Advances in Social Sciences 社会科学前沿, 2026, 15(4), 333-340
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2026.154314

Hans汉斯

论数据处理者安全保护义务

张亚娜

苏州大学王健法学院，江苏 苏州

收稿日期：2026年3月12日；录用日期：2026年4月15日；发布日期：2026年4月24日

摘　要

数据具有复制简便性以及传播快速性，如未在立法上设定数据处理者的安全保护义务，将带来数据安全风险。数据处理者履行数据安全风险把控能力要求、收益与风险承担原理以及企业社会责任决定了数据处理者应当承担安全保护义务。根据法律规范内容将数据处理者安全保护义务类型化为数据分类分级管理义务、数据安全技术保护义务、数据隐私保护义务。以期对学理研究和司法实践有所裨益，进而为促进我国数据安全健康发展贡献绵薄之力。

关键词

数据处理者，安全保护义务，数据安全

On the Security Protection Obligation of Data Processors

Yana Zhang

Kenneth Wang School of Law, Soochow University, Suzhou Jiangsu

Received: March 12, 2026; accepted: April 15, 2026; published: April 24, 2026

Abstract

Due to the simplicity of data replication and the rapid speed of data transmission, if the security protection obligation of the data processor is not set in the legislation, it will bring data security risks. The data processor's performance requirements of data security risk control ability, income and risk bearing principle and corporate social responsibility determine that the data processor should assume the security protection obligation. According to the legislative content, the security protection obligation of data processors is classified into data classification management obligation, data security technology protection obligation and data privacy protection obligation. So as to be beneficial to theoretical research and judicial practice, and then contribute a small contribution to the healthy development of data security transactions in China.

文章引用: 张亚娜. 论数据处理者安全保护义务[J]. 社会科学前沿, 2026, 15(4): 333-340.
DOI: 10.12677/ass.2026.154314

Keywords

Data Processors, Security Protection Obligation, Data Security

1. 引言

《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》)和《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)塑造的网络和数据安全监管框架。这一顶层设计旨在实现双重目标：既要充分激活数据要素潜能，保障数据资源的合法流通与利用，又要筑牢安全防线，有效遏制数据滥用风险。在此框架下，数据处理者享有使用数据并获取收益的正当权益，但权利与义务是对等的，须同步履行严格的安全保护责任，对所处理的数据资产实施周密且全周期的风险防控。

在数字经济社会中，处理科技与防范科技的双向快速发展，数据处理者借助庞大的数据资源，配置大数据算法，高效率推进社会生活与经济发展，从各个数据主体中获取的数据进行处理，提供生产数据产品或服务，使得其处理的数据成为数据安全的重要问题。《数据安全法》第四章系统构建了数据安全保护义务的规范体系，为上述治理目标提供了坚实的法律支撑。身处信息时代，数据安全始终是贯穿数字经济发展的核心命题。判断数据处理行为是否合规，关键在于能否在高效利用数据资源的同时，恪守基本的安全保护底线。数据处理者不仅要对自身处理的数据质量负责，更需对数据整体安全态势负责，应摒弃被动应对的滞后思维，转而建立前瞻性的风险预警机制，将“安全内嵌于业务”的理念落到实处，切实履行法律赋予的各项安全保护义务。本文将对数据处理者的安全保护义务内容进行分析，对其产生的理论基础以及规范构造等内容予以探究，以《数据安全法》为规范依据，并结合《网络数据安全管理条例》的具体规定，对上述内容展开探讨。

2. 数据处理者安全保护义务的界定

2.1. 数据处理者安全保护义务的内涵

数据是指固定于一定的载体之上，能够满足人们生产和生活需要的电子记录。对应保护的数据将合法性、价值性、属人性作为数据保护一般性实质要件的必选项，而将管理性、集合性、公开性作为数据保护一般性实质要件的弃选[1]。只要具备或满足合法性、价值性、属人性三个要件，相应数据就应当纳入法律保护范围，根据情况采取必要的、具有期待可能性的风险防范措施以保护处理数据免受损害。数据处理行为是自然人或者企业让渡自己的数据权益，数据处理者通过分析处理加工成数据产品或服务，是促进数据成为生产要素进行流通交易的重要环节，为避免数据处理者滥用、泄露其所处理的数据，应当对数据处理者的安全保护义务作出规范。

我国立法认可了信息与数据的在规范层面的区分意义，并将数据与信息的本质等同，认为数据是信息的一种电子化或其他形式的记录。我国现有立法规定了数据信息的安全保护义务，比如《中华人民共和国消费者权益保护法》第二十九条规定了经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息；《网络安全法》中规定的网络运行安全保护义务；《中华人民共和国商业银行法》第二十九条规定的存款人信息保护义务。在数据安全保护范

式下，政府不再将进入数字基础设施对代码和算法进行监管作为主要出路，而是通过向数据处理者施加安全保护义务，让代码设计者为自己的发明所造成的影响负责。在《个人信息保护合规审计管理办法》颁布实施后，数据处理者不仅需要履行数据安全保护义务，同时也需要满足“充分履行”这一法定要求。

数据处理者在收集处理数据过程中，也应当保障数据安全，根据情况采取必要的具有期待可能性的风险防范措施以保护被处理数据免受窃取泄露。数据处理者应当履行与其优势经营地位、行业特殊性和行为危险性相适应的义务，应当对被处理数据者进行处理告知以及使用通知，应当定期对数据处理系统进行安全检查，消除数据安全隐患，如数据处理者未充分履行以上义务，构成违反法定义务行为，将承担相应责任。

一方面，数据处理者源源不断收集数据来巩固其数字基础设施地位；另一方面，数据处理者以代码和算法构筑起反数据流动的屏障，限制作为生产要素的数据资源自由流动。随着数据处理者对数据的垄断局面不断巩固，数据权益主体以及处理主体之间的信息不对称也不断加剧。这种不对称性所产生的机会不对等与对暗箱操作的担忧，不仅体现在数据处理者和用户之间，还体现在数据处理者和政府之间。

数据处理者的安全保护义务体现在其数据处理行为的各方面，包括从得到原始数据开始到将数据处理完毕之后的销毁，从数据处理的技术手段以及工具保密措施到数据处理人员的岗位安全保护，以及对处理数据的合法获取以及不能随意扩大处理数据的范围。本文将数据处理者的安全保护义务范围确定在数据接收方、数据发送方、数据处理方各主管部门以及人员，在进行数据安全保护时，不能无限扩大数据安全义务保护范围，但也应全面考虑纳入义务范围的各项数据以及各种数据处理行为以及数据处理主体。

2.2. 数据处理者安全保护义务的主体界定

权利的真正条件是义务，义务的唯一合理性在于权利。法律实践通过“权利－义务－责任”机制来实现公平与正义，其中义务通常根据法律关系中行为主体的职能和地位来设计，不同的职能和地位承担的义务不同[2]。数据治理强调数据的可用性、透明度、高质量、数据安全保护与相关责任机制。数据处理者作为数据实际控制者，对确保数据处于有效保护和合法利用的状态承担直接责任，基于法律所赋予的义务成了数据安全保护的主要责任者[3]。

“数据处理者”一词在《数据安全法》《网络安全数据管理条例》《中国人民银行业务领域数据安全管理办法》中均有关于此的权利义务内容描述并且详细写了关于数据处理者的安全保护义务内容。数据处理者即是实施数据处理活动的组织和个人，包括自然人、企事业单位等民事主体，也包括国家机关以及法律、法规授权的具有管理公共事务职能的组织[4]。

信息处理者以及数据处理者都依托于时代发展以及技术完善，信息处理者同时也担任着数据处理者的职能，数据处理者对信息处理者的规范也有一部分的借鉴，在此基础上，二者存在相同点并通过立法拘束其处理行为有着类似性。在数字技术条件下对电子化的个人信息处理时，个人数据表现个人信息时，数据处理者包括个人信息处理者；在非数字技术条件下对非电子化的个人信息处理时，数据处理者的范围则不包括个人信息处理者[5]。

《中华人民共和国民法典》(以下简称《民法典》)第一千一百九十八条规定的安全保障义务适用于特定主体，即经营场所、公共场所经营者、管理者或者群众性活动的组织者。“数据安全保护义务”并非新设义务，其实质是《民法典》侵权责任编中的安全保障义务在网络安全领域适用时的特殊表达[6]。数据安全保护义务的主体是特定的，即数据处理者，即对数据进行收集、计算、传输等活动的主体，主要包括数据平台经营者以及管理者，例如商业银行、网站运营者、管理者等。之所以是这些主体是因为这些主体在处理数据的场合和活动中存在着数据密度大、涉及范围广，容易发生数据安全事件也容易在危险

发生后造成较大损害，故此，法律上对数据处理者提出了特别要求。

2.3. 数据处理者安全保护义务的法律性质

关于安全保护义务的性质，有附随义务说、法定义务说等观点。法定义务说借鉴德国法上交往安全义务以及我国安全保障义务建立起来的，是对社会中不断扩张的行为义务配以侵权法上的责任。立足合同违约角度和事实侵害角度，在不同情况下，安全保护义务所体现的性质不同，也因为权利人选择不同救济手段，使得认定的安全保护义务内容各有不同。不能单一认定安全保护义务是一种法定义务或者附随义务。在现阶段的立法司法实践中，首先在立法中规定了数据处理者负有安全保护义务，在数据处理活动中也有合同义务约定，因此两种义务性质在实践中都存在。对于探讨数据处理者违反安全导致保护义务导致侵权损害发生，应当做到全面评价。

在数据处理行为的合同中，本身就要求数据处理者在处理数据时保障其处理数据的安全，不得侵犯数据主体的隐私生活安宁，强化数据安全保护义务尽可能降低人为因素导致的数据泄露事件[7]。法定义务仅从法律规定界定数据安全保护义务性质，忽视了当事人之间可能达成的合同关系，另有一些安全保护义务本身就是合同履行的主要内容。数据处理者在数据处理行为在公共数据平台领域可能遇到的危险隐患预见可能性较高，数据处理活动衍生出潜在的数据泄漏危险，应当采取各种措施避免安全风险的发生。个人数据所有者与数据处理者之间达成一份关于数据产品或服务的合同，而在合同中体现的要求数据处理者履行数据安全保护义务。根据数据处理者与数据主体达成的数据产品或服务合同，为其提供相应产品或服务，根据法律法规规定，将数据安全保护义务纳入合同中，当数据处理者违反合同义务时，数据主体根据合同要求数据处理者承担违约责任。数据处理者违反安全保护义务既可能构成侵权责任也可能构成违约责任，发生民事责任竞合。受害人有着损害赔偿请求权，对此按照《民法典》第一百八十六条之规定，由赔偿权利人选择进行救济损害。

根据我国法律规定以及相关司法实践来看，数据安全保护义务规定为法定义务更有利于打击数据侵权行为，将数据侵权纳入民法侵权体系中 尊重当事人意思自治内容，法定义务说在现有阶段能够更好地保护数据安全，本文更倾向于认定安全保护义务为法定义务。

3. 数据处理者安全保护义务的理论基础

根据传统民法理论，经传统民法思维路径进行理论源头梳理，数据安全保护义务的理论基础主要有危险控制理论、收益与风险相一致原理、企业社会责任理论等，也有学者从经济学、社会学、哲学等角度进行论证安全保护义务理论在现代社会的合理性。

3.1. 危险控制理论

网络空间安全治理不同于传统的社会治理模式，更强调在事前预防和控制潜在的各类安全风险。“危险控制理论”认为从事该特殊活动的人是“危险源”的肇始者和控制者，其对“危险源”具有一定的控制能力。即使行为人毫无过错可言，也缺乏道德上的可非难性，但是基于分配正义的要求，仍需承担损害赔偿责任。信息富有者和信息贫乏者之间存在着日益分化并不断扩大的“数字鸿沟”(Digital Divide)，从事实层面导致数据社会中的数据危险侵害有更大的危险性，造成的财产损失更加巨大，无形中增加了追究侵权责任的难度以及数据权益人的举证难度。故此以数据侵权责任进行控制“数据侵害危险源”是非常值得关注的。

相较于数据权益者，数据处理者的数据行为能够最大程度发挥数据资源效力，在数据处理过程中，数据处理者对处理数据具有更强的控制权，对数据进行计算、整合的行为与被处理数据之间具有紧密联系，数据安全保护也与之息息相关，故此就与数据紧密程度以及控制权来说，数据处理者更适于履行数

据安全保护义务。本质上是因为作为管理者或者所有者，其对本场所的领域最为熟悉，对出现的危险以及提示等更较易发现并且解决隐患。在数据空间领域，存在虚拟空间以及实体操作双重属性，数据处理者在自己管辖支配的领域有责任保护数据安全不受侵害[8]，对其在数据处理的法律关系中的职能和地位进行义务设计来实现实质公平和实质平等，维护数据安全。在数据安全事件中，其属于能够最先反应的主体也是能够避免数据损害扩大的关键源头之一，据此，数据处理者因着紧密联系以及对被处理数据的控制权，在安全事件中具有最广泛的保护能力与责任，数据处理者应当承担数据安全保护义务，保障数据安全以及数据市场秩序。

3.2. 收益与风险相一致原理

“营业收益风险理论”由法国的萨莱伊和约瑟兰德所倡导，是在“危险控制理论”基础上发展起来的针对企业经营者责任的理论。该理论认为，由于营业或物件的管理人从营业或物的积极作用中获得了利益，基于从其营业及物件中所获得利益的抵偿原理，法律要求产生危险的营业或物件管理人就其经营营业及管理物件所导致的损害后果承担侵权责任。数据安全保护义务应当分配给可以最小成本实现它的人，因为“凡成本高于收益的举措，必然不值得采取”[9]。

一是客观方面对处理数据的存储、加工及传输，义务人对其处理数据的场所、技术、环境有具体充分了解并对其安全性有安全保护义务，排除安全隐患，定期检查各项参数，保障其进行数据处理时的安全性；二是主观方面对“数据主体”的提醒、通知和保护，应当适配适当的技术为被处理数据进行“防御”保障，能够及时发现数据出现风险并做出行动，以防被外界或第三方侵害。同时应当及时对已发生的危险和损害采取积极的应对和救助措施。数据处理者进入市场进行数据处理行为，对比数据主体天然具有优势性，因其借用此处理行为将获取巨大利益并且暂无具体法规进行管理制约，便需要为其设定义务来平衡多方利益。

若只进行数据处理受益活动而没有义务规制将导致道德义务危害数据安全。数据权益人依法应当享有数据权益，立法规范保障其数据安全不被侵犯，个人隐私等不被泄露，数据处理者也是保障其数据安全的义务主体，从这个角度进行分析，数据处理者的安全保护义务不只是法定义务也是保障公私主体数据权益不被侵害的应有之义；在让渡数据将其交至数据处理者进行数据资源利用行为时，数据处理者从中获得收益，在数据安全保护义务范畴内其数据处理行为能够最大限度地降低双方维权的成本。数据安全若出现问题，受损害的主体是第三方(数据所承载内容涉及的相关权益主体)，数据处理收益在数据处理者一方，风险收益不对等，为保障实质平等，数据处理者应当承担数据安全保护义务。发生数据泄露或者损毁事件时，数据处理者应当采取防范制止侵害措施，在注意到对数据权益者有侵害时，信息差以及处理手段与防范技术差距大原因，数据权益者很难通过自己的手段或者方式进行维权以及减少降低损害，此时凭借着数据处理者掌握的资源与技术能够降低此类危险，由此降低维权的相对成本，也能更好地平衡因数据权益人让渡数据交给数据处理者进行处理由此带来的未知危险，避免让第三方承担数据处理者风险行为引发的损失。

3.3. 企业社会责任理论

“企业社会责任理论”认为，保障服务对象利益是信息企业社会责任应有之义。当前在政府的数据治理中，保障数据权利的法律法规是相对匮乏的，各数据主体的权利几乎处于“裸奔”的状态。因此更加需要企业承担社会责任，主动承担数据安全保护义务，在数据处理促进经济社会发展的同时发挥企业社会责任，将保障数据安全做到数据处理的各方面。企业可以参照 GDPR 关于数据保护官(Data Protection Officer)的规定，在企业内部设立专门的“平台数据合规官”，由具有法律、管理、数据等专业知识和技

能的复合人才对平台的数据安全进行风险管控[10]。

数据处理者有能力控制数据处理过程中产生的安全风险，其应根据情况对数据安全风险采取必要的、具有期待可能性的防范和处置措施，以确保相应利益不受侵害[2]。作为数据处理者保障其处理数据的利益是企业社会责任本身应当体现的内容，数据处理者的行为被纳入大数据安全法的立法调整范围内，在数据产品的上游处理环节，数据处理者恪守安全保护义务能够更好地建设数据治理体系的全面化，在数据泄漏事件发生或其他数据安全问题发生时能够及时止损。数据处理者违反安全保护义务后，对其侵权行为承担责任，以过错程度区分侵权人的连带责任与补充责任，在承担补充责任情况下数据处理者承担超出责任范围的赔偿后可向第三人进行追偿。

4. 数据处理者安全保护义务的类型化分析

4.1. 数据分类分级管理义务

数据类型化是构建数据分类分级管理制度的核心环节，数据处理者根据国家标准对数据分类分级，并对不同类型和数据进行不同处理，从而拆解出不同类型和重要程度安全义务内容，对于重要数据的处理采取更加严格的安全保护义务，对于一般的数据采取基本的安全保护义务要求，对于行业特性的数据处理运用行业特性进行安全保护义务设定。在行业领域进行数据分类时，需要根据行业领域数据管理和使用要求，结合行业领域现有的数据分类基础，灵活选择业务属性，对数据进行逐级分类。

我国现有立法并没有统一的数据分类分级标准，且数据的分类审查制度有待完善。在不同行业的立法以及地方立法中规定了相关分类分级标准，比如《金融数据安全数据安全分级指南》《证券期货业数据分类分级指引》《贵州省政府数据数据分类分级指南》等，还有就是时代发展的人工智能司法实践中提出的司法数据分类分级，这些都应当纳入数据分类分级管理的范畴中，通过“种类列举 + 原则性规定”进行个案分析，构建覆盖全生命周期的安全防护体系，对相关数据类型与等级实行动态管理，实现“分级防护、动态治理”目标，保障数据安全[11]。

数据处理者识别处理数据应按照分类分级管理义务进行分类分级。不同的数据类型对应不同的数据处理方式以及所负担的安全保护义务，判定数据处理者是否履行安全保护义务的标准也同时对标分类分级的数据。可借鉴欧盟的《通用数据保护条例》(GDPR)的数据处理评估制度，设置适当和成比例的技术与组织措施管控数据安全风险防范，德国数据伦理委员会提出的算法风险评估方案，主张对数字服务企业使用的算法进行五级的风险评级制度，对不同级别的算法采取不同强度的监管[10]。制定安全管理制度确定负责人，对外来侵入网络风险进行技术防范，监管网络运行状态，保障被处理数据的安全环境，对重要数据的备份加密。数据安全性遭到破坏后可能造成的影响(如可能造成的危害、损失或潜在风险等)是确定数据安全级别的重要判断依据，在《金融数据安全数据安全分级指南》第五条指出安全性(包括保密性、完整性、可用性)是信息安全风险评估中的重要参考属性。

对此若数据处理者未按照行业所属分类分级要求或未合理正当分类数据，造成数据处理过程中发生损害数据或者泄漏数据行为，应当负有责任。法律规定要对数据分类分级进行处理，根据数据不同属性以及重要程度等不同进行相关的类型化研究，数据处理者若违反该规定，极有可能造成数据因未受到应有保护手段或处理方式导致数据侵权，危害其他数据处理者或数据权益人。

4.2. 数据安全技术保护义务

结合《数据安全法》第二十七条和《网络数据安全管理条例》第九条以及其他法律的有关规定，数据处理者为强化数据安全防护需要采取的技术性措施主要包括：配套数据处理技术以及数据安全“防火墙”技术，避免其处理数据的泄漏风险。

加强管理完善健全配套管理措施。处理者在进行数据处理时，应当保障数据处理环境的安全，以及数据处理工作人员的保密工作要求，不能存在不确定因素导致数据泄漏或损毁风险。例如，要定期对数据处理从业人员进行组织管理，定期对处理数据进行整合管理审查等，确保数据处理行为正当合规。数据处理活动订立的合同存续时间较长、交易内容含糊、各方利益需求因外界情形变化需随时调整、其存续甚至不以明确的承诺为前提，故而无法用传统的合同法进行解释[12]。数据主体通过授权数据处理者访问浏览记录与消费记录，通过算法分析，换取数据处理者提供的“精准推送服务”；在平台或 APP 弹框界面的授权访问内容，数据主体勾选同意之后双方达成的数据服务合同，数据处理者未提及自身的安全保护义务进行提及，未来应完善数据处理者监管范围。

坚持技术革新与数据处理标准，做到与时俱进。在进行数据处理过程中，技术安全保护是核心行为，数据处理环节最主要依靠的就是处理数据的技术手段，在高效安全条件下将数据转化为资源和生产要素，因此对数据处理者使用的技术从安全到革新都提出要求，控制数据处理的运行成本以及保护成本。

数据安全管理与技术保护的机制健全，要求数据处理者应当定期组织开展数据安全教育，全流程数据安全管理制度、技术规范和操作规程，采取安全技术措施保障其处理数据的处理系统和存储环境的安全，不管是从数据人员还是到处理者建构的处理环境中的技术安全等，设置数据安全管理岗位，实行管理岗位责任制，配备安全管理人员和专业技术人员，都要求其全面保障其处理数据的安全。

4.3. 数据隐私保护义务

数据安全保护限制数据处理者过度收集数据权益人的相关数据，因此要求严格限制数据授权范围，为保障数据者本身应有的知情权，数据处理者要将数据处理的算法以及隐私政策进行披露。

第一是数据处理告知义务。数据处理者在处理数据也应当履行处理告知义务，使得数据权益者知晓数据被处理，从而有关于数据可能泄漏预期并做出防范措施，进一步提高了数据安全。也要求对重要数据的处理向监管部门进行告知。在数据处理过程中如果存在不安全因素或者可能出现危险时应当进行说明和警示，对可能出现的危险对数据权益人进行合理说明。

第二是数据授权范围限制义务。数据处理者应有权根据处理数据所需的内容收集数据，不应强制“一揽子授权”收集不必要的数据。《2024 年美国隐私权法案》(APRA)，该法案明确了国家层面的数据隐私保护措施，建立了强有力的执行机制以追究违法者的责任；支持数据最小化，相关条款将对于个人数据的收集和使用限制在提供产品或服务所必需和相称的范围内，将进一步限制敏感数据的传输和使用，并对生物识别和遗传信息制定更严格的规则。数据处理者应根据法律法规的规定，根据个人授权范围收集、持有和使用数据，并确保个人数据和个人信息的合理使用。避免数据处理中的冗余，增加数据处理成本，从而增加数据产品或服务的价值，从而将这一成本转嫁给消费者。通过限制数据收集授权的范围，数据处理者的安全保护义务仅限于其收集的数据，避免了冗余数据的安全保护成本，进一步提高了其处理数据环境的安全保护。数据处理者在进行特定数据处理活动时，应当对每条个人信息取得个人同意，不包括对多条个人信息和多次处理活动的一次性同意。不得将个人信息作为数据处理者识别个人身份的特征。

第三是算法与隐私政策披露制度。互联网平台运营者在使用个人信息和个性化推送算法向用户提供信息时，除对推送信息来源的真实性、准确性和合法性负责外，还必须首先征得个人同意；并设置易于理解、易于访问、易于操作的个性化推荐选项，允许用户拒绝接受定向推送信息，允许用户根据个人特点重置、修改和调整定向推送参数；允许个人删除定向推送信息服务收集生成的个人信息。当数据处理者使用个人数据与信息和点击算法向用户显示信息时，互联网平台运营商必须首先获得个人同意，并设置易于理解、易于访问和易于操作的具体建议，允许用户拒绝接对性地推送的推送信息。

网络平台经营者应当建立与数据相关的平台规则、隐私政策和算法策略披露制度，及时披露制定和

裁决程序，确保平台规则、保密政策和算法的公平公正。规定平台运营者必须严格履行第三方安全管理义务，严格履行个性化推荐安全义务，不得利用数据和平台规则进行不正当竞争。

第四是数据处理不当的通知义务。数据泄露事件时有发生，不只是数据处理者的义务缺失，也有不法分子利用技术等对数据处理者处理系统进行攻击窃取数据。因此更需要数据处理者对其处理者数据设置严格的保护，并做出数据泄漏的处理预案，在发生数据安全事件时，能够及时通知泄露数据主体进行及时采取措施，从而降低数据安全事件带来的损失。

若数据处理者不进行通知，任由泄露数据流通而数据主体不知情的情况，更可能导致数据主体受到影响或损失，例如遭遇电信诈骗、被转移财产、借助数据进行违法犯罪活动，都是对数据主体的二次侵害。故此要求数据处理者不只要事前做好数据保护措施，在处理数据时也要建立防火墙机制，在不慎数据被泄露窃取后能够有及时的预案，将损失减至最小，这也应当是其安全保护义务的内容。

5. 结语

数据处理者所履行的安全保护义务，兼具私益性与公益性，数据成为新时代各主体都争抢的信息高地，而数据处理者所处理数据具有数量巨大、传播便利性、风险不可控性增大的特性，且数据处理者又掌握着不对等的数据信息，个人容易处在弱势地位且国家处于被动地位，为了规制平衡二者的信息差，立法对数据处理者施加的安全保护义务具有正当性。因此数据处理者的安全保护义务既具有私益性，其保护了处理者本身不被数据裹挟走向错误道路，也具有公益性，保障国家数据安全以及稳定的市场。

参考文献

[1] 管荣齐. 论数据保护的一般性实质要件[J]. 学术论坛, 2025, 48(6): 17-31.
[2] 周昀, 姜程潇. 关键数据处理机构的数据治理结构[J]. 法学杂志, 2021, 42(9): 42-52.
[3] 王玎. 论数据处理者的数据安全保护义务[J]. 当代法学, 2023, 37(2): 40-49.
[4] 程啸. 论数据安全保护义务[J]. 比较法研究, 2023(2): 60-73.
[5] 苏成慧. 信息处理者安全保障义务的体系阐释[J]. 河北法学, 2026, 44(1): 120-138.
[6] 杨显滨. 论场内数据交易的法律制度建构[J]. 政治与法律, 2024(5): 159-176.
[7] 周瑞珏. 数据泄露风险治理中网络安全保险的介入路径[J]. 北方法学, 2024, 18(2): 76-90.
[8] 李想. 数据处理者的数据安全保护义务及刑事责任[J]. 大连理工大学学报(社会科学版), 2025, 46(5): 72-84.
[9] 张永健. 法经济学分析: 方法论 20 讲[M]. 北京: 北京大学出版社, 2023: 289.
[10] 张凌寒. 数据生产论下的平台数据安全保障义务[J]. 法学论坛, 2021, 36(2): 46-57.
[11] 郑文阳. 数据分类分级管理的法治化省察及推进——以公共数据为侧重[J]. 东南法学, 2025(1): 36-54.
[12] 唐林垚. 关系合同视角下数据处理活动的技术流变与法律准备[J]. 法学家, 2023(1): 42-56+192.