Dispute Settlement 争议解决, 2025, 11(2), 337-346
Published Online February 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.112083

Hans汉斯

小型个人信息处理者豁免义务研究

王贝宁

青岛大学法学院，山东 青岛

收稿日期：2025年1月15日；录用日期：2025年2月18日；发布日期：2025年2月28日

摘　要

在数字经济蓬勃发展的背景下，小型个人信息处理者的活动日益频繁，其豁免义务研究成为平衡企业发展与个人信息保护的关键。本文梳理国内外法规及研究，明确其收集、存储、使用共享、删除销毁及跨境规则，从合法利益、风险差异、成本效益、比例原则和优位利益豁免等理论，剖析义务豁免依据，并列举数据提供、记录、非敏感数据处理及信息处理义务豁免情形。同时，针对监管与处罚，提出运用数字化工具、监管沙盒及协同监管等优化策略，细化经济与非经济处罚措施，力求构建合理制度，促进小型个人信息处理者合规发展，保障信息权益，且随技术与环境演变持续完善该制度。

关键词

个人信息保护，小型个人信息处理者，义务豁免

Research on the Exemption Obligations of Small Personal Information Processors

Beining Wang

Law School of Qingdao University, Qingdao Shandong

Received: Jan. 15th, 2025; accepted: Feb. 18th, 2025; published: Feb. 28th, 2025

Abstract

In the context of the booming digital economy, the activities of small personal information processors have become increasingly frequent, and the research on their exemption obligations has become crucial for balancing enterprise development and personal information protection. This article sorts out domestic and foreign laws, regulations, and research, clarifying their rules regarding collection, storage, use and sharing, deletion and destruction, and cross-border transfer of personal information. It analyzes the theoretical basis for exemption obligations from the perspectives of legitimate interests, risk differences, cost-benefit, the principle of proportionality, and the theory

文章引用: 王贝宁. 小型个人信息处理者豁免义务研究[J]. 争议解决, 2025, 11(2): 337-346.
DOI: 10.12677/ds.2025.112083

of overriding interests exemption. It also lists the exemption situations such as data provision, record-keeping, non-sensitive data processing, and information processing obligations. Meanwhile, for supervision and punishment, this article proposes optimization strategies such as using digital tools, regulatory sandboxes, and collaborative supervision, and details economic and non-economic punishment measures. It strives to construct a reasonable system to promote the compliant development of small personal information processors, protect information rights and interests, and continuously improve this system with the evolution of technology and the environment.

Keywords

Personal Information Protection, Small Personal Information Processors, Obligation Exemption

1. 引言

在当今数字化浪潮席卷全球的时代，个人信息已成为重要的经济与社会资源。小型个人信息处理者如雨后春笋般涌现，在各个领域发挥着独特作用，然而其发展与个人信息保护之间的矛盾日益凸显。一方面，小型企业资源有限、技术能力不足，在面对繁杂严格的个人信息保护法规时，常陷入合规困境，沉重的合规成本可能阻碍其创新与成长步伐；另一方面，个人信息的安全与合理使用关乎公众权益，若缺乏有效监管与规范，极易引发信息泄露等风险。

对此，深入探究小型个人信息处理者豁免义务极具现实紧迫性。通过梳理国内外相关法规及学术成果，剖析其在收集、存储、使用共享、删除销毁及跨境传输等环节的规则，挖掘豁免义务的理论根基与实践情形，并谋划监管处罚优化策略，成为构建平衡企业发展与信息保护机制的关键路径[1]。这不仅有助于为小型企业营造适宜的发展环境，激发市场活力与创新动力，还能切实保障个人信息安全，维护公众合法权益，推动个人信息保护法律体系在实践中不断完善与发展，以适应数字经济的动态变化。

2. 小型个人信息处理者的核心规则架构

2.1. 收集和存储规则

小型个人信息处理者通常规模较小、资源有限，可能缺乏专业的信息安全团队和完善的技术设施，业务模式相对简单，数据处理量较小，但涉及的个人信息类型可能较为多样。所以小型个人信息处理者应当明确收集规则，明确收集行为的目的与范围，收集目的应具体、明确、合法，与自身业务紧密相关，如小型电商收集用户地址仅用于商品配送，不收集与业务无关的信息。此外，还应简化同意流程，通过采用简洁易懂的语言和交互方式获取用户同意，如弹窗提示、勾选框等，避免冗长复杂的条款。对于儿童等特殊群体，需获其监护人同意。小型个人信息处理者还要严格履行告知义务，以显著方式向用户告知信息收集的目的、方式、范围等，如在 APP 启动界面或网站首页展示隐私政策链接。

国外实践做法如下，欧盟根据《一般数据保护条例》规定，数据主体的同意必须具体、清晰，数据主体可随时撤回同意，并要求数据控制者采取安全保障措施[2]。小型个人信息处理者虽无强制设立数据保护专员要求，但也要确保数据处理合规。美国的《儿童在线隐私保护法案》及相关规则要求，面向 13 岁以下儿童的小型在线服务运营商，收集信息前应当获得家长同意，要明确告知收集信息的类型、用途等。《加州消费者隐私法案》规定，企业要向消费者明确其收集的个人信息类别，消费者有权要求企业删除

个人信息[3]。韩国的国务总理直属机构“个人信息保护委员会”会对企业个人信息收集与使用情况进行调查，违规者将被要求改正并处罚金或罚款。

小型个人信息处理者存储规则需要遵守以下要求。第一，安全措施适当化，鉴于资源有限，可采用成本效益相适应的安全措施，如使用云存储服务时选择有安全保障的供应商，定期进行数据备份。第二，存储期限合理，根据业务需要和法律规定确定合理的存储期限，如交易记录保存至纠纷诉讼时效期满后一定时间。在一定期限后，应当及时删除或处理个人信息。第三，访问控制严格，建立严格的访问权限管理制度，限制员工对个人信息的访问，仅允许必要人员在授权范围内访问，如采用多因素身份认证。

2.2. 使用与共享规则

在数字经济时代，大部分小型个人信息处理者在处理数据前，已获得用户等信息主体的同意与授权[4]。《中华人民共和国个人信息保护法》对个人信息共享限制提出明确要求。一般的个人信息方面根据第二十三条的规定，向他人提供时要告知接收方的名称或姓名、处理目的及个人信息种类等，并获取个人单独同意。敏感个人信息处理规则更严，第二十九条指出需取得个人单独同意，第三十条表明处理敏感信息时，除了要满足第十七条第一款事项外，还应告知个人处理的必要性及对其权益的影响，对处理情况进行记录。

学者们认为，这些规定有助于平衡数据共享与个人信息保护之间的关系。知情同意作为获取个人信息的合法性基础，让用户对个人信息的流向和使用有一定掌控权，从而保护其隐私和个人信息权益。事前影响评估机制是个人信息保护的重要“关口前移”措施，全面评估可能对个人权益产生的影响，有助于提前发现和预防风险，避免或减少对个人权益的损害[5]。明确个人信息共享限制和要求，有利于规范个人信息处理者行为，增强其责任意识和合规意识，促使其采取更有效的技术和管理措施保护个人信息安全。

2.3. 删除与销毁规则

《中华人民共和国个人信息保护法》对个人信息共享的边界作了明确划分。拿一般个人信息来说，按照第二十三条的要求，在将其提供给他人时，要向接收方清楚表明名称或姓名、联系手段、处理目的、处理途径以及个人信息的具体类型等内容，而且必须得到个人的单独许可。在敏感个人信息方面，其处理规则更为严苛。第二十九条着重指出，处理这类信息必须取得个人的专门同意；第三十条进一步规定，除了满足第十七条第一款所规定的事项外，信息处理者还应当向个人说明处理敏感信息的原因和后续影响。此外，第五十五条特别强调，当进行如敏感个人信息处理这类会对个人权益产生重大影响的活动前，个人信息处理者有提前开展影响评估的义务，并记录处理过程[6]。通过这些举措，切实保障个人信息在各个环节都符合安全与合规标准，全面维护个人权益，使其免受各类潜在风险的冲击，从而构建起更为稳固的个人信息保护屏障。

有学者认为，这些规定有助于平衡数据共享与个人信息保护之间的关系。在数字经济时代，数据共享虽能创造巨大价值，但也存在侵犯个人信息权的风险。知情同意作为获取个人信息的合法性基础，能让用户对个人信息的流向和使用有一定的掌控权，从而保护其隐私和个人信息权益，有助于提前发现和预防风险，避免或减少对个人权益的损害。也有学者强调，明确个人信息共享的限制和要求，有利于规范个人信息处理者的行为，增强其责任意识和合规意识，促使其采取更有效的技术和管理措施保护个人信息安全[7]。

2.4. 个人信息跨境规则

全球经济的数字化和日益增长的互联网连接相辅相成，共同推动了跨境数据的收集、使用和传输活动的迅速增加。各方都认识到，无论是大型跨国科技公司、不同领域的公司、微型、中小型企业，还是工人和消费者，值得信赖的跨境数据交流必不可少。

关于针对个人信息处理者从事跨境数据流动的有关立法，大多数国家主要通过严格的跨境数据流动审批制度和数据本地化要求的方式来实现对数据主权的维护。《个人信息保护法》与欧盟 GDPR[1] 均针对个人信息跨境传输作出了规定，体现了国家层面对域外效力的积极保护义务。在数字经济领域，数据本地化策略在不同国家有不同表现。一些数字经济欠发达的国家以及部分发达国家，如欧盟、韩国等实施有限禁止本国数据出境政策，而伊朗、印度等国家则完全禁止本国数据出境，要求数据存储于境内。中国对于个人信息跨境传输的监管主要体现在个保法与相关法律上。《中华人民共和国数据安全法》第二十七条强调数据处理者应健全数据安全管理制度，采取相应的技术措施和其他必要措施来保障数据安全。个人信息处理者跨境提供个人信息，可通过网信部门安全评估、专业机构认证、签订标准合同或遵循法定路径。小型个人信息处理者大致需要满足三步骤，参加网信安全评估、获取专业机构认证、签订标准合同明权责。同时要满足告知境外接收方信息，获个人单独同意或有合法基础，应确保境外接收方不在限制或禁止清单内。

美国联邦政府层面未出台统一的个人信息跨境立法，但 APEC“跨境隐私规则体系”(CBPR)。美国、加拿大、日本、韩国以及中国台湾等国家和地区于 2022 年联合发布全球跨境隐私规则声明，宣告全球跨境隐私规则(CBPR)论坛成立。美国商务部部长 Gina M. Raimondo 宣称，该论坛建立的 CBPR 和处理者隐私识别系统认证(PRP)，是数据隐私认证领域的首创之举，能够证明企业达到了国际认可的数据隐私标准。CBPR 体系源于 APEC，但 CBPR 将独立管理并与 APEC 体系分离。美国将 CBPR 推广至全球来提升各国政府、大型跨国科技公司、甚至中小企业的参与，强化对消费者的隐私保护。

《通用数据保护条例》对个人信息跨境传输实施严格监管，小型个人信息处理者需要遵循条例的相关规定，包括数据主体同意、充分性认定和适当保障措施。适当保障措施类如标准合同条款或约束性规则。欧盟委员会通过了新的两组标准合同条款，第一个是适用于数据控制者与数据处理者之间的数据委托处理活动，这是欧盟首个数据处理协议模板；第二个是适用于向第三国传输个人数据的情形[8]。委托处理 SCCs 条款核心要点主要包括七项，一是数据控制者向数据处理者提供处理活动指示；二是保障数据处理的安全性，尤其是实施技术和组织措施；三是处理敏感数据；四是规范次级数据处理者的使用，包括事先特定手按或一般性书面授权情形；五是进行国际数据传输；六是数据处理者协助数据控制者，如在数据主体请求、数据保护影响评估等情形；七是数据泄露通知等要求。

对于中国本土企业而言，在接受从欧盟境内传输的数据时，首先需要结合具体情况判断在个人数据跨境传输所涉情况是否可以适用 GDPR，如果不适用，则需要与数据传输方签署跨境传输 SCCs。对国外如欧盟地区企业而言，涉及从中国境内提供个人数据，要适用我国的个信法中的个人数据跨境传输的监管框架。国家网信部门在制定标准合同时可以参考新版 SCCs 的内容，区分不同的传输模式，明确传输双方的义务与责任。

约束性公司规则 [2] 是专门为跨国公司量身定制的内部数据保护政策，旨在促进个人数据跨境传输进出欧盟，符合 GDPR 要求。约束性公司规则作为具有法律约束力和可执行性的政策，为企业等个人信息处理者的个人数据传输建立了合理的框架[9]。

3. 小型个人信息处理者豁免义务的具体情形

3.1. 小型个人信息处理者信息处理义务的可豁免性的理论依据

小型个人信息处理者往往是创新的活跃力量，尤其是新兴的数字经济领域，许多创新性的产品和服

[1]《欧盟通用数据保护条例》第 44 条一般原则：规定了数据控制者或处理者将个人数据传输至欧盟以外的第三国或国际组织时，只有在确保第三国或国际组织能提供充分的数据保护水平等特定情形下，才允许进行跨境数据传输。

[2]约束性公司规则源于 GDPR 的第 47 条。

务都源自小型企业的创意和尝试。合法利益豁免能够为其提供一定的灵活性，使其在不损害用户个人信息主体权益的前提下，使用有限的个人信息资源进行产品和服务的创新研发。而对于想要进入新市场或拓展业务的小型个人信息处理者，合法利益豁免可以降低其合规门槛，在一些新兴行业或业务模式尚未完全成熟的领域，过于严格的个人信息保护要求可能会成为小型企业进入的障碍。通过合法利益豁免，它们可以在一定范围内现行探索业务可行性，积累经验并逐步完善个人信息保护措施，有利于促进市场竞争和多元化发展。

合法利益豁免突破了原有的同意机制的限制，强调信息使用价值的实现。由于个人信息权利是复合权利，并具有可拆分性。有学者认为数据权益与个人信息存在交织关系，并将个人信息权益作为“母权”，数据权利可作为“子权”[10]。这体现在小型个人信息处理者行使权利需要受制于个人信息主体的权益，信息主体不仅享有知情权和删除权，还包括同意权、更正权等多项权利。个人信息保护法侧重于确立个人信息处理的基本原则和核心权利，知情权是用户对其信息处理过程进行监督和控制的基础，而删除权则是直接关系到个人对其信息的最终处置权。对于知情权和删除权的限制进行了明确规定，因为这两项权利在实践中与信息处理的合法性、正当性以及个人权益的平衡密切相关。法律未对其他权利的限制进行一一列举，而是通过一些基本原则和规定，对权力的行使和限制提供一个相对灵活的框架，这样有利于在不同的情况下能够更好地平衡个人权益和公共利益、信息处理者的合法利益等各种因素。所以对其中某一具体权能的合理限制并不会对整个个人信息权利的行使产生根本性影响。

首先，风险差异理论，指不同主体或行为的风险性质、程度存在差异，应据此采取不同的管理和应对措施。经济学家弗兰克·奈特对风险与不确定性的区分，为风险差异理论奠定了基础。由于小型个人信息处理者数据处理规模和范围小，信息泄露等风险危害范围窄，如个体美容店记录少量会员基本信息用于预约服务，风险低于大型连锁美容机构。德国社会学家乌尔里希·贝克在风险社会理论中指出，不同主体面临的风险不同，风险的分配和管理应与主体的风险承受能力和风险特征相适应[3]，为小型个人信息处理者的风险差异分析及义务豁免提供了理论支撑。

其次，成本效益理论。小型个人信息处理者遵循严格信息处理义务成本过高，适当豁免可使其在合理成本内开展业务，效益应大于成本，如小型网店建立复杂信息安全系统和数据保护流程会不堪重负。成本效益原则作为一种广泛应用于决策制定和资源分配的基本经济原则，已被众多经济学家和管理学者所研究和倡导，虽无特定学者专注于其在小型个人信息处理者义务豁免中的应用，但在战略成本管理等领域，相关研究为该理论的应用提供了基础。

再次，比例原则要求手段与目的相适应，限制手段对权利的侵害应在必要限度内[11]。小型个人信息处理者能力有限，要求其承担与大型企业相同责任可能不公平，可根据比例原则适当豁免其义务，平衡监管要求与实际履行能力。该原则源自德国，众多行政法学者对其进行了深入研究和发展，如我国的蒋红珍教授对比例原则在个人信息保护领域的全阶式、截取式、概括式适用等进行了研究，陈征教授则从宪法角度对比例原则进行了解读。

最后，优位利益豁免理论，它与上世纪七十年代美国提出的“公平信息实践准则”有关，源于利益衡量的法学思想，当不同利益冲突时，需权衡确定更值得保护的优位利益来解决冲突。在信息控制者处理个人信息所达成的利益超越信息主体的信息权益这种情形下，即便未获信息主体同意，也能够对个人信息予以合法的处理操作。小型个人信息处理者在某些情况下，其处理信息所带来的公共利益或自身合法利益可能更优，可适用该理论豁免部分义务，促进信息流通与利用。上世纪九十年代欧盟的《个人数据保护指令》规定了合法利益豁免规则，赋予信息控制者为实现合法利益可不受知情同意规则限制处理

[3]德国社会学家乌尔里希·贝克在《风险社会》一书中，首次提出“风险社会”的概念。贝克指出风险社会建立在对“作为现代化一部分的系统性地生产出来的风险和危害怎样才能被避免、最小化或引导”这一问题的解决基础之上。

个人信息的权利，为优位利益豁免理论的形成奠定了基础，不过当时未明确提出“优位利益豁免”概念。

3.2. 豁免义务的例举

豁免小型个人信息处理者的部分数据提供义务。《关于公平访问和使用数据的统一规则》对中小微企业进行倾斜保护，对于小微企业而言，如小微企业制造或设计的联网产品及关联服务所产生的数据，无需承担企业与用户、企业与企业间的数据提供义务。就中型企业来说，《数据法案》把豁免的时间跨度限定为联网产品投入市场或开始使用后的 1 年之内。除了对中小微企业豁免其部分数据提供义务，《数据法案》还建立灰色名单和禁止合同惯例清单，从源头把控并将可能存在不公平的合同相关内容筛出来、禁止掉，让中小微企业等小型个人信息处理者不会被迫接受不合理的合同条件，从而在谈判时更有底气去争取有利的条款，增强小型个人信息处理者的议价能力。欧盟委员会后续还将制定示范合同条款，并引入一项不公平性测试，防止大型企业滥用数据共享机制，损害中小微企业的利益。

适当豁免小型个人信息处理者的记录义务。我国的《个人信息保护法》第五十五条和欧盟 GDPR 条例第三十条都提及信息处理者的记录义务豁免，主要是两方面原因，一方面是证明自身进行的个人信息处理活动的符合法律法规的要求；二是有助于在发生泄露等安全事件时快速发现原因，立即采取相应补救措施、查找相关责任人，并为日后避免类似情况提供借鉴。欧盟 GDPR 前言第 13 条规定，考虑到记录义务对微小型和中兴企业的负担，将上述法定记录义务予以特别豁免。具体而言，不需要履行记录义务的公司应当从企业雇员人数和三种数据处理活动的情形两大标准界定，一是雇员少于 250 人的公司，二是数据处理活动是偶然发生且不太可能危机任何个人的权利或自由且不涉及刑事定罪或犯罪的数据。因此，企业雇员人数少于 250 人且不存在以上三种情形之一的(无需三种情形同时存在)，才能豁免记录义务[12]。虽然雇员人数的认定标准容易，但数据处理活动存在的三种情形仍需审慎认定，具体而言，个人信息处理者处置例如工资管理、潜在客户和供应商非偶然性的数据，或者管理一些涉及敏感数据再或者是数据处理可能涉及如地理定位系统、视频监控等权利和自由时，个人信息处理者仍然需要履行记录义务。GDPR 第三十条规定记录可采用书面形式，其中也包括电子形式的书面记录。电子形式的记录因其便于企业随时添加、删除和修改文件而受到广泛推荐[13]。相比之下，纸质书面记录更合适数据处理活动变化不大的小型企业。中国个信法并未明确要求记录义务的形式，也没有规定记录的更新要求。法国数据保护机构建议企业对数据处理中的任何变化及时、定期更新。

非敏感数据信息的可豁免性。对于敏感消费者信息，小企业没有任何豁免权是毋庸置疑的，敏感信息通常包括像消费者的医疗信息、财务信息、社保号码等，这些信息一旦泄露可能会对消费者造成严重的损害，如身份盗窃、经济损失等。但是可以让小企业在处理非敏感数据方面享受一定的豁免。于 2024 年 5 月 24 日签署，并将于 2025 年 7 月 31 日生效的美国《明尼苏达州消费者数据隐私法案》规定了小企业等小型个人信息处理者在处理过程中可豁免非敏感数据信息[4]。该法案的适用主体为在明尼苏达州经营或向其居民提供商品或服务的企业，前提是该企业在一个日历年内，控制或处理至少十万名明尼苏达州消费者的个人数据，不包括仅为完成支付交易而控制或处理的个人数据。虽然没有具体说明豁免的内容，但可能包括在某些情况下，不需要像处理敏感数据那样严格的同意程序来处理非敏感数据[14]。例如，对于消费者的一般购物偏好数据(如喜欢购买的服装品牌、颜色等)，在符合一定商业用途和保障一定安全措施的前提下，小企业可能可以在没有消费者明确的每次同意的情况下，将这些数据用于市场调研或内部分析等用途。不过，这并不意味着小企业可以随意滥用这些非敏感数据，仍然要遵循基本的数据保护原

[4]2024 年 6 月 24 日，Shearman & Sterling 发布的“Minnesota Governor approves new Consumer Data Privacy Act (24 May 2024) - A&O Shearman”一文提到，《明尼苏达州消费者数据隐私法案》于 2024 年 5 月 24 日获明尼苏达州州长批准，2025 年 7 月 31 日生效，该法案豁免了符合联邦标准定义的小企业，但小企业出售敏感个人数据仍需获得同意。

则。

信息处理义务的可豁免性。除了对信息主体权利的合理限制外，还应当包括对个人信息保护原则以及信息处理者义务的部分或全部豁免。尽管取得个人同意是处理个人信息的一般原则，在满足特定条件时，信息处理者的告知义务可以被豁免。换言之，法律对个人信息处理者的义务予以部分或全部排除、豁免，实质上是对个人信息权利的一种合理限制。如果不是这些信息的直接来源者，数据处理者应当告知数据主体包括处理者的身份、联系方式、处理目的、处理事由、处理种类等信息，并且应当在不晚于获得个人数据后一个月内通知到数据主体。考虑到不需要告知的情形，GDPR 第 14 条第 5 项[5]还规定了不需要告知的例外，如数据主体已经知晓将要告知的信息、告知无法操作或者或牵涉到数据处理者的不成比例的投入。美国则通过《加州隐私法》(CPRA)等立法，排除了不符合一定条件的小型个人信息处理者的管辖范围，还提出了家庭数量的标准[15]。定量标准可以依据某段时间或某个时间点的统计值。

4. 小型个人信息处理者面临的问题

4.1. 法规遵循困境

小型个人信息处理者在遵循法规方面面临诸多难题。现行个人信息保护法规体系繁杂，条款细致入微且更新频繁，小型企业难以精准把握。以欧盟《一般数据保护条例》为例，其对数据处理的各个环节都有严格规定，小型企业解读和落实时易出现偏差。同时，小型企业资源有限，缺乏专业法务和合规团队，难以承担高昂的法规解读、培训及合规体系建设成本。在技术投入上也力不从心，无法像大型企业那样构建完善的信息安全防护体系，这使得小型企业在法规遵循上困难重重。

4.2. 豁免义务界定难题

理论层面，合法利益、风险差异等豁免义务理论虽有依据，但在实践中难以精准应用。不同理论的适用边界模糊，如合法利益豁免中，“合法利益”的范围难以明确界定，小型企业在创新业务时，很难判断自身行为是否符合要求。从豁免情形来看，现有法规和研究列举的豁免情形不够清晰[16]。在非敏感数据处理豁免中，“非敏感数据”的界定标准不统一，不同地区和行业理解存在差异，小型企业在实际操作中无所适从。

4.3. 监管处罚困境

监管手段上，传统监管方式难以满足小型个人信息处理者监管需求。小型企业数量庞大、分布广泛且业务多样，监管部门人力和技术资源有限，难以实现全面有效监管。监管沙盒等新型监管模式在应用中存在部门协调不畅、标准不统一等问题，无法充分发挥作用。处罚方面，当前处罚机制对小型企业不够合理。经济处罚若仅依据营业额按比例罚款，可能对利润微薄的小型企业造成过重负担；非经济处罚中，责令暂停业务、吊销许可证等措施对小型企业影响过大，可能导致其直接倒闭，不利于小型企业发展和市场稳定。

5. 监管与处罚机制

流行的欧洲概念将个人数据视为个人基本权利的体现，这一观念在网络空间日益频繁的当下显得尤为重要。随着人们在网络世界中进行着无数的交易和日常活动，个人信息的价值不断攀升，其处理过程

[5]GDPR 第 14 条第 5 项规定，第 1 至 4 款的规定：……提供此类信息被证明是不可能的，或者会涉及不成比例的努力，特别是对于出于公共利益的存档目的、科学或历史研究目的或统计目的的处理，需符合第 89 条第 1 款所述的条件和保障措施，或者就本条第 1 款所指的义务而言，该义务可能会使实现该处理的目标变得不可能或严重受损。在这种情况下，控制者应采取适当措施保护数据主体的权利、自由和合法利益，包括使信息公开可用……

中所带来的风险也日益受到关注。布鲁塞尔效应，指欧盟凭借自身所具备的单方面市场规制力量，在缺乏其他国家以及国家机构配合协作的条件下，依然能够制定出全球市场遵循的规章制度，从而在全球范围内产生影响力的现象。

布鲁塞尔效应的本质是一种“市场驱动的协同效应”，其影响范围广泛，涉及数据隐私、消费者健康和安全、反垄断等多个领域。它使欧盟在国际规则制定方面具有重要地位，其规则和标准被许多国家和国际组织借鉴和采用[6]。不过，对于布鲁塞尔效应，也存在一些争议和挑战。对于小型个人信息处理者来说，这意味着他们需要更加关注欧盟的法规动态[17]。一方面，这些政策和标准可能会对小型个人信息处理者的业务产生直接或间接的影响。《通用数据保护条例》对个人数据的保护提出了很高的要求，小型个人信息处理者可能需要调整其数据处理方式和流程，以确保符合欧盟的标准。另一方面，合规成本将增加，由于欧盟的监管政策严格，小型个人信息处理者为了遵守相关规定，可能要增加了合规成本。这包括技术投入、人员培训、审计等方面的费用。例如，为了满足 GDPR 的要求，小型处理者可能需要购买更高级的加密技术来保护数据安全，或者聘请专业的数据保护顾问来确保合规性。再一方面，布鲁塞尔效应可能会导致市场准入门槛提高，同样对个人信息保护的要求也提高。对于小型个人信息处理者来说，这意味着他们在进入国际市场时，需要面对更高的市场准入门槛。例如，一些国际客户可能会要求供应商必须符合欧盟的 GDPR 标准，否则将拒绝合作。这就要求小型处理者在开展业务时，要充分考虑到欧盟市场的需求，提前做好准备。在这种背景下，小型个人信息处理者需要深入了解并遵守相关规定，以确保自身的合法运营。

5.1. 监管策略优化

运用数字化新型监管工具，建立个人信息监管平台。及时要求小型个人信息处理者将个人信息处理活动的相关数据实时上传至平台，监管部门通过平台进行数据分析和风险监测。根据小型个人信息处理者的行业类型、数据处理量、风险程度等因素进行分类，采用分类监管模式，根据小型企业的行业类型、数据处理量、风险程度等因素进行分类，对高风险企业加强监管力度和频率，反之则适用宽松方式。例如，对于涉及大量敏感个人信息(如医疗健康、金融数据等)处理的小型企业，如小型私人诊所、小额贷款公司等，实行定期与不定期检查相结合方式。而对于仅处理少量普通个人信息的小型企业，如社区的便利店，可以采用定期报送合规报告、随机抽查的方式进行监管。

2015 年英国金融行为监管局首次提出“监管沙盒”理念[7]，于金融科技领域而言，其在风险管控与创新激励层面展现出了极为重要的借鉴价值，由此收获了广泛关注。在国际范围内，该模式也大受欢迎，新加坡、中国香港以及澳大利亚等诸多国家和地区均结合自身实际状况加以借鉴与应用。部分研究者更是指出，监管沙盒极有可能成为支撑监管科技 3.0 版本的理想路径。

监管沙盒由过去以防范和补救消费者合法权益受到侵害为目的“防御型”保护模式像促进消费者利益增加的“进取型”保护模式转变。通过有效整合市场监管部门在规范市场秩序方面的专业优势、网信部门对网络空间的管控能力以及公安部门强大的执法力量等多部门资源，打破部门壁垒，实现信息共享与行动协同，凝聚成的监管合力，从而确保监管工作的全面性、精准性与权威性，为市场的健康稳定发展筑牢坚实根基[8]。例如，市场监管部门在日常企业经营检查中发现个人信息处理违规线索后，及时移交。

[6]欧洲数据保护委员会(EDPB)等官方机构发布的指南和解释文件，会对 GDPR 的具体要求和适用情况进行详细说明，其中也会提及小型个人信息处理者在数据保护方面的义务和需要做出的调整。

[7]来源于英国金融行为监管局官网：作为“监管沙盒”理念的提出者，英国金融行为监管局(FCA)的官方网站上有关于 2015 年首次提出“监管沙盒”理念的相关文件和报道，对其在金融科技领域的应用及目的等有详细说明。

[8]《解读美国消费者金融保护局的“监管沙盒”》https://mp.weixin.qq.com/s/ZE91mdcbF2KDP7M6ckmanA

5.2. 处罚机制细化

发生个人信息泄露、篡改、丢失的情况时，个人信息处理者必须即刻采取相应的补救举措，同时要切实履行通知相关方的义务。如果个人信息处理者所处理的个人信息数量达到了国家网信部门所明确规定的标准，那么其就有责任设立专门的个人信息保护负责人一职，以确保个人信息在处理过程中的安全性与合规性，最大程度地保护信息主体的合法权益免受侵害，维护个人信息处理活动的正常秩序。但是小型个人信息处理者一般人数和规模较少，不需要引入个人信息保护负责人。处罚机制因其直接涉及到对小型个人信息处理者的权利限制而成为关注的重点。《个人信息保护法》在第七章规定了法律把责任，对违法处理个人信息保护义务且情节严重的个人信息处理者，采取“双罚制”[18]，对个人信息处理者的违法行为的责任追究体系十分完整，涵盖了民事、行政与刑事领域。除了常规的罚款、停业整顿、吊销许可证等行政处罚手段外，个信法还规定了相关的违法行为将被计入信用档案且予以公示。这不仅会影响小型个人信息处理者的商业信誉和声誉，还会对其后的业务开展和合作造成不利影响。个信法虽然提出为小型个人信息处理者制定专门规则，但具体规定国家网信部门尚未出台。

经济处罚的调整。根据小型个人信息处理者的营业额、利润水平等财务指标，设定合理的罚款数额。《中华人民共和国个人信息保护法》第六十六条[9]规定，可采用按比例罚款的方式，如罚款金额为企业上一年度营业额的1%~5%，但设定最高限额为100万元，防止罚款过高。同时，对于积极配合调查、主动采取补救措施的小型企业，可在上述罚款幅度基础上酌情减轻20%~50%的罚款金额。法律规定框架内结合小型个人信息处理者的特点做出的细化与变通，既体现了对不同规模企业的合理监管，又避免了因罚款过高对小型企业造成毁灭性打击，增强了法规的可操作性与适应性。对于积极配合调查、主动采取补救措施的小型企业酌情减轻罚款金额，也符合行政处罚中合理行政、过罚相当等原则，有助于鼓励企业主动纠错，积极履行个人信息保护义务[19]。

非经济处罚的适用体现在以下行为。第一，责令暂停部分业务。《个人信息保护法》第六十六条规定，情节严重的可责令暂停相关业务，由此细化出了暂停期限等，使处罚措施更具可操作性和确定性，能够根据违规情节轻重给予相应惩戒，促使企业重视个人信息保护。第二，限制小型个人信息处理活动范围。这是基于个人信息保护的目的和要求，当企业出现违规行为时，限制其处理特定类型或来源的个人信息，促使企业规范处理行为，保障个人信息安全[20]。第三，进行公开道歉。虽《个人信息保护法》未明确规定此项，但公开道歉作为一种声誉罚，有助于恢复受损的社会公共利益和个人权益，增强企业责任意识和自律意识，同时要求声明内容经监管部门审核，保证了道歉的真实性和诚意，也体现了监管部门对处罚措施的规范和监督。第四，吊销小型个人信息处理者的相关业务许可证或营业执照。《个人信息保护法》明确了对情节严重的违规行为可采取此类措施，以最严厉的方式惩治严重违法的小型个人信息处理者，维护个人信息保护的法律秩序和社会公共利益，保障公民的个人信息安全，同时强调充分保障企业的陈述、申辩等合法权益，符合正当程序原则，避免行政权力的滥用。

6. 结论

在当今时代，数字经济蓬勃发展，小型个人信息处理者大量涌现，给市场增添活力的同时，在个人信息保护方面却面临诸多困难。深入研究其豁免义务，对协调企业发展与个人信息保护的关系而言至关重要。小型个人信息处理者在信息处理的收集、存储、使用共享等各环节都设有专门规则，较好地平衡

[9]《中华人民共和国个人信息保护法》第六十六条：“……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……”

了企业资源技术受限的状况与信息安全需求。豁免义务不仅有坚实的理论支撑，在实际操作中也存在多种情形，极大地促进了企业创新和市场多元化发展。优化监管与处罚机制是保障其合规发展的关键，借助数字化工具分类监管和“监管沙盒”等方式，以及合理调整处罚力度，能够有效促使企业履行个人信息保护义务。然而，该豁免义务制度并非一成不变，需要持续完善，以此适应不断变化的技术和社会环境，推动数字经济健康、稳定地发展。

参考文献

[1] 王勇旗. 数字时代个人信息处理的法律制度研究[D]: [博士学位论文]. 重庆: 西南政法大学, 2021.

[2] Burri, M. (2023) Trade Law 4.0: Are We There Yet? *Journal of International Economic Law*, **26**, 90-100. https://doi.org/10.1093/jiel/jgac053

[3] Gulyamov, S. and Raimberdiyev, S. (2023) Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*, **1**, 1-32. https://doi.org/10.59022/ijlp.119

[4] 程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021.

[5] 程啸. 论数据安全保护义务[J]. 比较法研究, 2023(2): 60-73.

[6] 周汉华. 探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向[J]. 法学研究, 2018, 40(2): 3-23.

[7] 张新宝. 互联网生态“守门人”个人信息保护特别义务设置研究[J]. 比较法研究, 2021(3): 11-24.

[8] Voigt, P. and von dem Bussche, A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing AG, 38.

[9] Corning, G.P. (2024) The Diffusion of Data Privacy Laws in Southeast Asia: Learning and the Extraterritorial Reach of the EU’s GDPR. Contemporary Politics, 30, 1-22.

[10] 陈旭琳. 个人信息协同保护的法经济学研究[D]: [博士学位论文]. 长春: 吉林大学, 2021.

[11] 王丽洁. 个人信息处理中比例原则审查基准体系的建构[J]. 法学, 2022(4): 49-63.

[12] 王雅蓉. 小型个人信息处理者保护制度的域外立法经验[EB/OL]. 互联网法律评论, 2023. https://www.secrss.com/articles/42845, 2024-12-15.

[13] Freiherr von dem Bussche, A. and Zeiter, A. (2016) Practitioner’s Corner Implementing the EU General Data Protection Regulation: A Business Perspective. *European Data Protection Law Review*, **2**, 576-581. https://doi.org/10.21552/edpl/2016/4/16

[14] 贺文奕. 信息存档中的个人信息保护义务豁免——基于欧盟实践的评析与借鉴[J]. 档案学通讯, 2022(4): 58-66.

[15] Hofmann, S.C. and Pawlak, P. (2023) Governing Cyberspace: Policy Boundary Politics across Organizations. *Review of International Political Economy*, **30**, 2122-2149. https://doi.org/10.1080/09692290.2023.2249002

[16] 程啸. 论公开的个人信息处理的法律规制[J]. 中国法学, 2022(3): 82-101.

[17] 高富平. 个人信息保护: 从个人控制到社会控制[J]. 法学研究, 2018, 40(3): 84-101.

[18] 程啸. 论个人信息共同处理者的民事责任[J]. 法学家, 2021(6): 17-29.

[19] 蒋红珍. 《个人信息保护法》中的行政监管[J]. 中国法律评论, 2021(5): 48-58.

[20] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122+207-208.