今天要谈到的主角，是 Uber。其由于一件数据泄露“陈年旧案”，第四次遭到了安全控告。

近日，澳大利亚信息专员办公室（Australian Information Commissioner，OAIC）发布了一份关于其对 Uber 2016 年发生的一件极具争议的违规事件的调查报告，确认 Uber 侵犯了超百万澳大利亚人的隐私。

前几年，有黑客成功入侵 Uber 数据库并窃取 5700 万全球用户和司机的数据。泄露的数据包括 Uber 客户的姓名、电子邮件地址和电话号码，以及 700 万司机的个人信息和 60 万个驾照号码。

针对上述事件，OAIC 表示，Uber 的违规行为包括：

• 没有采取合理措施保护个人信息免受未经授权的访问；

• 未删除或去识别化那些不再需要的基于特定目的的个人信息。

Uber 被要求建立一项信息安全计划，并设专人负责。该计划需有能力识别澳大利亚用户信息面临的安全性、完整性风险，比如信息丢失、被未经授权访问等。并且要求对员工进行培训。

Uber 对此在声明中表示：他们已经进行了技术更新，包括为其核心乘车业务信息系统获得 ISO 27001 认证，以及更新了其内部安全政策，并将与第三方评估机构合作，实施进一步的改变。

针对这次事件，Uber 在近几年陆续因该事件受到了来自美国、英国和荷兰的处罚。

1. Uber 与美国 50 个州和哥伦比亚特区的总检察长达成了 1.48 亿美元的和解，并且承诺之后的数据处理将更加透明。

2. 英国对 Uber 罚款 385,000 英镑（约 529,000 美元）。

3. 荷兰的数据保护机构也对 Uber 罚款 60 万欧元（约 70.7 万美元），因为没有在 72 小时内对此事件进行报告。

Uber“四处受罚”的原因是由于其全球性的结构。在不同的当地法律下，其所触犯的法规、所遭受的处罚也不相同。因此，在 OAIC 控告其违反澳大利亚《隐私法》时，Uber 曾辩称，它并不受该法的约束，因为它已将澳大利亚人的个人信息转移到美国。

然而，现公布的报告让 Uber 认清了澳大利亚《隐私法》要求：当澳大利亚人向一家公司提供个人信息时，他们会受到《隐私法》的保护，即使这些信息在公司集团内被转移到海外。

如今，数据已经成为全球最为关注的技术相关要素之一，其重要性也在个人、企业、政府等各方面所体现。我们享受数据带来的便利太久，却还未对其背后的安全风险有足够的重视。即便《数据安全法》将于今年 9 月开始施行，不少企业对于数据安全的概念仍旧停留在如何通过审查，而不是如何保护数据。更何况，光有企业的努力是远远不够的，个人的数据安全意识也有待提升。亿赛通也时刻以保护国家、企业、个人的信息安全为己任，坚持做好中国数据安全专家。

新闻来源于网易

不同主体的数据安全法解读系列

典型案例 TYPICAL CASES

上海联影医疗科技有限公司

客户简介

上海联影医疗科技有限公司是专业从事高端医疗影像设备及其相关技术研发、生产、销售的高新技术企业。联影筹建于 2010 年 10 月，总部位于上海嘉定，是国内唯一一家产品线覆盖全线高端医疗影像设备，并同时拥有全球领先的核心技术、雄厚资本实力及顶尖人才优势的集团。

需求背景

作为医疗影像设备制造的高新技术企业，联影的核心文档安全是企业极其重视的部分，专利发明、产品著作权、设备设计图稿等都是公司的重要资产。联影为提高企业内部数据的安全性，实现办公文档内容流转安全可控，文档脱离公司管理平台后能有效防止文件的扩散和外泄，需要建立一套完善的安全管理系统。

解决方案

智能加密：智能语义识别根据文档内容进行策略匹配，判断是否为企业核心机密数据，自动筛选进行加密处理;

内容安全防护：防止核心数据通过复制拖拽、截屏录制打印输出以及副本另存等方式泄密；

安全分级控制：实现人员密级、数据密级的安全分级管理控制，满足组织数据分级安全管理要求；

终端防护：确保核心机密数据的内部安全使用、防止数据有意无意泄露，从源头保护数据文档；

审计报表：提供统计分析能力，实现安全现状可度量、事件可追溯、态势可查询；

数据安全传输：数据始终以密文形式传输、存储和使用，保障传输过程中的安全；

权限控制：文档全生命周期管理，如阅读次数、阅读时限及过期自动销毁等保护。文档协同权限、还原及文档内容保护、打印水印等控制。

项目成果

部署加密软件后，联影实现了公司内部文件可以在所有涉密终端上无障碍流转，方便业务交流，安全、高效的完成各项工作，大大的提高了工作效率。同时在数据资产安全保护方面，有效的防止了内部核心信息非法授权阅览、拷贝、篡改等，以达到既防止文档外泄和扩散，又支持内部知识积累和文件共享的目的。

江西济民可信集团

客户简介

江西济民可信集团 1999 年正式创建，是以医药为核心、健康地产和医疗康复产业为两翼的大型健康产业集团。集团现有员工 12000 余人，总部位于中国南昌，在江西、北京、上海、江苏、浙江多地设有产业平台和研发机构。2018 年营收突破 300 亿元，跻身中国制药工业 100 强第 6 位、蝉联中国医药工业 100 强第 10 位。

典型案例 TYPICAL CASES

需求背景

集团各区域分支的地理分布决定了数据管理者的管理思路，另外再加上早期出现了几起移动设备的丢失并造成了一定的影响，更加使济民可信的管理者坚定部署数据防泄密管理系统的决心。

解决方案

1. 文档透明加密系统

文件加密：对文档进行高强度加密和对使用者透明解密。实现盗走了，拿走了，没法用；操作简单，应用方便，现场无痕；

外发控制：对外发文件能控制文件的打开方式、权限控制、操作记录；

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

审计报表：实现对身份、操作行为的完整记录、报表分析与查询，以便审计。

2. 文档外发管理系统

文档加密：采用高强度加密技术对外发数据进行加密保护，防止非法用户暴力破解泄密；

身份认证：外发文档提供多种安全身份认证机制，包括：密码口令认证、机器绑定认证、硬件 USB-KEY 认证及混合认证等，在身份认证通过后才可正常、安全打开外发文档；

权限控制：外发文档提供细粒度权限控制保护，包含文档使用权限如只读、打印、修改等控制；

文档生命周期管理：阅读次数、阅读时限及过期自动销毁等保护；文档协同权限如修改、还原以及文档内容保护、打印水印等控制；

内容防护：为防止使用者恶意将文件内容扩散，系统对其内容进行高强度安全控制，如内容剪切保护、禁止截屏、禁止另存为及打印控制等。

项目成果

通过部署文档透明加密系统和文档外发管理系统后，让江西济民可信集团庞大的工作业务系统的数据得到优化管理，无论其内部、外部威胁环境都无法窃取企业敏感的医药数据，让集团所有员工都能够高效的进行安全工作。