企业个人信息保护合规手册

朱凯 夏蕊 蒋皓宇◎著

详细解读个人信息保护相关新规
系统梳理企业的业务流程和场景

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

企业个人信息保护合规手册

朱凯 夏蕊 蒋皓宇◎著

中国法制出版社
CHINA LEGAL PUBLISHING HOUSE

图书在版编目（CIP）数据

企业个人信息保护合规手册 / 朱凯，夏蕊，蒋皓宇著. -- 北京 : 中国法制出版社，2024. 8. -- ISBN 978-7-5216-4587-3

Ⅰ. D923.74

中国国家版本馆 CIP 数据核字第 20244UC108 号

策划编辑：赵　宏

责任编辑：陈晓冉　　封面设计：杨鑫宇

企业个人信息保护合规手册

QIYE GEREN XINXI BAOHU HEGUI SHOUCE

著者/朱凯　夏蕊　蒋皓宇

经销/新华书店

印刷/河北鑫兆源印刷有限公司

开本/710 毫米×1000 毫米　16 开　　印张/ 17.75　字数/ 188 千

版次/2024 年 8 月第 1 版　　2024 年 8 月第 1 次印刷

中国法制出版社出版

书号 ISBN 978-7-5216-4587-3　　定价：69.80 元

北京市西城区西便门西里甲 16 号西便门办公区

邮政编码：100053　　传真：010-63141600

网址：http://www.zgfzs.com　　**编辑部电话：010-63141835**

市场营销部电话：010-63141612　　**印务部电话：010-63141606**

（如有印装质量问题，请与本社印务部联系。）

朱凯，华东政法大学法学学士、英国阿伯丁大学法学硕士，上海律协数据合规与网络安全专业委员会委员，上海科技法律联盟数字经济专业委员会委员，华东政法大学兼职硕导，上海对外经贸大学兼职硕导，上海中岛律师事务所管理合伙人、高级合伙人。朱凯律师执业近20年，长期专注于汽车、互联网、新能源、创新科技、新兴服务业等行业的直接投融资、企业并购、股权激励和股权治理、企业合规、数据安全合规和个人信息保护、商事争议解决等法律服务领域。

夏蕊，复旦大学法律硕士。擅长领域包括：投融资与并购、复杂商事争议解决、公司合规等。曾为多家国内外知名企业提供争议解决和专项法律顾问服务，在多起围绕公司、股东、股权、公司决议等方面的复杂商事案件中维护了客户的合法权益。此外，夏蕊曾为多家大型银行、投资公司、国有企业、上市公司等处理投融资、跨境并购、私募基金、公司合规等业务，在非诉领域亦积累了丰富的法律服务经验，能帮助客户全面把握风险。

蒋皓宇，上海中岛律师事务所合伙人，毕业于华东政法大学。蒋皓宇律师的主要执业领域为国际法律业务，包括涉外企业合规、跨境交易及争议解决等，涉及行业包括国际贸易、能源环保、智能制造、时尚消费、互联网等，并曾在中国香港地区、欧洲多地进行工作和交流，具备丰富的涉外实务经验。

前　言

个人信息保护是任何一个法律体系社会在进入数据化时代后所面临的新问题、新挑战。过去的隐私保护制度虽然包含了个人信息保护的内容，但对信息的利用却太过消极，更多的是从人身权利的角度出发，保护个人的基本人权、禁止或限制个人信息的交流传递。而当今的个人信息保护，更多强调的是信息应如何合法利用，从运用先进数据处理技术和发掘数据要素价值的角度出发，引导人们在合法、合规的基础上最大限度地利用个人信息为生产生活和经济发展服务。

21 世纪以来，随着数字技术的迅猛发展，个人信息日益成为一种重要的数据化资产，个人信息保护也逐渐上升为全球性的关注议题。这一趋势推动了全球个人信息保护立法进程不断加快。据统计数据显示，2000 年至 2010 年，全球颁布个人信息保护法的国家数量较十年前翻了一番，达到 40 个；而 2010 年至 2019 年，这一数字更是增长至 62 个，创下历史新高。预计这一趋势将在未来几年持续下去，到 2029 年，全球将有超过 200 个国家或地区拥有个人信息保护法。

中国的个人信息保护制度之建立，正是全球个人信息保护制度建立和完善这一历史性发展的重要一环。2021 年 8 月 20 日《中华人民共和国个人信息保护法》的正式颁布，标志着中国个人信息保护立法迈入了新的历史阶段。这部法律的出台，既是“百年未有之大变局”背景下对全球个人信息权益保护的制度回应，也是顺应数字时代发展趋势的必然

要求。这部《个人信息保护法》凝聚了国内外先进立法经验，体现了中国特色社会主义法治理念；在借鉴域外立法智慧的基础上，又充分吸收了本土实务经验；既将个人信息权益保护作为基本原则，又注重规范个人信息处理活动，实现了“个人信息权益”的私权保护与“个人信息处理”的公法监管的有效平衡。同时，该法还统合了私主体和公权力机关的义务与责任，兼顾了个人信息保护与利用，为我国网络社会和数字经济发展奠定了坚实的法律基础。

企业在个人信息保护制度中扮演着双重角色：既是个人信息保护制度的受益者，也是个人信息保护制度的责任人。一方面，个人信息保护制度的建立和完善，可以帮助企业促进个人信息数据的利用，更好地了解消费者需求、提高营销效率、创新商业模式；另一方面，企业是个人信息收集、处理和利用的主要主体，更容易发生个人信息泄露、侵权等问题。因此，个人信息保护制度不仅是企业的机遇，也是企业的责任。企业只有积极参与个人信息保护制度的建设，切实履行个人信息保护责任，才能在个人信息保护中获得更大的收益。

本书是由中岛律师事务所的高级合伙人朱凯律师，带领团队两位在数据合规和个人信息保护领域提供法律服务的卓越的律师，共同创作完成的实务性指导图书。作为领导者的朱凯律师自 2019 年起专注于网络安全、数据安全和个人信息保护的法律服务工作和实务性业务研究。在当前这样一个信息化、数据化时代，作为法律从业者，作者深刻感受到技术推动着国家法治的迅速发展变化，技术发展和社会生活的网络化、数据化将每个人不可逆地推向未来的浪潮。在此过程中，作者不断思考如何理解网络、数据和个人信息之间的关系，观察它们相互之间的影响，并把握法律制度的变革、发展和趋势。本书内容包含了作者多年来在个人信息保护法律服务领域积累的经验的总结，对企业个人信息保护合规司法实践具有指导价值。

以个人信息保护为基础，作者深入讨论了全球个人信息保护的整体环境、中国个人信息保护法律制度的发展和现状，以及《个人信息保护法》与《网络安全法》、《数据安全法》之间的相互关系和意义。此外，作者还探讨了企业根据当前法律规定所需承担的保护合规义务。

同时，个人信息保护制度作为一套新的制度，正在不断发展和完善。因此，作者也希望引导读者了解这一全新而完整的法律体系的历史沿革、变化过程和发展趋势。毕竟，作为实务性法律的运用者，企业高级管理人员应具备前瞻性和预见性，以适应不断演变的个人信息保护要求。

本书的目标读者为企业中负责合规、数据安全和法律事务管理的专业人员，为他们提供实现企业个人信息保护合规目标的指导。本书提供了实用的方法和步骤，帮助读者从零开始，系统梳理企业的业务流程和场景，对个人信息进行分类和处理，并建立一套完整的内部个人信息保护制度，以及掌握在面临企业个人信息安全风险时妥善处理这些事故的方法。

本书涵盖了最新的重要的个人信息保护制度，具有极强的时效性。基于丰富的实务经验，作者在本书中快速、系统地分析和对比了企业个人信息出境的可选路径，并结合企业的具体使用场景提供指导，帮助企业判断和选择合适的出境合规路线。

此外，本书在实际操作层面也具有一定的指导作用，介绍了企业如何从零开始建立个人信息保护制度体系，读者可以根据书中内容结合企业自身情况，逐步建立起个人信息保护的初步制度。作者将复杂的概念和法律制度转化为易于理解的内容，并提供了按部就班的实操引导。本书还揭示了个人信息保护领域的最新制度发展趋势。读者将受到启发，并从全面理解个人信息保护的角度受益，将这些知识和信息应用于实际工作中。

本书结构按照逻辑顺序设计，旨在逐步引导读者了解和实施个人信

息保护合规。第一章对基本概念进行界定，为全书奠定了基础。第二章介绍了欧盟、美国和亚洲主要地区的个人信息保护规则。在当前国际环境下，个人信息保护不仅局限于一个国家或地区，在深入学习和了解本国制度的同时，了解域外制度和环境也是必要的。特别是欧盟的《通用数据保护条例》，其所涵盖的长臂管辖已经对我国境内的外贸企业产生了深远影响。第三章详细介绍了我国的个人信息保护制度，以《个人信息保护法》为核心内容，不仅包括《个人信息保护法》的规定，还涵盖了与之相关的《网络安全法》和《数据安全法》，以及重要的技术性文件《信息安全技术 个人信息安全规范》和《信息安全技术 个人信息安全影响评估指南》，提供了个人信息保护法律制度内容。第四章和第五章更加注重实操，构成了个人信息保护合规过程中最关键的两个环节——制度建设和安全事件处置。这两章的内容既可成为企业的实操指南，按部就班、逐渐实施，也可用作企业的自查工具，逐一对比、补充不足。

我们深知，企业个人信息保护是一项长期而艰巨的任务，需要全社会的共同努力。我们希望本书能够为企业和个人提供一些帮助，促进企业个人信息保护事业的健康发展。最后，向所有致力于企业个人信息保护的读者致以诚挚的敬意！

目　录

第一章　隐私和个人信息保护概述

第二章　域外个人信息保护法制发展现状

第三章 我国个人信息保护主要制度规范

第四章 企业个人信息合规管理制度建设

第五章 企业个人信息安全事件处置及个人信息保护管理

第一章　隐私和个人信息保护概述

第一节　什么是隐私，个人信息和隐私的关系

隐私是一种古老而基本的权利，它涉及个人生活中的私密、尊严和自主性，指的是个人在不受侵犯、干扰或公开的情况下，独自或与他人共享的信息、行为和空间。1948 年的《世界人权宣言》（Universal Declaration of Human Rights）第 12 条、1950 年的《欧洲人权公约》（European Convention on Human Rights）第 8 条第 1 款、1966 年联合国《公民权利及政治权利国际公约》（International Covenant on Civil and Political Rights）第 17 条都对隐私权有明确规定。

全球最早的隐私权国内法律通常被认为是德国在 1970 年颁布的《赫塞州数据保护法》（Hessian Data Protection Act）。该法比其他国家关于数据保护和隐私权的立法更早，标志着现代数据保护法律的诞生，为其他国家的立法提供了参考。其规定涉及个人数据的收集、处理和使用，以确保这些行为不会侵犯到个人隐私。虽然它没有明确给出隐私权的定义，但其核心理念是确保个人隐私得到保护。由于当时人类社会还没有进入信息化时代，该法所指的数据更多侧重于与个人有关的信息，故《赫塞州数据保护法》确立的是保护个人隐私的重要原则，这些原则后来成为

其他国家和地区隐私和数据保护法律的基础。比如，欧洲的《通用数据保护条例》（General Data Protection Regulation，GDPR）就受到了德国数据保护法的影响。

更有影响力的是美国的1974年《隐私法案》（Privacy Act）。该法案主要针对美国联邦政府机构收集、维护、使用和披露个人信息的行为进行规范，其核心目标是保护个人隐私，同时确保个人能够查阅和纠正政府机构记录中关于他们的信息。遗憾的是，美国1974年《隐私法案》没有对隐私作出明确的定义。事实上，在美国的法律体系中并没有一个统一的关于“隐私”的定义，对隐私权的保护通常是通过一系列具体的法律条款实现的，这些条款规定了政府和企业在处理个人信息时应遵循的原则和限制。美国最高法院在多个案件中对隐私权进行了讨论，其中著名的案件之一是1965年的格里斯沃尔德诉康涅狄格州案（Griswold v. Connecticut）。在这个案件中，法院裁定了“隐私权”的概念，该概念源于宪法对个人自由的保护，主要涉及个人生活中的隐私权利。通过这个案例确立了隐私权的基本原则。

在我们的日常生活中，关于隐私，最常见的是当我们安装一款新的手机软件（App）时，软件在用户注册阶段弹出来的“隐私协议”（或“隐私政策”）。但是，当仔细审读这些“隐私协议”时，我们会发现这类常见的“隐私协议”约定的实际主要内容并不是关于隐私的，而是关于个人信息保护的。这就引出了我们首先需要辨析的第一组法律术语——隐私和个人信息。

我国《民法典》第四编“人格权”第六章专章规定了隐私权和个人信息保护。隐私权作为一项重要的人格权，主要通过《民法典》人格权编的规则予以保护，并辅以相应的单行法和司法解释，形成周延的保护。《民法典》第一千零三十二条规定了自然人享有的隐私权及隐私覆盖的范围：“自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄

露、公开等方式侵害他人的隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。”

在个人信息保护方面，《民法典》第一千零三十四条则规定：“自然人的个人信息受法律保护。个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。”

隐私与个人信息之间存在一种微妙的联系，这导致许多人难以明确区分法律上的隐私与个人信息。在不对比这两个概念的情况下，很多人容易将隐私与个人信息等同起来。然而，尽管二者存在交集，它们却是截然不同的法律概念。《民法典》第一千零三十二条在定义隐私时，将个人不愿意被他人了解的私密信息纳入了隐私范畴；而私密信息本身也构成了个人信息的一部分，与《民法典》第一千零三十四条所规定的个人生物识别信息、健康信息、行踪信息等形成了相互交织和重叠的关系。因此，在法律语境中，虽然隐私与个人信息存在一定程度的重叠，但它们仍是具有不同内涵和法律保护要求的独立概念。从法律规范适用的视角出发，隐私权与个人信息权益保护在一定程度上的交汇表现为法律规范之间的竞合，因此，在处理涉及隐私权与个人信息权益的问题时，应当充分注意法律的选择适用。

区分隐私和个人信息，主要应当从以下五个方面入手。

一、权利属性不同

隐私权主要表现为一种精神性的人格权，关注的是个人在私密领域的尊严、名誉和心理安宁。隐私权保护的是个人免受他人侵犯的权利，使其能够独立地控制与自己相关的私密信息。相较之下，个人信息权益

则是一种综合性权益——既包括精神性利益，又包括财产性利益。其关注的是个人数据的处理、使用和保护，以确保个人信息的安全、完整和可控。在实际运用中，个人信息权益的保护和利用应当并重，既要维护个人的隐私尊严，又要确保个人信息的合法合规使用，以充分发挥信息资源的价值。

二、权利的主、被动性不同

隐私权作为一种被动性的人格权，主要是保护个人免受他人对其私密生活的侵犯。这意味着隐私权着重维护个人私生活的安宁，确保个人的私密信息不被他人公开披露，以及保障个人在私生活领域的自主决定权。隐私权的保护主要表现为防范和制止他人对个人隐私的侵犯行为，如偷窥、监听、泄露个人信息等。相对而言，个人信息权益作为一种主动性的人格权，更注重的是个人对自己信息的支配和决定。权利人不仅可以被动地防御他人对其信息的侵犯，还具有排他性、积极性和能动性地控制和利用自己的个人信息的权利。个人信息权益的主要内容包括权利人在个人信息的收集、存储、处理、使用和传播等方面的知情权、同意权、访问权、更正权、删除权、限制处理权和数据携带权等。这些权利赋予了权利人在信息处理过程中更多的自主权，以维护个人信息的安全和个人隐私。

三、授权同意标准不同

隐私权涉及个人不愿被他人知晓的私密信息，保护的是个人私生活的安宁和尊严。因此，《民法典》在侵犯隐私权的免责事由中要求必须经过“权利人明确同意”，表明只有在权利人明确表示同意的情况下，其他主体才能合法地收集、使用或披露其隐私信息。这样的规定有利于强化对隐私权的保护力度，避免权利人在不知情或不清楚的情况下被剥