个人信息超范围收集与泄露问题分析研究报告

中国网络空间安全协会

中国消费者协会

新华网

2025 年 3 月

编者按

中国网络空间安全协会是由中央网信办主管的网络空间安全领域的全国性社会组织，中国消费者协会是依法成立的对商品和服务进行社会监督的保护消费者合法权益的社会组织，新华网是国家通讯社新华社主办的综合新闻信息服务门户网站。

面对个人信息超范围收集、泄露等违法违规处理个人信息问题的挑战，中国网络空间安全协会、中国消费者协会、新华网在“国际消费者权益日”之际，编制了《个人信息超范围收集与泄露问题分析研究报告》，旨在唤起社会各界对这一问题的进一步关注和重视，为企业、法律从业者和广大网民提供参考，共同构建更加安全、可靠、透明的个人信息处理环境，让个人信息在数字空间中得到进一步的尊重和保护。

本报告聚焦个人信息超范围收集和泄露问题，结合已经处置的 11 个典型案例，**一是**梳理了个人信息超范围收集与泄露的整体情况，提出目前个人信息超范围收集和泄露的典型问题，包括个人和企业能力与信息不对称加剧信息滥用、技术防护不足导致泄露频发、海量数据汇集放大泄露后果等；**二是**从企业、个人和技术三个层面指出个人信息超范围收集和泄露的原因，分别是企业合规缺位与安全管理缺失、个人判断能力欠缺与寻求救济困难、保护与利用在技术上存在冲

突等；**三是**建议通过加强个人信息保护宣传教育、建立健全平台用户投诉机制以及开发“一键关闭权限”功能等技术手段，破解个人信息超范围收集和泄露的难题。

引言

个人信息超范围收集是指信息收集者在未经用户明确同意，或超出为实现特定服务目的所必需的范围，收集与业务无关或超出最小必要限度的个人信息。而**个人信息泄露**是指因安全措施不足、人为过失或恶意行为导致个人信息被未经授权访问、公开或非法传播，造成隐私或安全风险。个人信息超范围收集与泄露主要发生在互联网应用、金融、医疗、教育等重要领域，其中互联网应用领域问题尤为突出。

个人信息超范围收集与泄露的危害体现于社会、企业和个人三个层面:

在社会层面，由于个人信息安全风险具有溢出性、扩散性，超范围收集和泄露个人信息易导致公共安全遭受威胁。不法分子可能利用相关个人信息实施电信诈骗、网络攻击等犯罪活动，破坏社会秩序，一些个人信息可能被境外势力用于间谍活动，危及国家安全。

在企业层面，个人信息泄露不仅会严重损害企业商誉，导致客户信任下降、市场份额流失，还会增加企业在信息安全治理、合规整改等方面的成本，威胁企业可持续发展。

在个人层面，超范围收集和泄露个人信息易导致敏感个人信息被滥用，加剧个体在网络环境中的风险暴露，威胁个人的人格尊严和人身、财产安全。

目录

第一章 个人信息超范围收集与泄露的典型问题

一、个人与企业能力和信息不对称加剧信息滥用

在各种个人信息超范围收集与泄露问题中，个人信息滥用现象愈发严重。此类问题的根源在于个人与企业之间能力和信息的高度不对称性，即企业或机构与个人在技术能力、知识储备和资源获取上的差距，具体表现为以下两种情形。

一是技术能力差异导致信息收集失衡。企业和机构凭借其技术能力，能够轻易收集用户的个人信息，而普通用户由于缺乏技术知识，难以有效阻止。技术能力的差距使得个人信息处理者在信息收集过程中占据主导地位，用户往往处于被动接受的状态。

> **案例 1**：2023 年 9 月，某学术平台在用户进行文献检索、下载时，未经用户同意便收集其浏览记录、搜索偏好等信息，用户难以及时察觉并阻止其收集。

个别互联网应用通过过度索要权限的方式，迫使用户在功能使用和个人隐私之间做出妥协，进一步加剧了信息收集的失衡。

> **案例 2**：2024 年 5 月，某词典软件在不通知用户的前提下，其系统自动为客户默认勾选“已阅读并同意服务条款和隐私政策”的选项，若用户拒绝，系统将会自动闪退，无法正常使用。

二是知识储备差距引发信息认知偏差。企业和机构在法律和技术相关知识方面占据优势，而普通用户对此了解有限，导致双方对信息处理的认知能力存在显著差距。一些企业在隐私政策中使用复杂的专业术语，使得用户难以理解其真实含义，从而在不知情的情况下同意信息收集。这种认知偏差使得用户无法有效保护自身权益，甚至未能意识到自身信息被滥用。

案例 3：2024 年 1 月，某餐饮企业软件在个人信息收集环节，强制索取精准位置信息，由于用户普遍缺乏相关法律知识，既未意识到自己拥有拒绝提供信息的自主选择权，也不了解这种强制索取行为是否符合法律法规，最终只能被动接受。

上述个人信息收集方式不仅侵犯了用户的相关权利，还可能导致用户的隐私被过度暴露，甚至被用于商业分析或其他未经授权的用途，进一步加剧了个人信息滥用的风险。

二、企业技术防护不足导致泄露频发

技术防护不足也是个人信息泄露的主要诱因之一，具体表现为以下三类情形:

一是技术防护短板凸显。技术防护是保障个人信息安全的关键所在，但一些企业和机构在此方面存在明显不足。数据库加密是防止数据泄露的基础措施，但有的企业未能落实

这一基本防护手段，暴露出其在数据安全技术应用上的严重缺陷。

数据库加密只是技术防护的起点，其他如数据脱敏、访问控制、入侵检测等技术手段同样十分必要。然而，一些企业由于技术投入不足或安全意识薄弱，往往忽视这些关键环节，导致数据泄露事件频发。此外，由于网络攻击手段不断升级，传统的防护技术已难以应对复杂的威胁环境，企业和机构亟须加强技术研发和创新，构建多层次、全方位的安全防护体系。

二是管理漏洞引发危机。数据管理漏洞往往源于企业对信息安全的重视程度不足，未能建立完善的管理制度和监督机制。例如，个别企业未制定明确的数据分类分级标准，导致敏感数据与非敏感数据混同管理；未实施严格的权限控制，导致员工可以随意访问超出其职责范围的数据；未建立有效的审计机制，导致数据泄露事件发生后无法追溯责任。这些问题不仅增加了数据泄露的风险，也削弱了企业的整体安全防护能力。

案例 4: 2023 年 11 月，某药房内部人员利用管理漏洞盗卖客户数据，根源在于缺乏全流程的数据管理制度。从数据采集、存储、使用到传输的各个环节，均存在泄露风险。该药房未能严格限制和监控员工的数据访问权限，导致内部人员轻易获取并出售大量客户信息。

三是责任逃避加重风险。在个别政务系统的合作项目中，合作方不履行个人信息保护和数据安全义务极易直接导致信息泄露风险现实化。

> **案例 5：**2023 年 9 月，某政务系统的承包商在测试数据时未履行安全义务，导致大量公民的个人身份信息和社保记录等敏感数据泄露。

政务系统涉及的数据安全性至关重要，但承包商在测试过程中未采取有效的安全措施，使得这些关键数据暴露在风险之中。一旦这些数据被滥用，将严重损害政务系统公信力和公民权益，甚至可能引发社会不稳定因素。责任逃避不仅体现在合作方的安全义务履行不到位，还体现在企业和机构在数据泄露事件发生后的应对不力。例如，个别企业在发现数据泄露后，未能及时向公众披露信息，导致用户无法采取有效的补救措施，同时未能积极配合监管部门调查，导致事件处理进展缓慢，造成更为严重的后果。

三、海量数据汇集放大泄露后果

一是海量数据集聚放大安全管理挑战。由于信息化的普及与数据的规模效应，个别个人信息处理者掌握的个人信息量级极大，数据规模的扩大一方面加大了安全管理的难度，另一方面也催生了安全风险的聚集。

当个人信息处理者的服务器遭受攻击时，大量数据将在

短时间内被整体盗用，导致用户的各类信息被不法分子获取，一方面使得大量信息主体直接暴露在隐私泄露和诈骗等下游损害的风险中，另一方面大量信息被用于恶意数据分析后产生的新信息更是可能危及公共安全。

二是大量数据交互暴露安全防护薄弱环节。数据接口作为信息交互的关键通道，一旦存在漏洞，便可能导致信息泄露事件的发生。数据接口是不同系统、平台或应用程序之间进行数据传输和共享的桥梁，无论是企业内部系统之间的数据交换，还是与外部用户或第三方服务之间的数据交互，都需要通过数据接口实现。由于数据接口需要对外开放以实现信息交互，其暴露在外部环境中的特性使其更容易成为攻击目标。

数据接口的漏洞可能源于设计缺陷、配置错误或未及时更新安全补丁，攻击者可以利用这些漏洞绕过安全防护，直接获取敏感数据。此外，随着云计算和微服务架构的普及，数据接口的数量和复杂性不断增加，进一步加大了安全管理的难度。因此，企业需要加强对数据接口的安全防护，采用多层次的安全策略，确保数据在传输和共享过程中的安全性。

三是漏洞响应机制滞后加剧风险聚集传导。一方面，漏洞的发现和修复需要技术支持和时间，在此期间，数据泄露的风险将持续存在。由于数据接口的复杂性和多样性，漏洞的检测和修复往往需要专业的技术团队和大量的时间投入。

然而，在漏洞被发现之前，攻击者可能已经利用漏洞获取了大量敏感个人信息，给企业和用户带来了不可挽回的损失。另一方面，泄露数据造成的个人信息失控风险往往具有不可逆性，即便漏洞被修复，泄露的数据仍可能被不法分子长期利用。

第二章 个人信息超范围收集与泄露的成因

个人信息与社会经济的深度融合，使得个人信息超范围收集与泄露问题呈现多因交织的复杂态势，其成因在企业层面、个人层面和技术层面均有体现。本部分将分别在各层次剖析成因，以便在后续治理中精准施策。

一、企业层面：企业合规缺位与安全管理缺失

在数字经济时代，企业作为推动国民经济发展的重要组织形态，一方面需要掌握庞大的数据资源以开发利用，另一方面也需要担负起法律赋予的保护用户个人信息之职责。从企业层面来看，个人信息超范围收集与泄露存在合规制度缺位与安全管理缺失两大成因。

（一）企业合规制度缺位

企业合规制度是企业依法、长久、健康经营的重要保障。在个人信息处理活动中，企业合规的缺位表现在三个方面：

一是个别企业合规制度不够完善，难以全面满足合规要求。个别企业即使存在合规制度，但其制度也不能完全实现法律法规对个人信息保护的全部要求。例如，在收集环节，个别企业未清晰界定收集个人信息的目的、方式和范围，或者缺少可供参考的执行标准，从而导致技术人员收集了用户地理位置、通讯录、行踪轨迹等非必要的个人信息，这并不符合《个人信息保护法》的目的限制原则和最小必要原则的要求。此外，个别企业对告知同意、敏感个人信息处理、个

人信息跨境提供等规则的转化执行也不能达到法律的要求，在推出新的业务模式、产品或服务时，缺乏对数据来源、存储位置、技术安全等的合法合规审查，风险意识淡薄，欠缺风险评估机制。

二是个别企业合规制度浮于表面，事后审查流于形式。相较于行政监管机关和用户个人，个别企业近乎处于技术、信息的绝对垄断地位。面对行政机关，这些企业利用信息不对称的优势，制定具有合法外观的个人信息保护合规制度以应对行政监管。面对用户个人，个别个人信息处理者制定的合规制度表面上似乎优先考虑个人信息保护问题，但实际上内部操作方式仍存在向用户隐瞒其超范围收集个人信息等不合规行为。

三是有些企业应急响应机制不健全，落实执行存在困难。个别企业缺乏应对个人信息泄露事件的有效应急响应机制，不能及时发现信息泄露的情况，从而导致泄露范围不断扩大，或者在发现泄露后不能合理评估风险程度，没有及时明确地通知用户、报告监管部门，从而导致发生严重的个人信息泄露事件。也有企业虽然制定了应急响应机制，但却在实践中不真正落实，在履行个人信息泄露通知的义务上不合理地利用《个人信息保护法》第57条第二款规定的“自由裁量空间”，即“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”，

在发生个人信息泄露事件时倾向于内部“消化”，以维护企业声誉、避免企业商业价值受损。

（二）安全管理缺失

在个人信息处理活动中，企业的安全管理缺失体现在四个方面:

一是个别企业过度追求数据资产化利益。在数字经济时代，企业将用户数据视为核心生产要素，形成数据“收集—加工—变现”的闭环商业模式，这种资产化进程容易导致企业过度追求个人信息利用而忽视个人信息保护。例如，在激烈的市场竞争中，个别企业为了追求短期商业利益，过度依赖个人信息进行精准营销和市场分析，认为收集的个人信息越多，就能更好地了解消费者需求，从而在市场竞争中占据优势，却忽视了超范围收集个人信息可能带来的法律风险和社会危害。

二是个别企业员工行为管理存在漏洞。虽然个别企业制定了个人信息保护合规制度，但在实际执行过程中存在严重漏洞。例如，员工未严格遵守数据访问权限规定，导致他人能够获取超出其权限的个人信息；员工离职后，未及时回收与处理其使用的存储有个人信息的设备，增加了信息泄露风险；员工与外部人员恶意串通，倒卖公司收集、存储的个人信息，造成个人信息大规模泄露等。

三是个别企业与第三方合作缺少个人信息保护安全管

理。实践中存在大量由合作方故意或者过失泄露个人信息的情况，除了泄露者的责任，委托方有时也存在安全管理缺失问题。例如，个别企业在与第三方合作时，未提前审查第三方个人信息保护能力，或者在合同中仅模糊规定所提供的个人信息“不得用于约定外用途”，但缺乏违约赔偿细则，又或者提供个人信息后未能持续追踪第三方个人信息保护情况。

四是个别企业数据全生命周期管理缺位。实践中个别企业将安全管理的重点放在个人信息收集、存储、使用等环节，往往忽视对历史数据的管理和删除。个别企业没有建立明确的历史数据自动删除机制，当用户注销账户要求删除个人信息时，企业无法及时响应或操作繁琐，导致用户的删除请求难以实现。还有个别企业虽然声称会定期删除过期数据，但实际执行不到位，大量已无法实现处理目的的个人信息长期存储在数据库中，容易导致历史数据大规模泄露事件的发生。另外，在数据销毁过程中，缺乏专业的技术手段和监督机制，数据可能未被彻底销毁，仍有恢复的可能，这为不法分子获取信息提供了可乘之机。

二、个人层面：判断能力欠缺与寻求救济困难

（一）信息主体认知不足导致“同意”形式化困境

在现有“同意”机制下，个人信息主体难以有效认知该软件或平台收集与使用的个人信息的类型、范围、方式，如

街头自动售卖机诱导用户进行刷脸支付并收集无关信息。对于绝大多数不具备专业知识的用户而言，识别判断产品或服务所必需的个人信息之边界几乎是不可能的，即使是现有的法律明文之边界也与实践中的具体信息数据类型难以完全对应。这使得用户在面对复杂的个人信息处理规则时处于信息不对等的劣势地位，无法真正理解个人信息将被如何使用并作出合理决策。

（二）个别企业捆绑授权模式削弱用户选择权

《信息安全技术-个人信息安全规范》（GB/T 35273-2020）第 5.3 条要求，个人信息控制者不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求。但在现实中，大量的平台与应用软件采用“全选同意”“一次性授权”的授权方式。

案例 6： 2023 年 6 月，某银行软件强制用户同意隐私协议，不同意隐私政策就无法使用，只能退出 App。

上述“默认勾选”“捆绑授权”的设计不仅进一步削弱了用户对所收集数据与核心功能之关联性的判断能力，甚至在一定程度上阻碍了个人信息主体行使知情权与选择权。用户往往出于使用产品或服务之需要，在不知情的情况下被迫同意超必要范围之信息的收集与使用。此外，“一键授权”

的操作习惯将导致用户对权限请求的敏感度下降，个人信息主体意识在重复、机械的习惯性授权过程中逐渐淡化。

（三）技术复杂性与后果滞后性加剧安全风险

由于个人信息处理具有技术专业性与后果滞后性的特征。前者使得普通用户在信息量爆炸、地位不对等、“算法黑箱”中迷失，无法洞悉个人信息处理之细节；后者导致超范围使用的可能危害并非即时显现，其潜在风险难以在授权处理信息之初被准确预估。在此种认知偏差的驱使下，个人极有可能为了一时之便利而将隐私问题抛诸脑后，对超范围收集行为放松警惕，从而为后续的信息安全埋下隐患。

（四）个人信息主体救济困难助长违法行为

个人信息超范围收集与泄露情况还呈现出无形性、隐蔽性、广泛性的特征。在已有的涉信负面案件中，所牵连的主体往往动辄数以万计，且分布范围不受地域限制。

案例 7：2022 年 2 月，某虚假知识竞赛平台泄露事件中，近 350 万学生的个人信息被第三方诈骗团伙所掌握。

由于个人信息权益难以进行精确的估值作价，司法实务中对因个人信息侵权所导致的精神损失也尚无精准的计算方法，被害者难以得到相应的赔偿。此外，个人信息违法行为造成的下游损害也因网络加害行为取证难度大、身份定位难，个人即使上报公安机关也难以追踪到“真凶”，不但损

失难以追回，还因后续个人信息可能被持续不当处理而产生不安定感。尽管当前公益诉讼的范围已拓展至个人信息保护领域，但分属于不同个案中的受害者在遭遇个人信息泄露时常处于孤立无援的境地，这无疑是此类案件频发的重要因素，迫切需要畅通个人通过诉讼手段维权的渠道。

三、技术层面：保护与利用在技术上存在冲突

（一）数据收集技术层面的原因

一是个别企业缺乏明确的技术规范和标准。在当前的技术环境下，对于个人信息收集的技术规范和标准尚不完善。一些企业和机构在收集个人信息时，缺乏明确的指导原则和操作规范，导致收集行为随意性较大。

> **案例 8：**2022 年测评发现，个别儿童智能手表使用的操作系统过于老旧，旧版本操作系统默认授予 App 权限，无需用户授权，从而导致儿童的位置、通讯录、人脸画像等隐私信息被轻松获取。

二是个别企业数据收集技术的过度应用。随着大数据、人工智能等技术的发展，数据收集技术得到了广泛应用。然而，一些企业和机构为了获取更多的个人信息，过度依赖数据收集技术，导致个人信息被超范围收集。

案例 9： 2023 年 1 月，某互联网借贷公司伪装成正规借贷公司在搜索引擎、网络短视频平台等发布广告，吸引有贷款需求人员填写公民个人信息后，在当事人未授权的情况下，通过代理将相关信息出售给贷款人归属地的贷款公司牟利。这些公司利用技术手段广泛收集个人信息，远远超出了正常借贷业务所需的范围。

三是个别企业存在技术漏洞导致的个人信息收集失控。数据收集系统中存在的技术漏洞也是导致个人信息超范围收集的重要原因。一些企业和机构在开发数据收集系统时，由于技术水平有限或安全意识不足，未能充分考虑系统的安全性和稳定性，导致系统存在漏洞。

案例 10： 2023 年 8 月，某网站存在数据泄露问题，网站约 22 万个人信息数据被挂在境外论坛售卖。经查，涉案公司主要提供网上咨询服务，建设有一网站，在日常工作中收集了个人和企业等大量公民信息，但未能按照有关等级保护工作要求落实网络安全保护主体责任，因而导致个人信息泄露。

（二）数据存储技术层面的原因

一是个别企业的存储技术存在安全性隐患。目前，一些企业和机构在存储个人信息时，采用的存储技术存在一定的安全隐患。传统的数据库存储方式容易受到黑客攻击、数据

泄露等威胁。此外，一些企业在存储个人信息时，没有对数据进行分类管理，将敏感信息和普通信息混在一起存储，增加了信息泄露的风险。

二是个别企业的存储设备和系统的老化与维护不善。随着时间的推移，存储设备和系统会逐渐老化，性能下降，容易出现故障和安全漏洞。一些企业和机构为了节省成本，未能及时对存储设备和系统进行更新和维护，导致存储设备和系统存在安全隐患。

三是个别企业采用云存储带来的安全风险。云存储作为一种新兴的存储方式，具有成本低、可扩展性强等优点，得到了广泛应用。然而，云存储也带来了一些安全风险。一方面，云存储服务提供商的安全管理水平参差不齐，一些小型云存储服务提供商可能缺乏足够的安全技术和管理措施，导致用户的个人信息存在泄露的风险。另一方面，用户在使用云存储服务时，可能会将个人信息存储在多个云存储服务提供商的服务器上，增加了信息泄露的可能性。

（三）数据使用技术层面的原因

一是个别企业数据处理目的模糊造成数据滥用。在个人信息处理技术的应用过程中，一些企业和机构对个人信息收集、存储、使用等处理行为的目的界定不够清晰，易导致个人信息被滥用。

案例 11：某公司出于防范盗窃等目的，于 2021 年 4 月委托某信息科技公司在超市大门位置安装了一台具有人脸识别功能的摄像头，对进入超市人员进行拍照、人脸识别分析比对。该公司在经营过程中使用具有人脸识别功能的摄像头收集人脸数据图片未经消费者同意，且经营现场无明示收集脸部信息的目的、方式、范围和收集规则等，侵害了消费者个人信息依法得到保护的权利。

二是个别企业数据使用操作不规范。在数据使用过程中，一些技术人员的不规范操作也可能导致个人信息泄露。

三是个别数据分析技术的局限性。数据分析技术在个人信息的使用中发挥着重要作用，但目前的数据分析技术也存在一定的局限性。一方面，数据分析技术可能会产生错误的分析结果，导致个人信息被误判和滥用。另一方面，数据分析技术的发展速度较快，一些企业和机构可能无法及时跟上技术的发展步伐，导致在使用数据分析技术时存在安全隐患。

综上所述，个人信息超范围收集与泄露在技术层面存在着多方面的原因，这些原因导致了个人信息保护与利用之间在技术上的张力。在数据收集、存储、使用等各个环节，都存在着技术规范不完善、技术漏洞、不规范操作等问题，这些问题不仅影响了个人信息的安全性和隐私性，也阻碍了个人信息的合理利用和数字经济的健康发展。

第三章 个人信息超范围收集与泄露的对策

《网络安全法》《个人信息保护法》实施以来，中央网信办会同相关部门出台了《App 违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》《儿童个人信息网络保护规定》《个人信息出境标准合同办法》《个人信息保护合规审计管理办法》等一系列个人信息保护相关的规章制度，在全国范围内持续开展 App 专项治理，个人信息保护治理取得明显效果。

从 2021 年至今，中国网络空间安全协会受理处理违法违规收集使用个人信息投诉举报 9.6 万条，协调 3500 余家 App 运营者进行整改。从 2018 年以来，中国消费者协会开展 100 款 App 个人信息收集与隐私政策测评活动，并通过发布个人信息保护领域消费者权益保护报告、消费警示提示等开展社会监督和消费教育。

2024 年 10 月，中国网络空间安全协会在中国消费者协会和新华网的支持下成立个人信息保护专业委员会，该分支机构主要职责是接受业务主管单位委托承担个人信息保护投诉举报的相关处理工作等。目前，网民关注较高的“App 无隐私政策”“未明示收集使用个人信息的目的、方式和范围”“一揽子授权”等问题明显改善，强制索权、无法注销账号等问题得到有效治理，网民投诉举报数量呈逐年下降趋势。但由于 App 数量庞大且频繁更新、个人信息处理场景复

杂、大数据和人工智能等新技术不断涌现，超范围收集和泄露等问题仍呈高发态势。应对个人信息超范围收集与泄露问题需要多管齐下、精准施策，既要注重安全保障，又不能忽视流通利用。本部分结合个人信息超范围收集与泄露的具体原因，建议从企业合规、个体救济、技术保障等方面多措并举应对治理难题。

一、企业合规：规范管理落实主体责任

（一）完善个人信息保护合规体系

一是制定完善的个人信息处理规则。企业应制定全面、细致且符合法律法规要求的个人信息保护制度，明确个人信息收集、存储、使用、传输、删除等各个环节的操作规范和责任分工，保证用户能够有效行使个人信息处理活动中的各项权利。在收集环节，规定收集个人信息时必须遵循“最小必要”原则，明确告知消费者收集的目的、方式和范围，并获得消费者的明确授权，坚决杜绝过度收集行为。在存储、使用、传输、删除等环节，制定全面且具有可操作性的规则，明确负责人和相关人员责任，确保个人信息被合法合规利用。

二是构建严格的内部合规审查流程。企业内部应设立独立、专业的法务或合规部门，对所有个人信息处理活动进行全方位、严格的审查，建立全流程数据安全管理机制。在项目实施前，必须确保数据来源的合法性、数据存储安全性、个人信息处理方式与隐私政策的契合性等合规要求，只有通

过严格审查的项目，方可进入实施阶段。在项目实施阶段，也应确立日常审查流程，制定严格的审查制度，落实个人信息保护合规审计要求，及时察觉并纠正潜在的违法违规行为。在项目实施结束后，应当及时审查历史数据存储的必要性，及时删除非必要的历史数据。

三是引入外部中立的合规监督力量。仅靠企业自身开展合规工作难以完全消除因利益驱动、管理漏洞等因素导致的个人信息超范围收集与泄露风险。为避免风险防范流于形式，内部的合规制度仍需要引入外部中立的力量对合规情况进行监督。**首先**，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，应当承担“守门人”义务，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；**其次**，对于敏感个人信息，平台企业应聘请外部中立的数据风险评估专业人员，定期为平台企业开展个人信息安全风险评测，出具敏感个人信息数据安全风险评估量表；**第三**，个人信息处理者还应当履行法律法规规定的个人信息保护合规审计义务。

（二）强化个人信息处理员工管理

一是规范员工操作行为准则。企业需制定严格、细致的员工操作规范，明确员工在处理个人信息过程中的具体职责与权限范围。对于涉及个人信息处理的关键岗位，务必实行最小权限原则，即员工仅能获取完成本职工作任务所必需的

最小限度的个人信息。同时，要强化对员工日常操作行为的监督与管理，通过建立详细的审计日志等方式，全面记录员工对个人信息的操作过程，以便及时发现并纠正任何违规操作行为。

二是开展全面深入的安全培训。企业应定期组织员工参与个人信息保护安全培训，全面提升员工的安全意识与业务能力。培训内容应涵盖丰富的法律法规知识、企业内部的合规制度、安全防护技术以及应急处理流程等多个方面。通过生动的案例分析、逼真的模拟演练等多元化形式，让员工深刻认识到个人信息保护的重要性，切实掌握正确的个人信息处理方法和安全防护技能。同时，要对培训效果进行科学、有效地评估与考核，确保员工真正将安全意识切实转化为实际行动。

三是加强员工职业道德教育。除了在技术和操作层面开展培训外，企业还应大力加强员工的职业道德教育，着力培养员工的诚信意识和强烈的责任感。通过举办职业道德讲座、开展企业文化建设活动等多种方式，使其自觉遵守企业的规章制度和职业道德准则。对于违反职业道德、泄露个人信息的员工，要给予严肃的纪律处分，情节严重的要依法追究其法律责任，以此营造良好的企业内部风气。

（三）健全落实应急处理安全机制

一是建立高效的信息泄露监测体系。企业要建立一套完

善、高效的信息泄露监测体系，能够及时、准确地发现个人信息泄露事件。通过实时监测系统日志、用户反馈以及相关业务数据的异常变化等多种渠道，广泛收集可能存在信息泄露的线索。利用大数据分析等技术手段，对收集到的数据进行深入分析和处理，精准识别出异常情况。

二是制定详细的应急处理预案。企业应预先制定详细、周全的应急处理预案，一旦发现个人信息泄露事件，能够立即启动应急响应机制，按照既定流程有条不紊地进行处理。首先，要迅速采取有效措施控制泄露范围，如立即关闭相关服务器端口、暂停涉及泄露风险的业务功能等。同时，组织专业的调查团队对泄露事件进行全面、深入地调查，尽快确定泄露的原因、时间、范围以及受影响的用户群体等关键信息。根据调查结果，及时、准确地通知受影响的用户，向其详细告知事件的情况以及企业将采取的补救措施。在整个处理过程中，要积极主动地配合监管部门的调查工作，如实提供相关信息，争取监管部门的支持与指导。

三是进行全面的事后恢复与改进。对于个人信息处理者作出自由裁量决定，选择不履行通知义务后，应当就其决定涉及的内部程序、考量的相关因素作出报告，提供给主要职责部门以备监管审查。在成功处理个人信息泄露事件后，企业要对受影响的数据进行全面、细致地恢复和修复工作，确保数据的完整性和可用性。同时，要对整个事件进行深入、

全面的复盘，仔细分析企业在合规制度、人员管理、应急处理等方面存在的不足之处。针对发现的问题，及时制定改进措施并加以落实，通过持续不断地改进和完善，全面提升企业应对个人信息泄露事件的能力，有效降低未来发生类似事件的风险。

二、个体救济：倾斜保护化解救济困局

（一）加强个人信息保护宣传教育

一是强化宣传教育培养保护意识。如前所述，在个人层面，公民对个人信息保护意识淡薄、个人信息处理者对信息保护的重要性与必要性认知之不足，是个人信息超范围收集和泄露现象频发在个人层面的重要原因。为了推进对个人信息的法律保护，必须通过宣传教育增强个人信息保护的意识。在移动互联网蓬勃发展的当下，相关政府职能部门应当顺应时代新需求，充分借助各类媒体平台，包括网络、新媒体、电视节目等不同渠道，广泛开展个人信息保护宣传活动。通过普及个人信息保护知识，结合典型案例的要点分析与观点展示，切实提升公民对各类非法个人信息收集行为的识别与判断能力。

二是创新宣传模式共建网络生态。《个人信息保护法》作为个人信息领域的基本法，应充分发挥其关键作用。针对该法中的告知同意制度、目的限制原则、更正删除权等核心内容的内涵与适用，可通过短视频、交互式 H5 等新媒体形

式，将专业术语转化为可视化内容，使公民能够深入理解法律在个人信息领域赋予信息主体的合法权利与信息处理者的应尽义务，让个人在参与网络活动时保持足够的警觉，充分了解涉信行为在不同阶段可能存在的风险。同时，对于侵犯个人信息权益的行为，应积极鼓励并支持公民运用法律武器维护自身权益。需要注意的是，良好的个人信息保护法治环境需要个人信息处理者与信息主体双向发力。因此，《个人信息保护法》《数据安全法》等法律规定的具体处理规则也应在宣讲教育中被重点提及，确保其切实履行个人信息安全保护义务，全面落实个人信息数据的安全保护责任，从个人信息处理者的角度助力保障个人信息安全。

（二）建立健全平台用户投诉机制

一是完善平台规则、明确投诉机制。平台作为众多经营者和消费者的重要载体，其内部个人信息保护治理的依据除《个人信息保护法》《网络数据安全管理条例》等法律法规外，主要为自身平台规则。平台规则之于平台发挥着类似于“公司章程”的作用，是平台管理平台上违法和不当行为的直接依据。企业在平台规则制定中应当结合自身业务性质，充分考虑平台中可能存在的个人信息超范围收集、滥用和泄露等情况，制订符合风险管理和救济需求的平台用户投诉规则、受理形式、处置方式，设计明确可行、便于实施的平台投诉配套机制，以便制度化、常态化开展投诉受理工作。

二是设计便利的用户投诉方式。平台对用户投诉方式的设计应当以用户为核心，告知用户举报和投诉的流程步骤、渠道方式、时间节点、所需材料，及时处理用户的举报和投诉并予以反馈。此外，平台还可借助其技术优势，通过开发风险预警系统等为用户提供技术支持。

三是引入外部监督提升投诉实效。平台的投诉处理效率应当被视为其履行个人信息保护义务、承担个人信息保护责任力度的衡量标准之一，将处理结果定期以合理形式进行公开，接受外界监督。

三、技术保障：技术手段严守保护红线

赋予用户对自己个人信息的更多控制权，是个人信息保护的重要原则之一。开发用户自主控制工具，如“一键关闭权限”“个人信息可携带权”等功能，能够让用户更加便捷地管理自己的个人信息，增强用户对个人信息保护的参与感和主动权。

一是开发“一键关闭权限”功能。在移动互联网时代，各类应用程序为我们的生活带来了极大的便利，但同时也存在着过度索取用户权限的问题。一些应用程序在安装时会要求获取大量的权限，如位置信息、通讯录、摄像头、麦克风等，而这些权限中有些并非应用程序正常运行所必需的。“一键关闭权限”功能可为用户解决这一困扰。用户可以通过简单的操作，一键关闭应用程序对某些不必要权限的访问。这

不仅可以加强用户个人信息保护，还可以减少应用程序对设备资源的占用，提高设备的性能和续航能力。此外，“一键关闭权限”功能还可以提高用户对个人信息保护的意识。当用户能够自主控制应用程序对个人信息的访问权限时，他们会更加关注自己的个人信息安全，从而促使应用程序开发者更加规范地索取用户权限，形成良好的个人信息保护生态。同时，用户也会更加积极地向应用程序开发者反馈权限使用问题，促使开发者优化应用程序的权限管理机制。这种用户与开发者之间的良性互动，有助于推动整个移动互联网应用行业更加重视个人信息保护。

二是开发“个人信息可携带权”功能。“个人信息可携带权”是指个人享有的请求个人信息处理者提供相应的途径，将其个人信息转移至所指定的个人信息处理者的权利。这一权利的赋予，使得用户在个人信息的使用和管理上拥有了更大的自主权。以社交媒体平台为例，用户在某个社交媒体平台上积累了大量的个人信息，如个人资料、好友关系、发布的内容等。当用户想要更换到其他社交媒体平台时，通过“个人信息可携带权”功能，用户可以要求原平台将自己的个人信息以相应的途径转移到新的平台中，实现个人信息的无缝迁移。一方面，“个人信息可携带权”功能有助于用户充分实现对自己个人信息的决定权，方便用户获取和利用其个人信息，同时避免在不同平台上重复填写信息可能带来的隐私

泄露风险；另一方面，“个人信息可携带权”功能还可以促进个人信息的合理流动与利用，推动数据市场的竞争和创新。当用户能够自由地转移自己的个人信息时，个人信息处理者为了吸引和留住用户，会更加注重个人信息的保护和服务质量的提升，从而推动数字经济的健康发展。