EY安永
Building a better working world

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

2023-2024

# 全球数据流通与隐私科技发展报告

# GLOBAL DATA CIRCULATION AND PRIVACY TECHNOLOGY DEVELOPMENT REPORT

# 版权声明

## COPYRIGHT STATEMENT



**出品方**

安永（中国）企业咨询有限公司

上海赛博网络安全产业创新研究院

# FOREWORD

# 前 言

近年来，全球经济结构逐渐变化，人工智能等科技的崛起重塑着数字世界，数字化对全球经济面貌的影响持续加深，数据要素的重要程度提升；与此同时，主要国家和地区的数据安全与隐私保护法律法规均已走向成熟，而地缘政治也在影响着不同国家与地区的数据安全合规政策，数据流通与安全合规之间的不对称却呈现加剧的趋势。此外，数字世界仍持续面临着内外部的恶意攻击与频繁掠夺，数据安全与隐私保护与数据流通之间的平衡成为影响数字经济发展的关键因子。在此背景下，安永（中国）企业咨询有限公司（下文简称安永）与赛博研究院联合发布 2023–2024 年度《全球数据流通与隐私科技发展报告》。本报告全面梳理了国内外隐私保护与数据要素政策，对隐私科技的概念、内涵和外延进行更新，并通过对多行业头部企业的问卷调研，覆盖政府与公共部门、金融、消费品、生命科学、制造业等行业，客观了解企业数据合规与数据流通的现状与隐私科技的需求，并为企业数据流通实践提供参考案例与创新思路，供业内参考。

## 主要发现

- 中国、美国、欧洲、日本等全球主要经济体均已制定数据保护相关法律法规，且区域间数据跨境流动合作逐渐加深。同时，中国在数据要素流通领域的政策支持力度与制度建设走在世界前列。

- 企业的数据合规与隐私保护工作成熟度进一步提高，未建立针对性的方针、制度与流程的企业比例进一步降低。同时，企业并未放松数据合规与隐私保护工作，根据 2023–2024 年度安永调研，94% 的企业设有数据合规与隐私保护岗位，各公司负责数据合规与隐私保护的人员规模也稳中有增，只有 11% 的企业认为在数据合规与隐私保护的投入不满足需求。

- 数据出境成为企业目前数据合规工作中的难点，大部分参与调研的企业已开始了数据出境合规工作，但仍有部分尚未完成数据出境安全评估申报工作，选择合适的数据出境合规路径与业务场景复杂难以厘清是阻碍企业数据出境合规的最大困难。

- 国内数据要素市场数据仍处于起步阶段，数据交易规模仍较小，且业务场景较为有限。有 33% 的企业已开始开展数据交易和数据共享的业务，多数开展了数据交易的企业将数据用于产品优化中。安全合规不是企业数据交易的最主要困难，阻碍企业进行数据交易、共享的最大障碍是难以明确数据价值、缺少交易平台和缺少良好的数据供应方。

- 更多企业发现隐私计算的价值并付诸实践，隐私计算在更多风险控制和数据流通等业务场景中发挥着重要作用。在未来十二个月，更多企业选择保持对隐私科技的投入水平，力图稳中求进。

# CONTENTS | 目录

# 01

## 第一章 CHAPTER 1

# 数据经济时代的数据要素流通面临的机遇与挑战

EY安永
Building a better working world

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

01

# 第一章 CHAPTER 1
# 数据经济时代的数据要素流通面临的机遇与挑战

## 1.1 数据要素流通相关概念介绍

本报告首先对数据要素、数据要素流通、个人信息、隐私、数据安全、数据合规、隐私保护、隐私科技等概念及其关系进行界定，便于后续内容的理解。

信息被认为是和物质、能量并列的构成世界的三大要素之一。国际上较为经典的定义包括：信息是“用来消除不确定性的事物”（香农 1948）；信息是“我们在适应外部世界，控制外部世界的过程中同外部世界交换的内容”（维纳，1948）；中国国家标准《情报与文献工作词汇基本术语》（GB489885）将信息定义为“物质存在的一种方式、形态或运动形态，也是事物的一种普遍属性，一般指数据、消息中所包含的意义，可以使消息中所描述事件中的不确定性减少”。

数据是信息的表现形式，是为了让人们更好地使用或处理信息的一种编码形式。数据原本表示事物性质 / 数量变化的数值集合，最早应用于科学测量领域。随着现代信息技术发展，人们开始利用电子计算机和现代通信技术获取、加工、传递和利用信息，越来越多的信息通过计算机进行数字化编码并以数据库的形式存储，数据的内涵也因此开始扩大，不仅指代“有根据的数字”或是“计算加工的数字”，而且是成为“数字、文本、图片、视频”等一切信息类型在信息技术环境下的记录。现代信息技术发展丰富了数据的内涵，使得人类对数据资源的采集、生产、开发、保存等能力得到空前提升。企业、政府、个人都直接参与到了数据生产和消费。数据类型不仅包括结构化数据，还包括越来越多的非结构化数据。根据《中华人民共和国数据安全法》的定义，数据为“任何以电子或者其他方式对信息的记录”。根据重要敏感程度，数据可分为一般数据、重要数据、核心数据。其中，“核心数据”是关乎国家安全、国民经济命脉、重要民生、重大公共利益等数据，“重要数据”是与国家安全、经济发展，以及社会公共利

益密切相关的数据，其包含核心数据，两者主要在保护密级方面有一定区别。“一般数据”包括个人数据、企业经营数据等一般性数据。

数据要素是指以电子形式存在的、通过计算的方式参与到生产经营活动并发挥重要价值的数据资源。在数字经济中，数据要素的角色可与传统的生产要素（如劳动力、资本和土地）相提并论。数据要素是推动数字经济发展的核心引擎，是赋能行业数字化转型和智能化升级的重要支撑，也是国家基础性战略资源。

数据要素流通是指数据在不同实体或系统之间按照一定规则和标准进行流动和交换，数据要素流通是发挥数据要素潜在经济价值的主要方式之一。当前，根据数据与资金在主体间的流向进行划分，数据要素流通可以分为三种形式——开放、共享和交易。

个人信息是信息的一部分，是从个人相关数据中提炼出来的与个人有关的描述。根据《中华人民共和国个人信息保护法》和欧盟《通用数据保护条例》，个人信息可定义为“与已识别或者可识别的自然人有关的各种信息”。

隐私与个人信息存在交叉关系，但不能等同。根据《牛津词典》的解释，隐私是指独处不受干扰的状况；不受干扰或不受公众注目的自由。隐私是一个不断变迁、发展的概念，尤其是现代信息技术发展，作为法律概念的隐私权需求开始兴起，并在保护个人私域和个人自由方面呈现出传统财产权保护不可替代的作用。《中华人民共和国民法典》第1032 条指出“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”。其中，私密信息涉及敏感个人信息。

数据安全是指数据不被威胁的状态。当前，核心数据、重要数据、个人信息尤其个人敏感信息等是数据安全的重点保障范围，需要采取必要措施、确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

数据合规是推动数据安全实践的驱动力。以企业数据合规为例，是指企业经营管理行为要符合国家法律、行政法规、国际法律条约、行业准则、商业道德以及企业内部的管理制度。建设企业数据合规体系的构成要素包括：①管理层承诺；②风险评估；③流程嵌入；④记录保存。当前，数据合规既是企业安全治理体系和治理能力现代化的重要标志，也是国家安全治理体系和治理能力现代化的重要组成部分。

隐私增强技术 (PETs) 是一系列收集、处理、分析和共享信息，同时保护个人数据机密性的数字技术和方法的集合。目前，个人数据的收集和处理方法发生了变化。由于 PETs 能够从数据中获得相对较高的效用并最大限度地减少数据收集和处理的需求，在技术层面上更好地保护个人数据隐私，使社会更接近隐私设计（Privacy by Design，PbD）的过程和实践，所以该项技术逐渐成为隐私和数据保护新范式的基础。PETs 改变了组织收集、访问和处理数据（尤其是个人数据）的方式，为数据主体提供了更多的控制力，有助于增强对数据共享和数据重用的信任，提升数据安全和隐私保护。例如，对于无法在个人或实体之间公开的敏感数据，就可以利用 PETs 实现数据的协作分析。

在 2023 年发布的《2022–2023 全球数据合规与隐私科技发展报告》中我们将隐私科技定义为：在日常运营流程中，通过嵌入 IT 架构和业务场景支撑主体数据合规和隐私保护的一系列工具、服务及技术解决方案。今年，《2023–2024 全球数据流通与隐私科技发展报告》基于对国内外数据要素流通现状的深度研究，对隐私科技框架进行了更新与完

善，主要体现在凸显了隐私科技对于解决数据要素流通中的难点、堵点问题的关键作用。现将隐私科技定义更新为：在日常运营流程中，通过嵌入 IT 架构和业务场景支撑主体数据安全、合规流通，充分发挥数据潜在经济价值，实现数据保护与数据利用平衡的一系列工具、服务及技术解决方案。通过将隐私科技应用于各类数据流通实际场景中，在保证数据安全、可信流通的基础上，进一步推动数据高效流通、共享与开放，实现数据充分开发利用的目的。


图 1.1 数据要素流通相关概念介绍

## 1.2 数据要素流通的机遇与趋势

数据作为当今数字经济时代推动发展的核心动力之一，其全球战略地位正在不断攀升。我国于 2020 年 4 月在《关于构建更加完善的要素市场化配置体制机制的意见》中，首次将数据纳入生产要素范围，将其列为与土地、劳动力、资产、技术同等地位的第五大生产要素，并提出加快培育数据要素市场。此后，我国发布一系列政策文件，大力推动数据要素流通，鼓励充分挖掘数据要素潜在价值。为统筹数据资源，实现数据的整合共享和开发利用，我国成立了国家级、省级数据局，通过统一规划和管理，打破数据分散在不同行业和部门中导致的“数据孤岛”，促进数据的流通和共享，挖掘数据的潜在价值，为经济增长和创新发展提供强大动力。而在数据要素流通基础设施建设方面，我国积极开展“东数西算”工程，旨在优化全国算力资源的配置，实现东西部算力资源的互补和协同。通过构建全国一体化的算力网络，我国加强了数据存储、处理和分析的能力，为数据要素的高效利用提供了坚实的技术支撑。除我国外，域外多个国家及地区也已采取系列措施促进数据流通，发挥数据经济价值。例如美国就公共数据的开放利用已形成较为完备的法律法规体系并构建国家级开放管理平台，积极探索探究市场导向的数据运营模式，在确保数据安全和隐私保护的前提下加速公共数据的应用。

## 1.3 数据要素流通面临的挑战

**（1）仍待完善的法律法规与相关标准**

我国当前已经制定了一系列与数据要素流通相关的法律法规，但仍存在部分立法空白及不足之处。首先，目前我国尚未建立起完备的数据要素流通规制法律体系，在数据权属、交易规则、定价机制及利益分配等方面仅出台了总纲性质的整体建设方向指引文件，但仍缺乏明确系统化且可实际落地的操作规范。例如，在数据权属方面虽为解决数据确权难的问题提出了“三权分置”的权限划分机制，但未对其权利登记等确权细节及具体的权利划分界限、主体范围给出可操作参照。在交易流程方面，目前也尚未建立其标准化的规则，导致企业在进行数据交易时需要花费较大成本进行商务安全合规判断及利益分配磋商。其次，当前我国数据分类分级标准尚未统一，不同行业间对数据的分级分类管理要求存在差异，增加了数据要素流通的复杂性。此外，有关跨境数据流动的相关规定有待进一步完善，在保障数据安全与促进数据国际流通、合作之间需要更加精准的平衡。例如我国目前对于自贸区数据跨境流通提出了负面数据清单制度，但仅有个别自贸区开展了负面清单的制定，其落地较难，且负面清单的本身的合理性也存在争议。因此，如何进一步完善法律法规体系，制定统一的数据要素流通标准，是未来亟需解决的重要问题。

**（2）数据频繁流通引发的安全与隐私威胁**

数据要素的频繁流通在带来巨大经济利益的同时，也引发了一系列数据安全与隐私泄露问题。数据在采集、传输、存储和使用全生命周期中均面临被非法获取、篡改或删除的风险，可能导致重要信息泄露或系统瘫痪，频繁的数据流通无疑会大幅度增加以上风险。其次，逐渐深化的数据合作开发更使个人隐私保护面临新的挑战，例如典型的数据合作开发项目大数据分析技术，其使得个人信息更容易被精准识别和关联，增加了隐私泄露的可能性和后果的严重性。此外，当前数据滥用问题日益突出，部分企业及个人违反法律法规利用数据从事非法活动或不正当竞争，在目前多数数据流通活动尚缺乏完善的合规管理的背景下，以上问题将会更加泛滥。故当下如何在促进数据要素流通的同时，有效保障数据安全和个人隐私，是相关主体正在面临的严峻挑战。

**（3）数据要素市场仍不成熟**

近年来，数据要素市场虽处于高速发展阶段，但整体上仍处于初级阶段，数据要素市场培育的基础尚不坚实。目前数据要素的价值评估体系尚未完善，企业在数据交易、合作中难以高效、准确地衡量数据的经济价值，极易产生定价纠纷，严重影响了数据交易的质量和效率。而在数据交易模式方面，我国目前鼓励通过数据交易平台进行场内交易，但绝大多数数据交易仍系企业间自主进行的场外交易，据信通院统计，当前我国数据交易仅有 25% 为场内交易[1]。以上现状主要是由于当前我国当前数据交易平台建设尚不完善，除交易平台数量不足外，交易平台管理和运营也未形成科学高效的体系，极大限制了数据要素的高效流通。此外，当前我国数据要素市场的参与主体多元化程度较低，高质量数据的供应源头不足，数据供给端和需求端的匹配度不高，企业往往需要花费大量成本验证合作方的相关资质、数据保护能力及数据质量等信息，严重影响数据合作效率。以上可见，为有效控制数据流通成本，提

升数据流通效率，培育成熟的数据要素市场，完善市场运行机制，是未来发展的重要方向。

**（4）数据应用挖掘不足**

数据要素的价值在于应用，然而当前数据应用挖掘的深度和广度仍有待提升。许多企业和组织虽然拥有大量数据，但缺乏与之相匹配的数据分析和应用能力，导致数据资源未能充分发挥价值。除企业自身数据能力需要提升外，数据应用领域和行业也有待进一步开拓，当前我国成规模的数据应用领域主要集中在精准营销和信贷服务上，其他领域的市场规模仍然非常有限，甚至尚未形成有效的市场，数据创新应用的意识和能力还有待提升，特别是在传统行业中，数据驱动的创新模式尚未得到广泛应用。此外，数据要素的价值发掘离不开相关领域专业人才的培育，当前我国基础知识储备扎实且实践经验丰富的数据人才十分短缺，这也很大程度制约了数据应用的深入发展。因此，如何提高数据应用挖掘能力，充分释放数据要素的潜在价值，是数据经济时代的重要课题之一。

# 02

## 第二章 CHAPTER 2

# 数据要素流通制度建设及现状

EY安永 Building a better working world
SICSI CYBER RESEARCH INSTITUTE 赛博研究院

02

# 第二章 CHAPTER 2
# 数据要素流通制度建设及现状

在当今数字化时代，全球数据流通与市场化建设正成为推动经济增长和技术创新的关键动力。随着数据的价值在全球范围内被广泛认可，各国政府和国际组织纷纷致力于构建更加开放、安全和高效的数据流通体系，旨在促进数据资源的优化配置，激发数据驱动的创新活动，并确保数据流动的合规性和安全性。本节将对于域外及我国数据要素流通制度体系建设情况及要点进行详细分析。

## 2.1 域外数据要素流通制度建设及安全合规立法现状

**（1）美国**

在数据要素流通制度建设方面，美国将商业利益作为其数据政策的首要考量，致力于推进数据要素的市场化进程。通过倡导数据的自由流动和开放获取，旨在积累和控制更多的全球数据资产，进而巩固其企业在技术和市场领域的领先地位。

在数据产权方面，美国国会曾于 1996 提出建立数据库产权立法，但由于其可能削弱国家的研究能力而遭到美国国家教育协会、美国图书馆协会、美国国家科学院和美国国家工程院等组织强烈反对，近年来美国国内逐渐形成对数据确立产权可能会形成垄断的共识。对于政府公共数据的公开共享，美国采取大力支持推进的态度，其于 1966 年发布的《信息自由法》首次确定了政府信息“以公开为原则、不公开为例外”的基本原则，后于 2009 年发布《开放政府法》及《开放政府指令》要求联邦机构更积极地披露政府信息，并为公众获取政府记录提供更便捷的途径，加强数据共享和协作。而《政府信息公开和机器可读行政命令》和《联邦数据战略与 2020 年行动计划》则进一步明确了政府数据开放的原则、基本框架、数据基础设施建设和标准实践等内容。在地方层面，美国目前已有 16 个州发布相关规定，要求行政部门开放数据。而针对数据交易，美国当前以数据经纪交易作为其主要交易方式，鼓励数据自由交易。数据经纪商通过搜集、整合、分析和处理各类用户数据，构建出详尽的消费者画像、身份验证信息和个性化数据档案等数据产品，并将其销售给需要这些信息的企业和组织，用于目标市场营销、风险管理以及监测竞争者动态等目的。这些数据经纪商的数据获取途径多样，包括利用政府数据开放平台、向信用卡公司等机构购买数据、通过互联网爬虫抓取在线信息，以及收集各种线下资源数据。此外，为建立国际数据合作，美国也已开始致力于全球数据传输机制的建设，2023 年 6 月美国和

英国联合发布了《大西洋宪章：21 世纪美英经济伙伴关系框架》，同时宣布启动美英数据桥项目，旨在在确保严格的隐私保护措施的前提下，加强两国数据的互通性。随后于同年 7 月 10 日，欧盟委员会批准了欧盟 – 美国数据隐私框架（即隐私盾 2.0），此外，美国也正在与印度、巴西、印尼等国家就跨境数据问题展开多边磋商 [2]。

为确保数据流通中的个人隐私和数据安全，近年来美国就隐私保护颁布了一系列相关法案。1974 年，美国实施的《隐私法案》对政府机构应当如何收集个人信息、收集到的个人信息如何向公众开放及信息主体的权利等做出了详细规定。此后，美国采取分行业的分散立法模式，在金融、健康、教育、消费等行业领域制定数据保护规范。同时，美国多个州在其原有的个人信息保护法律基础上作出修订，进一步扩展“个人信息”定义，补充数据安全法律法规细节。今年，美国联邦层面由总统签发《敏感数据行政令》限制有关国家通过商业方式获取美国个人和政府的敏感信息，主要针对“数据承包商”等成批处理、出售或转让美国个人数据的公司。此外，美国国会也于今年通过了针对个人信息和数据隐私保护的《隐私权法案（草案）》，这是自 2022 年“ADPPA”之后，美国再次进行联邦层面统一的隐私保护立法 [3]。整体来看，美国的数据安全立法错综复杂仍缺乏统筹性的数据安全法案，但近一年来，美国已经开始启动联邦层面的隐私保护建设，以期形成全国统一的隐私保护标准，结束各州隐私法规混杂的局面。

**（2）欧盟**

数据要素的流通和市场化制度建设是欧盟推动数字经济转型的关键一环。欧盟通过一系列创新政策和法规，致力于构建一个安全、透明且高效的数据流通环境，实现数据驱动的创新和增长。

在数据要素流通制度体系建设方面，欧盟于 2003 年首次发布《公共部门信息再利用指令》，后于 2013 年和 2019 年进行修订，指令规定了公共部门信息范围、使用公共信息的授权、用户最感兴趣和最常使用的信息类型，以及公共部门应如何收费等内容。自 2019 年起，欧盟又逐步采取了一系列相关重要措施。《欧盟非个人数据自由流动条例》（FFD）的发布为商业数据的自由流动提供了基础性指导，确保数据在成员国间顺畅流通。随后，《欧洲数据战略》于 2020 年发布，旨在通过统一的数据治理框架、加强基础设施投资、提升数据权利意识和技能，以及构建公共欧洲数据空间等措施，完善数据市场的法律体系。为了达成其战略目标，欧盟还构建了“共同数据空间”实操平台和工具集，旨在促进特定关键领域的数据共享和利用。2021 年，《数据治理法案》（DGA）的出台进一步促进了数据共享，鼓励公共部门数据的再利用和企业间的数据交易。而 2022 年发布的《数据法案》（Data Act）对不同主体、数据类型和交易场景进行了细化规范，并为潜在的权利冲突设计了监管模式和争端解决机制 [4]。

而在数据安全保障方面，欧盟在数据安全和个人信息保护方面设立了一套在全球范围内容较为全面且严格的保障措施，形成了成熟而完备的数据保护体系框架。欧盟理事会和欧洲议会于 2016 年 4 月通过了《通用数据保护条例》（简称“GDPR”），该条例于 2018 年正式生效，GDPR 作为欧盟数据安全法律体系的核心，使得欧盟个人数据保护及监管达到新高峰。此后，欧盟以 GDPR 为基础，建立了统一的数据安全治理框架。2018 年 11 月欧盟颁布《非个人数据自由流动条例》统一非个人数据的自由流动，与 GDPR 共同构成了数据安全领域的关键立法体系，实现数据安全与数据流通的平衡；《电子隐私条例》作为 GDPR 在电子通信领域起细化和补充作用的特

别法，两者在监管规则上保持一定的一致性；2023 年 1 月，欧盟就电子证据的相关法规和指令草案达成协议，有关当局可直接向其他成员国的服务提供者发送获取电子证据的司法令，形成国际跨境司法协助和数据治理的新机制；而《为保持欧盟个人数据保护级别而采用的数据跨境转移工具全球数据合规与隐私科技发展报告 Global Data Compliance and Privacy Technology Development Report 06 补充措施》则为数据跨境流动中的数据保护问题提供进一步指导 [5]。

**（3）其他国家地区**

日本当前采用政府和企业共同协作为核心的数据要素发展策略，旨在加速社会的数字化转型进程，并促进数据的跨境流动。该国还提倡确保数据的可信流通，以支持和加强跨国数据的自由交换。日本政府在数字化转型的进程中采取了积极的措施，于 2021 年 9 月 1 日成立了数字厅，成为全球首个设立专门数据管理机构的国家。数字厅的职责包括监督国家信息系统的运行、促进中央与地方政府间的信息共享、与医疗、教育、防灾等领域的公共机构合作开发信息系统，以及整合来自土地、交通等私营部门的数据资源。在推动数据跨境流通方面，日本一直倡导数据的自由流动。2019 年 2 月，日本与欧盟签订《欧盟日本数据共享协议》旨在促进两个经济体之间数据的自由流动，并为数据驱动的创新和经济增长提供坚实的法律基础。2019 年 6 月，在 G20 大阪峰会上，日本提出建立“数据流通圈”的倡议，主张在确保数据安全的前提下，适当放宽个人数据保护标准，以促进跨境数据的顺畅流动，实现“基于信任的数据自由流动”。今年 7 月 1 日，日本与欧盟签订的《欧盟 – 日本关于跨境数据流动的协议》正式生效，该协议同时被纳入《欧盟 – 日本经济伙伴关系协定》，其条款将促进双方的业务发展，并反映出对数字保护主义的反对信号。在数据安全方面，2003 年 5 月日本《个人信息保护法》正式通过并于 2005 年 4 月 1 日正式施行，该法在《行政机关计算机处理的个人信息保护法》的基础上制定，对日本个人信息保护基本理念方针等总则性内容及与民间企业相关的一般法性内容进行了规定，系日本个人信息保护法制体系的基石，日本的个人信息保护法对个人信息处理活动的规范相对较为宽松，注重个人信息保护与数据合理利用的平衡。为《个人信息保护法》更好落地，日本地方公共团体信息系统机构对应修订了《个人信息保护基本方针》，旨在“确保行政机关等的事务和业务正常、顺利地进行，并确保个人信息的正确、有效的使用。

韩国在数据要素流通制度建设方面采取了一系列措施，以促进数据的自由流动和有效利用，同时确保数据安全和个人隐私保护。韩国政府推出“韩国数字战略”，旨在打造全球顶级水平的数字力量，扩大数字经济的覆盖范围，提升数字经济的包容性，构建政府数字平台和推动数字文化创新。在组织管理层面，韩国成立了国家数据政策委员会，承担着国家数据及新兴产业政策的统筹与监管职责。该委员会负责审查与国家数据政策相关的重大议题，并定期每三年更新《数据产业振兴基本计划》。韩国在数据产业的培育方面采取了积极措施。该国于 2021 年 10 月 12 日颁布了全球首部针对数据产业的基本法律——《数据产业振兴及利用促进基本法》，旨在通过法律手段推动数据产业的蓬勃发展和数据经济的全面振兴，从而在全球范围内率先确立了数据产业发展的先驱地位。而韩国的数据安全立法则体现了该国对于个人信息保护的高度重视和对数据驱动经济的积极适应。2011 年 3 月 29 日韩国颁布了《个人信息保护法》作为韩国在个人数据保护领域的基石，明确了韩国个人信息保护的统一性原则、

要求及参考标准，并发布《个人信息保护法施行令》，明确《个人信息保护法》授权的事项及实施所需的事项，帮助其进一步落地，2023 年 3 月 14 日韩国对《个人信息保护法》进行了部分修订以适应时代发展新变化。除统一性法律文件外，韩国在各行业不同场景下也制定了相应的数据保护法律法规，《信息通信网络利用促进和信息保护法》对电信业个人信用信息的收集、使用与保护进行全面和具体的规范；《信用信息使用和保护法》则是韩国关于金融业商业交易中信用信息提供和使用的法规，致力于健全信用信息相关产业，促进信用信息的有效使用和系统管理，妥善保护个人生活机密，防止信用信息被滥用和滥用；针对位置信息安全，韩国制定《位置信息保护和使用法》保护隐私权，防止位置信息的泄露、滥用和误用，提供安全的位置信息使用环境，激活位置信息的使用。

## 2.2 我国数据要素流通政策支持及制度建设现状

自数据被正式确立为我国五大生产要素之一后，我国随之发布了一系列数据要素安全、合规流通支持政策及法律法规等规范性文件，已初步建立起数据要素流通制度体系，确保在安全、合规的前提下推动数据充分流通，最大程度发挥数据潜在价值。

**（1）中央层面**

在全国范围，我国中共中央、国务院在 2020 年 4 月发布《关于构建更加完善的要素市场化配置体制机制的意见》中，将数据纳入生产要素范围，将其列为与土地、劳动力、资产、技术同等地位的第五大生产要素。2021 年底国务院制定“十四五”数字经济发展规划，是中国为推动数字经济高质量发展而制定的国家级专项规划，它明确了总体要求、主要任务、重点工程和保障措施，旨在通过优化升级数字基础设施、充分发挥数据要素作用、大力推进产业数字化转型、加快推动数字产业化、持续提升公共服务数字化水平、健全完善数字经济治理体系。而《国务院关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“意见”）（数据二十条）的发布则全面提出了构建数据基础制度体系的总体要求和具体措施，明确了数据产权制度的建立，强调了数据产权结构性分置的重要性，并提出了数据分类分级确权授权使用和市场化流通交易。同时，意见提出了建立合规高效、场内外结合的数据要素流通和交易制度，以及建立体现效率、促进公平的数据要素收益分配制度。为进一步落实“数据二十条”，我国资产评估协会于 2023 年发布《数据资产评估指导意见》明确了数据资产的定义，涵盖了数据资产评估的基本遵循、评估对象、操作要求、评估方法和披露要求等内容。财政部发布的《企业数据资源相关会计处理暂行规定》为数据资产入表提供了明确的操作指引。为激活数据要素潜能，释放新质生产力，我国于 2023 年底成立国家数据局统筹推进数字中国、数字经济、数字社会规划和建设。今年数据局发布 《“数据要素 ×”三年行动计划》强调了数据要素在工业制造、现代农业、商贸流通、交通运输、金融服务、科技创新、文化旅游、医疗健康、应急管理、气象服务、城市治理、绿色低碳等 12 个行业和领域的关键作用。行动计划的主要目标是到 2026 年底，数据要素应用的广度和深度显著拓展，数据要素乘数效应在经济发展领域得到显现，形成 300 个以上的典型应用场景，培育一批数据商和第三方专业服务机构，数据产品和服务质量效益明显提升，数据产业年均增速超过 20%。国家数据局将会同有关部门加强组织领导，开展试点工作，推动以赛促用，加强资金支持，加强宣传推广，确保行动计划的实

施效果。这一行动计划是中国推动数据要素市场化配置、促进数字经济发展的重要举措，对于构建以数据为关键要素的数字经济具有重要意义。

在促进数据要素流通的同时，我国同样重视数据利用的安全合规。在民法、行政法、刑法的立法框架上，我国形成了由三部单行法——《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》）与《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》）组成的数据安全立法体系，分别适用于境内所有网络运营者的包含处理个人信息及数据在内的行为、所有主体处理网络数据和非网络数据的行为、个人信息保护。在三部单行法律框架下，我国近年陆续出台相关法规、规章、部门文件及重要标准，针对特定领域、特定场景下的数据合规要求和落地指引制定了详细规定。在行政法规方面，《关键信息基础设施保护条例》对关键基础设施的认定保护及其运营者责任义务进行了明确规定，而《网络数据安全管理条例》则在三部法律的基础上，细化了数据处理者相应的数据安全保护责任和义务并对核心数据、重要数据的定义进行了阐释，给予数据处理者落地数据安全合规更加清晰细化的标准。在部门规章方面，由于不同行业、场景及对象数据安全保护侧重点存在差异，我国相关部门针对各自主管领域出台了一系列规章指导数据处理者等相关主体进行安全合规工作，例如在出境场景中颁布《个人信息出境标准合同办法》《数据出境安全评估办法》等规章明确数据出境合规路径具体操作要点，而今年出台的《促进和规范数据跨境流动规定》则豁免了部分重要级别较低数据的跨境合规要求，减轻了企业不必要的合规负担。在子领域方面，我国有《汽车数据安全管理若干规定（试行）》《生成式人工智能服务管理暂行办法》《电信和互联网用户个人信息保护规定》等规章，就各不同行业领域数据合规问题制定个性化制度。此外在部门文件方面，《互联网信息服务深度合成管理规定》《个人信息合规审计管理办法（征求意见稿）》等文件则是对于法律法规的要求进行了进一步可落地化。在国家标准方面，数据合规重要领域金融行业已有《个人金融信息保护技术规范》《金融数据安全数据生命周期安全规范》等标准对金融行业数据保护进行特别规制，在数据体量庞大的重点监管领域——互联网行业则出台了《电信和互联网数据安全评估规范》就互联网领域数据安全评估工作设置体系化的流程方案。在汽车领域也出台了《汽车采集数据处理安全指南》等标准，规定了汽车制造商对汽车采集数据的传输、存储和出境等处理活动的安全要求，为汽车制造商开展汽车的设计、生产、销售、使用、运维提供数据保护实施规范。此外，近年我国对于三部单行法中细节性的要求也进行了再规范，消除法律专业名词歧义，帮助企业顺利落地相关规定，就个人信息保护脱敏、告知同意等细节问题发布新标，《个人信息去标识化效果评估指南》明确了个人信息去标识化效果评定流程，并在附录给出了可参考的计算方法和阈值推荐，为去标识化技术的落地发展提供了更明确的指引；《个人信息处理中告知和同意的实施指南》则详述了告知同意的适用情形、基本原则、实施方式等内容。

**（2）地方层面**

在中央统一出台的政策法规以外，我国各省也针对本省内部数据要素流通实际情况制定了一系列相关制度和规范。

北京是我国目前数据要素制度建设较为成熟的地区之一，在制度创新优化方面采取了积极措施。2023 年 6 月北京市发布《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》（北京“数据二十条”），旨在探索建立结构性分置的数据产权制度，明确数据来源、持有、加工、流通、使用过

程中各参与方的合法权利；开展数据资产登记，推动数据资产评估和入表，探索数据资产金融创新；建设一体化数据流通体系，推进社会数据有序流通，鼓励数据商进场交易。后续又陆续发布《北京市企业数据知识产权工作指引（试行）》《北京市公共数据专区授权运营管理办法（试行）》及《北京市西城区加快推进数据要素市场高质量发展的若干措施（征求意见稿）》等文件，旨在通过政策引导和市场运作，促进数据资源的有效利用和安全流通，推动数字经济的高质量发展。此外，北京市还启动了全国首个数据基础制度先行区，规划了“2+5+N”的数据先行区基础架构，以推动数据要素市场的发展。到 2030 年，北京市的目标是数据要素市场规模达到 2000 亿元人民币，基本完成国家数据基础制度先行先试工作，形成数据服务产业集聚区。

上海则是以 2021 年发布的《上海市数据条例》为基础，辅以系列政府管理办法、规定、行动方案为主体，其他各类指南、实施细则等文件，构建了相对成熟且科学完善的数据要素管理体系。《上海市数据条例》旨在保护自然人、法人和非法人组织与数据相关的权益，规范数据处理活动，促进数据依法有序流动，保障数据安全，并加快数据要素市场培育。条例明确了数据的定义、数据处理活动的范围，以及数据安全的重要性。条例强调了公共数据的管理和开放，推动公共数据资源体系的建设，提高公共数据共享效率，扩大公共数据有序开放，并构建统一协调的公共数据运营机制。上海对公共数据的开放利用重视程度较高，今年发布的《上海市公共数据开放实施细则》《上海市公共数据共享实施办法（试行）》及《上海市公共数据开放 2023 年度重点工作安排》等文件对公共数据的开放共享方式、要求、主体及主要流程等具体操作规范进行了明确。此外，上海针对数据安全及个人信息保护开展了一系列专项行动，如“上海市铸盾车联车联网网络和数据安全专项行动”、“浦江护航数据安全专项行动”及“上海市电信和互联网行业网络和数据安全检查”等，旨在确保企业重要数据和个人信息处理的安全合规。

当前广东省在数据交易、流通方面呈现高速发展势态。2023 年深圳市和广东省分别发布了《深圳市数据交易管理暂行办法》和《广东省数据流通交易管理办法（试行）（征求意见稿）》强调了数据交易的合规性，明确了数据资源持有权、数据加工使用权和数据产品经营权等权利，并提出了数据价值评估指标体系，以激活数据资源的价值；明确了数据交易市场的各个主体，包括数据卖方、数据买方、数据商和第三方服务机构，并规定了其职责和运营要求。广东省还探索了数据经纪人制度，通过专业中介服务促进数据流通交易。此外，广州还发布了《广州市数据条例（征求意见稿）》规范了广州市数据管理体系，特别强调了南沙区在粤港澳大湾区数据合作中的重要作用，推动数据跨境流动和监管机制的创新。在数据安全合规方面，深圳于 2023 年发布了《深圳市企业数据合规指引》引导企业加强数据合规管理，提高数据合规意识与保护水平，内容涵盖了数据安全合规管理组织体系建设、数据合规管理制度体系建设、数据全生命周期合规、数据出境合规等方面。

其他各省市也基于地方情况出台了地方性数据要素相关法规及综合性数据立法。当前，贵州、天津、海南、山西、吉林、安徽、山东、辽宁、黑龙江、陕西、宁夏等地区面向公共数据领域，已出台大数据保护条例（包括草案）。厦门等地则出台发布《厦门经济特区数据条例》，不仅涉及公共数据，还涵盖了个人数据等相关规定。湖北、安徽、江苏、重庆等地还开展了系列网络及数据安全保护专项行动，兼顾数据的利用和安全合规。

## 2.3 隐私科技促进数据要素合规高效流通

当前高频率的数据流通中存在着不可忽视的数据安全及隐私泄露问题，数据交易共享都需要数据供方传输大量数据到数据需方，数据传输过程本身的安全合规性保障及后续对于需方数据安全能力的监督需要相关主体投入大量的时间和资金成本。此外，实际的数据交易共享过程中还存在数据供方“控制权保留”纠纷等问题，以上情况很大程度增加了数据流通时间及资金成本，可能严重影响数据流通积极性和效率。而隐私计算是在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，保障数据在流通与融合过程中的“可用不可见”，实现数据价值的转化和释放。在数据要素流通全过程中隐私计算能够发挥十分重要的作用，协助相关主体降低流通成本、提高流通效率。

**（1）实现数据“控制权”保留**

由于数据作为信息承载体的特殊性，在数据流通过程中其价值随着传播递减，传递次数越多，范围越广，价值耗损就越大，最终趋近于零，且数据供方往往难以在数据流通中掌握数据的“控制权”、难以追溯数据流转过程，使得其数据交易共享意愿降低。因此，在交易过程中确保数据要素不因提供、共享、融合而泄露或不受控制的传播，是保障数据要素有序流动的基础。而隐私计算一方面能够基于区块链技术构建数据共享平台，实现数据使用的全程可追溯、可审计，增强了数据流通的透明度和可信度，实现数据的可控可计量。另一方面，通过同态加密、安全多方计算等技术，实现在加密状态下对数据进行计算和分析，使各方仅可获得共同所需数据集合，并且辅以匿踪查询等技术措施，确保数据持有方无法知悉数据需求方查询信息内容，实现数据的数据可用不可见。

**（2）助推个人信息匿名化程度**

当前数据流通中存在着大量个人信息的流转，而对于个人信息保护我国法律法规提出了如授权同意等较高合规义务，这无疑增加了企业个人信息流通合规成本，而我国《个保法》及他国多部隐私法案中定义匿名化后的个人信息不再属于个人信息范畴，不需履行个人信息相关合规义务，例如我国《个人信息保护法》中将匿名化定义为“个人信息经过处理无法识别特定自然人且不能复原的过程”，这为企业个人信息流通提供了合规思路，即通过隐私计算实现数据的匿名化处理效果，在匿名化的前提下实现数据的“可用不可见”。但是随着大数据技术的发展和数据的泛在化，彻底实现匿名化难度较高，典型的例子是搜索记录的重新识别，美国在线网站曾经公布 2000 多万条匿名化处理的用户搜索记录，有研究人员通过把其中多条记录联合分析后，很容易就识别出特定个人的姓名和身份。在当前法律和行业标准尚未界定匿名化实现方式和验证标准的前提下，隐私科技技术需要对匿名化数据的重识别行为做出约束，通过规则设计避免算法运行过程中的中间态数据被重新识别到特定个人。

# 03

## 第三章 CHAPTER 3

# 企业隐私科技与数据流通应用现状调研

EY安永 Building a better working world
SICSI CYBER RESEARCH INSTITUTE 赛博研究院

03

# 第三章 CHAPTER 3
# 企业隐私科技与数据流通应用现状调研

在数字化时代，数据合规与隐私保护一直是企业关注的一大重点，企业开展数据合规与隐私保护工作不仅是为了遵守全球不断发展变化的法律法规要求，也是为了增强客户体验。在这两大目标驱动下，不少企业将数据合规和隐私保护视作企业的生命线。在《数据安全法》和《个人信息保护法》施行一年有余，本报告再次发起调研，了解和分析企业数据合规与隐私保护现状和趋势，包括数据合规与隐私保护人员、组织、流程和技术等方面。本次调研涉及多家头部企业，覆盖金融、政府与公共部门、汽车、消费品、生命科学、制造业等行业。

## 3.1 企业数据合规与数据流通概况

**1. 数据合规与隐私保护职能所属部门呈多元化**

今年有更多的被调查企业具备了数据合规和隐私保护职能，基本与去年的数值（98%）持平。《数据安全法》第四章明确了企业应遵循的数据安全保护义务，《个人信息保护法》第五章规定了企业作为个人信息处理者的义务，基于此越来越多企业在内部设立数据合规与隐私保护职能，推动企业内部履行合规义务。

信息安全部门、法务部门和合规部门仍然是数据合规与隐私保护工作的主要责任部门。调查结果显示，33% 的被调查企业信息安全部门需要担任部分数据合规与隐私保护职能，33% 的被调查企业合规部门和 44% 的被调查企业法务部门也需要担任部分职能。企业在考虑将数据合规与隐私保护职能安置到哪个部门时，可结合自身业务和组织架构进行设定，以更加符合和适应企业的需求。考虑到数据合规与隐私保护工作的复杂性和学科交互性，大部分被调查企业数据合规与隐私保护工作由多部门共同负责。

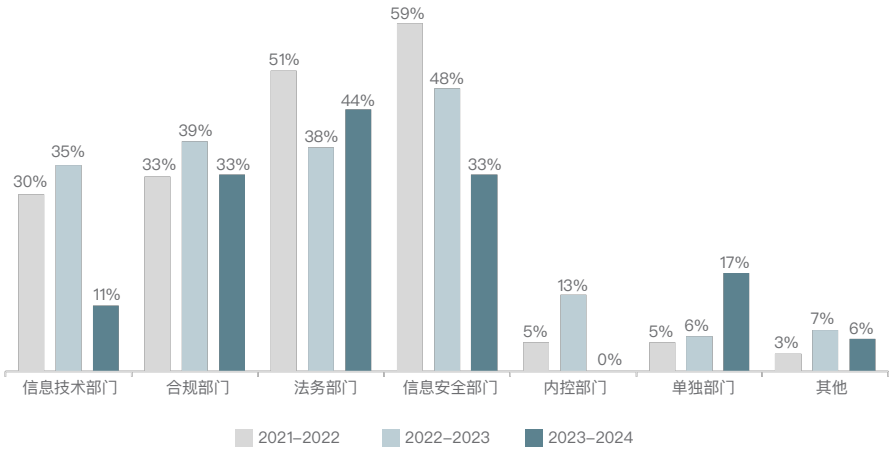



图 3.1 企业数据合规与隐私保护职能所属部门

与去年相比，信息安全部门和合规部门的占比有所下降，而法务部门、单独部门占比轻微上升。这些转变的出现可能是因为数据合规与隐私保护的合规条线的增加。除了常见的信息安全风险和合规风险，一些企业法务部门担任确保企业的数据处理活动符合国家的数据安全标准和要求的责任，法务部门需要通过专业的分析和评估，识别潜在的数据安全风险，并制定相应的应对措施。这有助于企业在面对数据安全挑战时，能够及时作出反应，减少潜在的法律风险和企业损失。法务部门还应进行适时地合规评估，确保企业的数据安全管理和保护措施符合国家和行业的标准。这包括对企业的数据安全政策、流程和技术的评估，以确保它们能够有效应对数据泄露、非法访问等安全事件，保护企业和个人的利益。

**2. 数据合规与隐私保护工作直接汇报角色有所转变**

法律事务部门主管成为当前数据合规与隐私保护工作的主要汇报对象，其次是首席信息官、首席运营官以及合规部门主管。

约 17% 的被调查企业的数据合规与隐私保护工作主要汇报对象为首席运营官、首席信息官及合规部门主管，而约 28% 的被调查企业的数据合规与隐私保护工作主要汇报对象为法务事务部门主管，与去年相比有明显的上升趋势。

这种变化说明，随着《个人信息保护法》和《数据安全法》施行以及监管部门的一系列执法行动，越来越多企业将数据合规与隐私保护工作视为企业应重点关注的事项。法务部门在保障数据安全方面扮演着至关重要的角色。首先，他们负责确保数据处理活动的合规性，这意味着他们需要密切关注相关的法律法规，确保企业的数据处理活动符合国家的数据安全标准和要求。这包括但不限于数据的收集、存储、使用、加工、传输、提供和公开等各个环节，确保这些活动都在法律允许的范围内进行。个保法第六十六条明确“严重违法行为可处五千万元人民币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”，违法违规事项不仅可能影响企业经营，也会影响消费者对企业的信任。

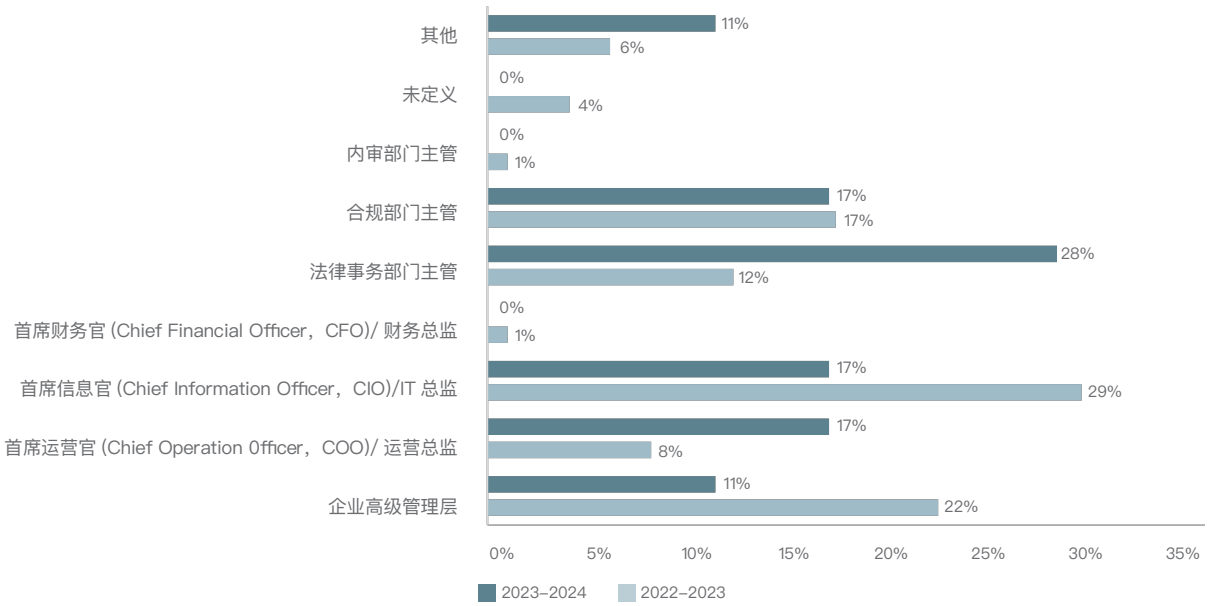



图 3.2 企业数据合规与隐私保护职能直接汇报工作的角色比例

**3. 大部分企业已委任数据安全负责人和个人信息保护负责人**

根据《数据安全法》第二十七条“重要数据的处理者应当明确数据安全负责人和管理机构”及《个人信息保护法》第五十二条“处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人”，满足法律规定情形的企业应设立数据安全负责人和个人信息保护负责人。本次调研发现，所有被调查企业已委任数据安全负责人和个人信息保护负责人。

然而具体如何设置数据安全负责人和个人信息保护负责人在法律法规中并未明确规定。通过调研发现，被调查企业更多地选择 CISO（56%）、CIO/IT 总监（22%）、DPO（16%）担任数据安全负责人。而对于个人信息保护负责人，被调查企业更多地选择由 DPO（61%）、CISO（11%）、法务主管（11%）担任。

同时，没有企业选择由 CEO 担任数据安全负责人和个人信息保护负责人。可见，目前数据安全负责人和个人信息保护负责人的任命基本已成定式，在信息安全管理体系中，职责分离的过程已被识别为一种信息安全控制措施。企业可根据自身组织架构以及业务与产品设立相应岗位，落实保护和监督责任。

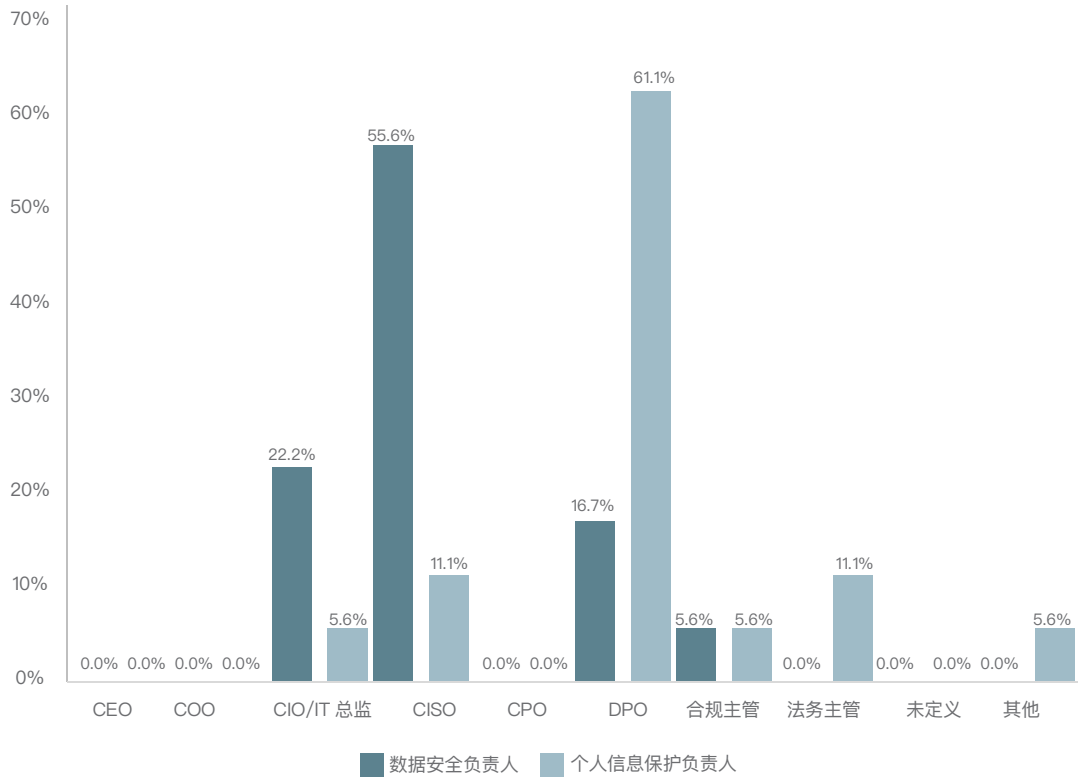



图 3.3 数据安全负责人和个人信息保护负责人的设立

**4. 企业负责数据合规与隐私保护工作的人员数量逐年提升，但仍存在人才缺口**

去年企业负责数据合规与隐私保护工作的人员数量“11–20 人”“6–10 人”“2–5 人”的占比仅为 6%、12%、46%，而今年企业对应的负责数据合规与隐私保护工作的人员数量占比为 6%、22%、56%，说明企业需要更多的数据合规与隐私保护人员以满足监管和消费者对数据合规与隐私保护日趋强烈的需求。

仅约 6% 的企业没有全职人员负责数据合规与隐私保护工作，虽然这个数字比去年的 13% 有显著的下降，这表明尽管企业对数据合规与隐私保护的需求日益增加，尤其是当前要面对日益严格的数据安全和隐私保护法规，但仍有部分企业无法满足这些需求。这些企业可能面临专业人员的缺乏，尤其是对于中小型企业来说，数据合规与隐私保护的专业人员存在较大的缺口，这成为部分企业无法满足实际的数据合规和隐私保护工作需求的原因之一。

此外，尽管有报告显示信息安全部门和法务部门是数据合规与隐私保护工作的主要责任部门，但当前数据合规与隐私保护的专业人员仍然存在较大的市场缺口。这导致部分企业无法有效实施数据合规与隐私保护措施，尤其是在面对复杂的合规要求和隐私保护挑战时。

因此，对于那些没有全职人员负责数据合规与隐私保护工作的企业来说，解决人才短缺问题、加强内部培训和提高员工的数据安全和隐私保护意识成为当务之急。同时，企业也需要积极探索外部人才引进策略，以填补这一关键领域的专业人员缺口，确保企业能够有效地遵守相关法律法规，保护个人和组织的数据隐私和安全。

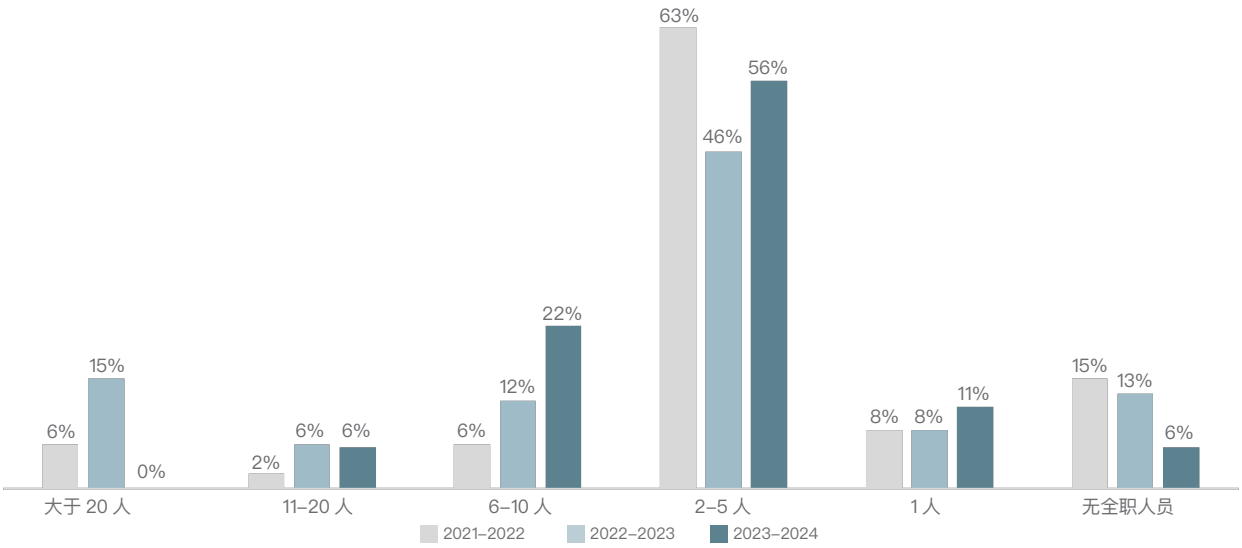



图 3.4 企业数据合规与隐私保护工作的人员数量

**5. 数据合规与隐私保护的投入日趋满足实际需求**

数据合规与隐私保护的投入一直是数据合规与隐私保护工作者关注的重点，通过对比，了解自身数据合规与隐私保护的投入是否与同等规模企业一致。调查发现，56% 的被调查企业过去 12 个月在数据合规与隐私保护的投入大于 200 万元人民币。39% 的被调查企业过去 12 个月在数据合规与隐私保护的投入大于 200 万元小于 500 万元人民币。17% 的被调查企业过去 12 个月在数据合规与隐私保护的投入大于 2000 万元人民币。

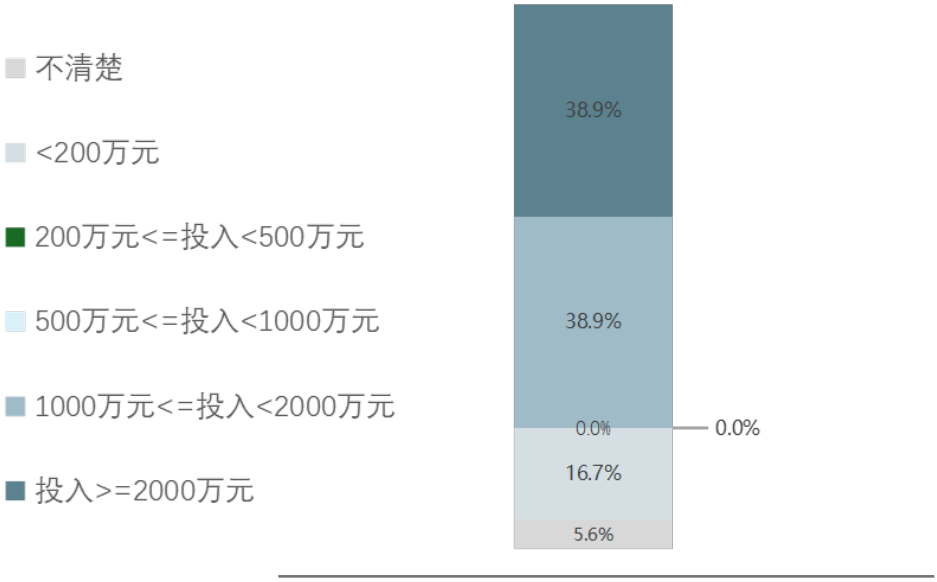



图 3.5 过去 12 个月企业数据合规与隐私保护的投入分布图（单位：人民币）

数据合规与隐私保护的投入日趋满足实际需求。89% 的被调查企业认为公司在过去 12 个月内数据合规与隐私保护方面的投入基本满足需求或超出需求。可见随着国内数据安全和隐私保护压力增大，企业在数据安全和隐私保护方面的投入逐步增加，更加积极主动地应对合规风险。

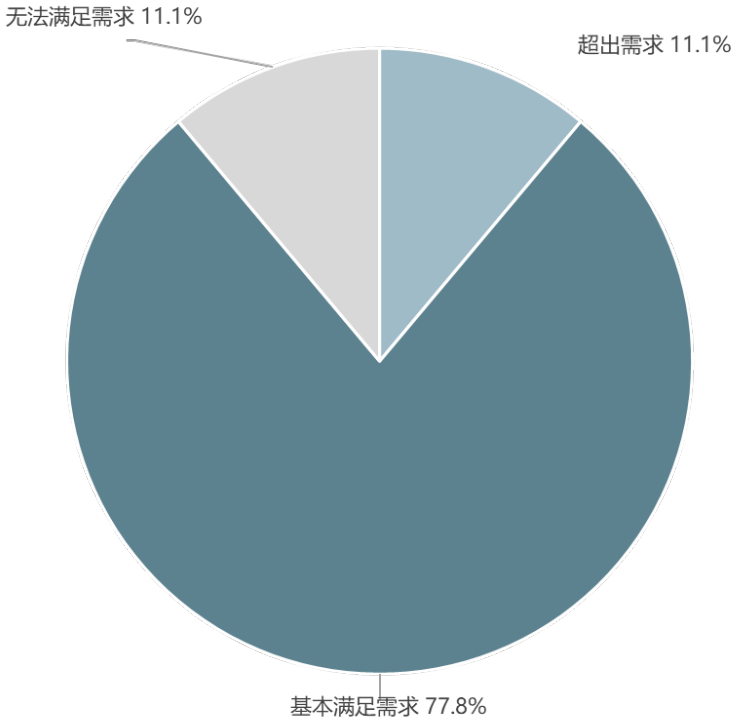



图 3.6 过去 12 个月企业数据合规与隐私保护的投入满足需求程度

**6. 数据合规与隐私保护成熟度逐步提升**

制度与流程是数据合规与隐私保护体系的重要组成部分，也是基础性工作。大部分企业在启动数据合规与隐私保护工作时，会从制度与流程建设着手，对内部管理进行标准化、规范化，设立运营流程以保证数据处理活动符合相关法律法规要求。

在制度建设方面，已有 94% 的被调查企业定义了相关方针政策以及管理制度与操作规程，并且有 11% 的被调查企业认为公司已制定了完善的管理制度和操作规程。

在制度执行情况和效果方面，大部分被调查企业对制度要求进行了落实执行，相比去年有所提升。今年，33% 的被调查企业认为执行效果有待提升。这些转变表明随着企业数据合规与隐私保护工作的深化，企业对于制度和流程落地的需求越来越强烈，企业数据合规与隐私保护成熟度不断提升。

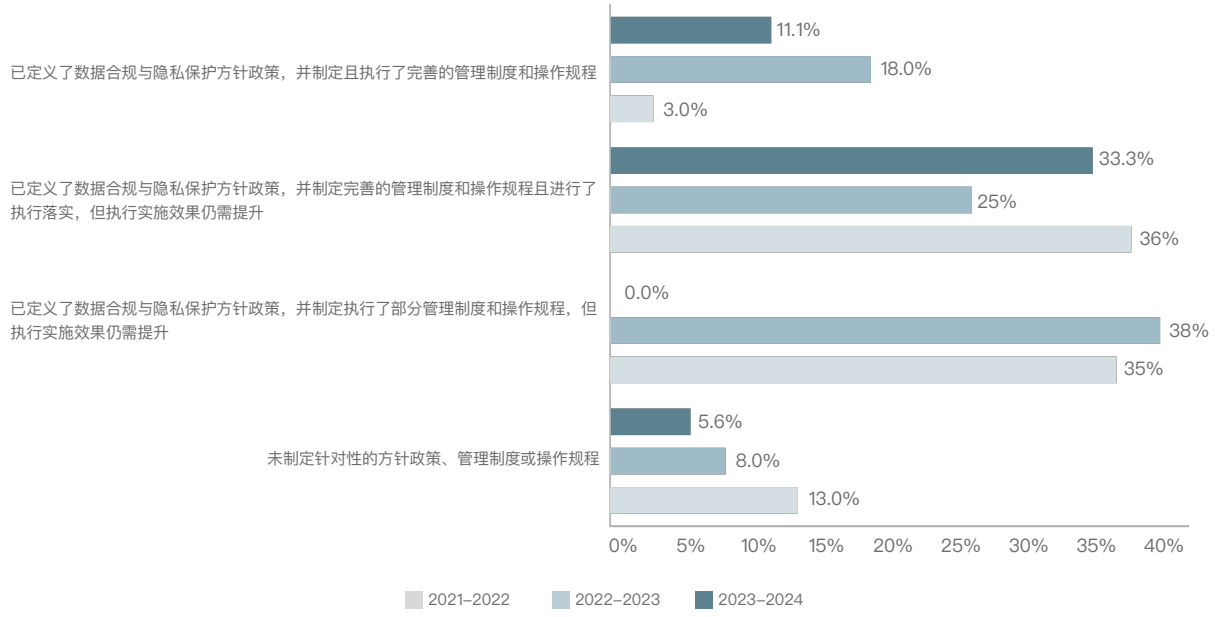



图 3.7　企业数据合规与隐私保护工作的人员数量

**7. 企业积极开展数据出境安全评估工作**

2022 年 9 月 1 日《数据安全评估管理办法》正式施行，以支持企业履行《数据安全法》第三十一条重要数据出境和《个人信息保护法》第三十八条个人信息出境相关义务。《数据安全评估管理办法》明确指出，办法施行前已经开展的数据出境活动，不符合办法规定的，应当本办法施行之日起 6 个月内完成整改。对此，适用该办法的企业，大部分（78%）被调查企业进行了积极响应，其中 28% 的被调查企业处于数据出境安全评估工作前期，即正在开展数据出境自评估，44% 的被调查企业已完成自评估。

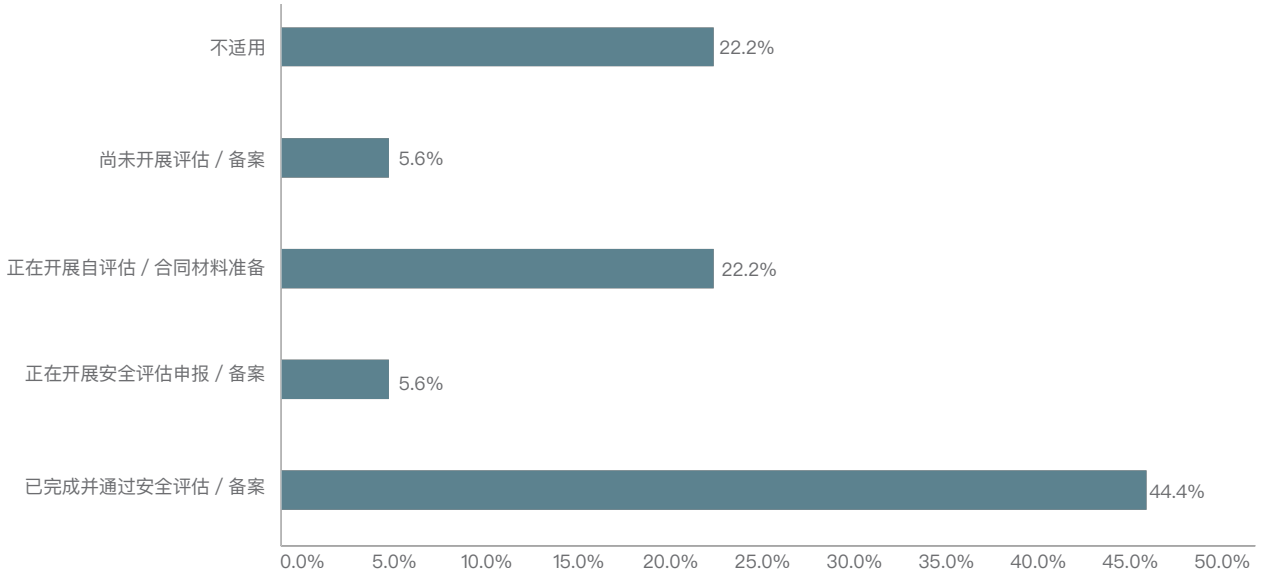



图 3.8 企业数据合规与隐私保护工作的人员数量

由于国内数据出境安全评估工作刚开始启动，企业在评估过程中存在许多挑战。在已经启动数据出境安全评估工作的被调查企业，44% 的被调查企业认为监管要求复杂且有待进一步明确。另外，39% 的被调查企业认为公司数据出境场景复杂，17% 的被调查企业认为公司缺乏隐私技术开展数据出境安全评估，6% 的被调查企业认为公司人员缺乏数据出境评估技能和知识，难以支持评估工作的开展；

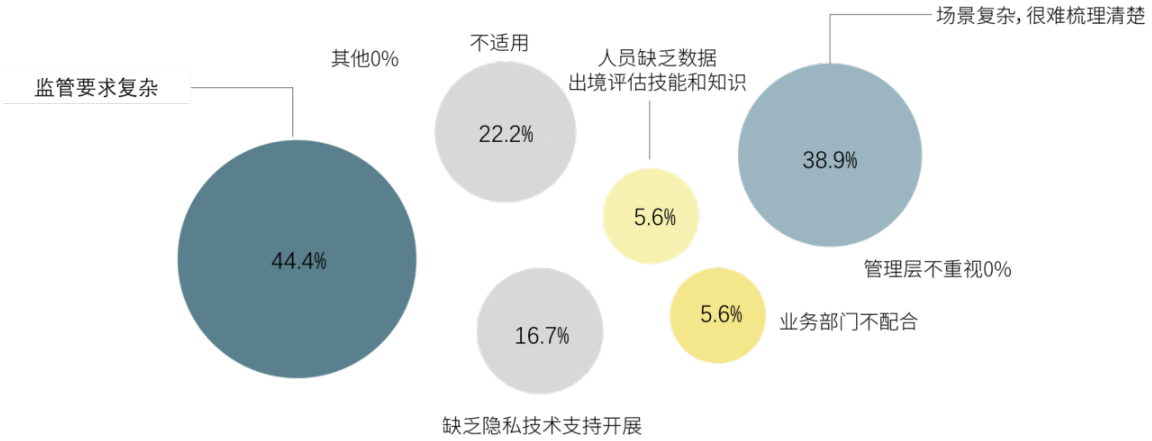



图 3.9 企业开展数据出境安全评估工作面临的挑战

针对这些挑战，短期可以借助内外部资源，对公司现有数据出境场景和风险进行梳理和评估。长期来说，可以从流程、技术和人员三方面入手，逐步完善企业在数据出境安全管理能力。流程方面，建立数据出境安全评估机制，在开展业务时若涉及数据出境应进行内部申请和自评估，必要时还需进行外部申报。技术方面，一是借助“数据自动化发现、分级分类与标识”和“数据流动监控”隐私科技解决方案掌握公司个人信息和重要数据的分布、流动、出境等情况，这与目前企业对数据合规与隐私技术解决方案迫切需求一致；二是通过“数据合规与隐私风险评估平台”将数据出境安排评估流程线上化，并将其嵌入业务活动设计阶段，形成关键控制卡点。人员方面，通过开展数据合规与隐私保护职能人员的技能培训和全员意识培训，增强人员数据出境安全。

**8. 企业间数据交易价值仍有待挖掘**

据统计，约 33% 的被调查企业进行过数据交易 / 共享。尽管参与数据交易的企业占比较低，但在已经进行过数据交易 / 共享的企业中，有 66.7%% 的企业通过数据交易 / 共享达到或部分达到了业务目标

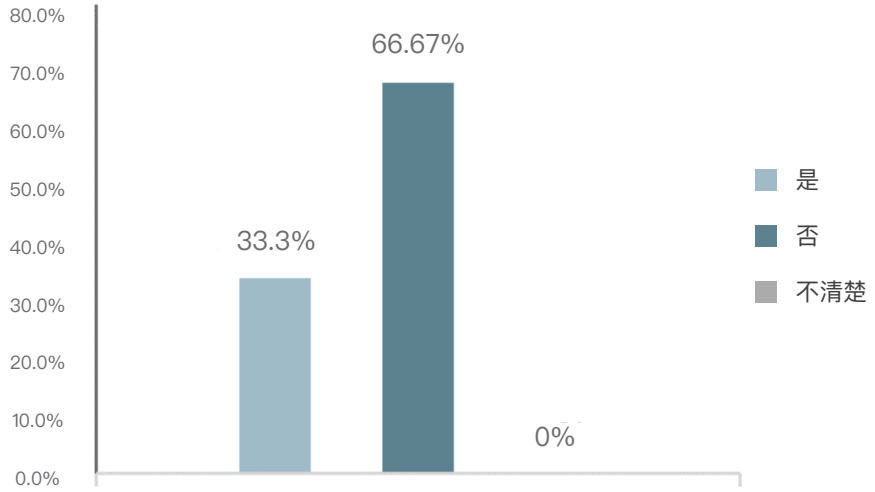



图 3.10 企业进行数据交易的情况

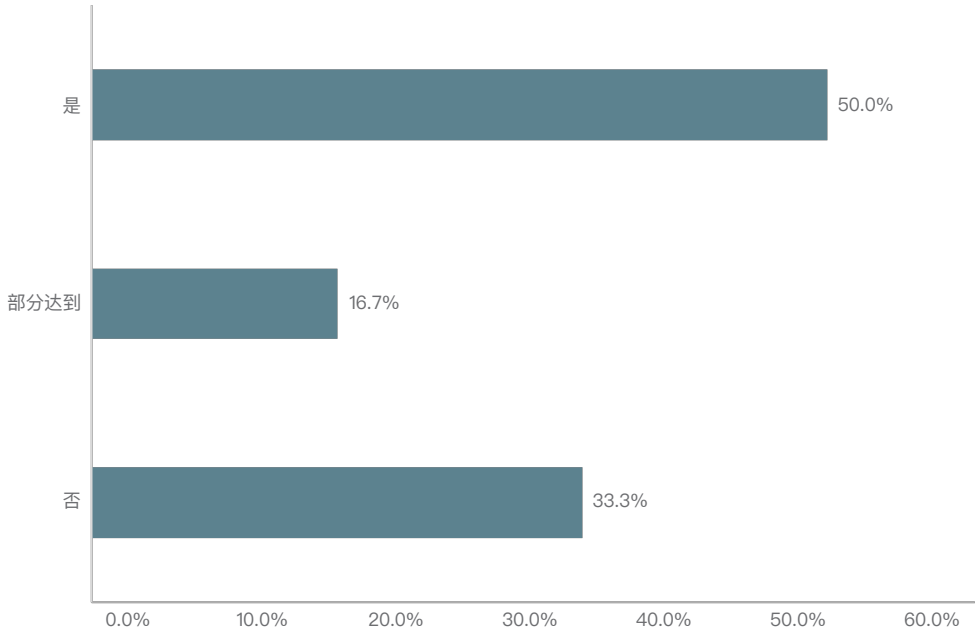
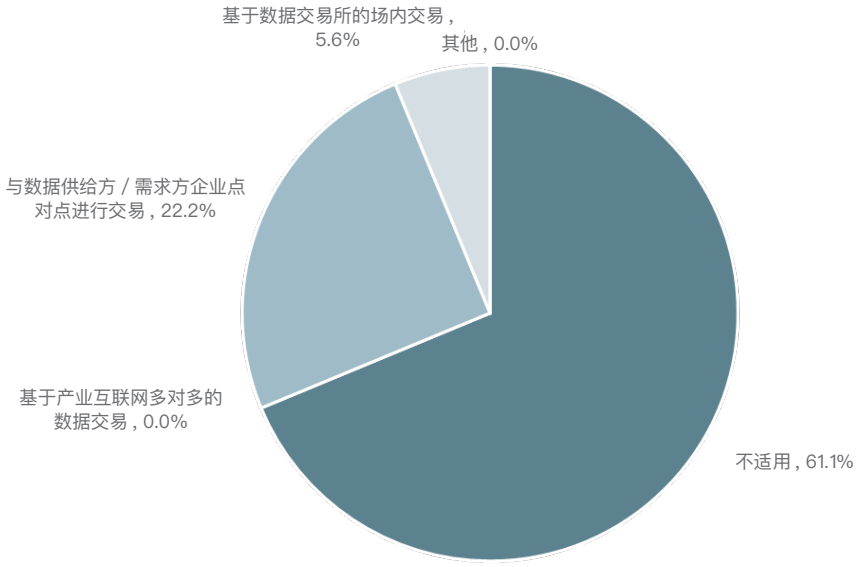
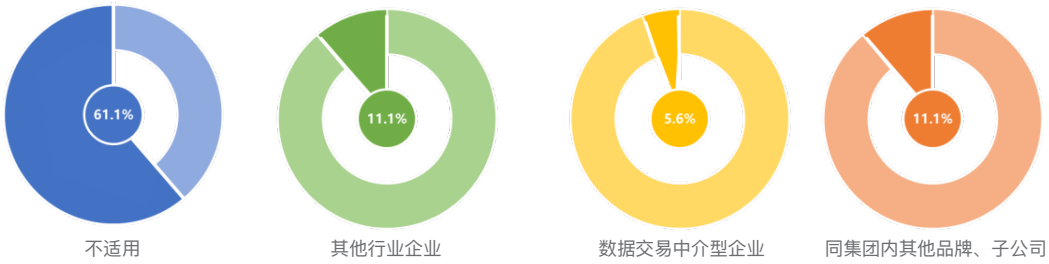



图 3.11 进行过数据交易的企业达成业务目的的情况

在进行过数据交易 / 共享的企业中，约 22% 的企业采用的是与数据供给方 / 需求方企业点对点的方式进行数据交易，约 6% 的企业是基于产业互联网多对多的方式进行数据交易。数据交易 / 共享的对象多为其他行业企业或同集团内其他品牌、子公司。

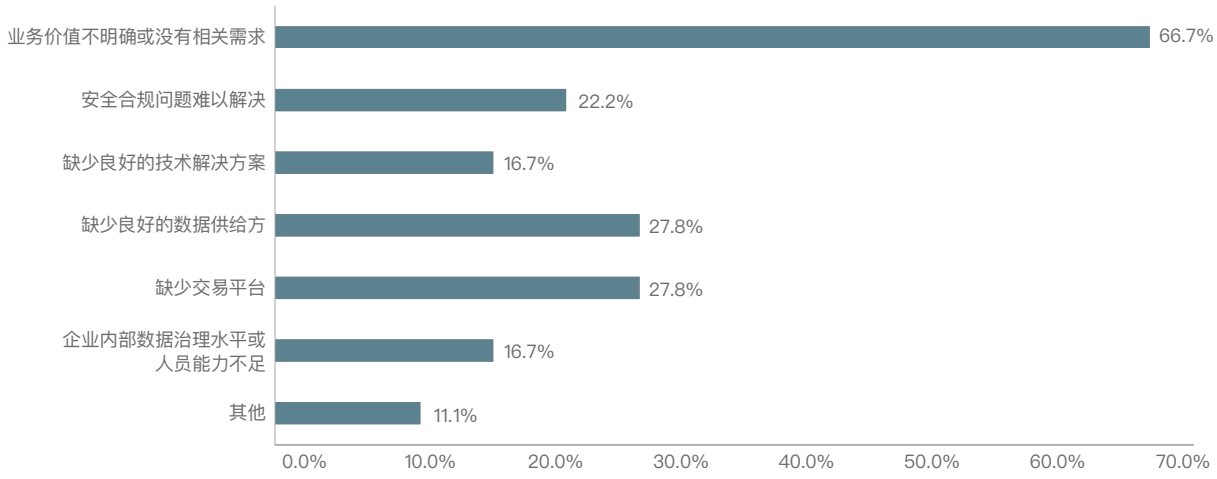



3.12 企业开展数据交易 / 共享的方式




3.13 企业开展数据交易 / 共享的对象

对于未进行过数据交易 / 共享的企业，调查了其认为目前阻碍公司开展数据交易的最大阻碍，67% 的被调查企业认为由于数据交易 / 共享业务价值不明确或没有相关需求。




3.14 目前影响企业开展数据交易的阻碍

## 3.2 企业数据合规与数据流通概况

随着《数据安全法》和《个人信息保护法》的施行，我国在数据安全和个人信息保护方面的监管不断增强。今年，除了数据出境需根据《数据出境安全评估办法》的要求向网信办申报，汽车数据安全管理也需根据《汽车数据安全管理若干规定（试行）》的要求向网信办报送。另外，银保监会下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，要求银行保险机构在个人信息保护方面进行自查自纠，并报送书面自查整改工作报告；各地通管局也发布《电信和互联网行业网络和数据安全检查的通知》要求企业自查自纠并上报总结报告。相信未来，数据合规与隐私保护企业自查整改上报、监管重点抽查的趋势将越来越明显，企业需不断提升自身数据合规与隐私保护水平。

个人信息保护和数据安全法律法规和监管日渐成熟的同时，企业的数字化进程也未曾放缓脚步。在日益增加的数据量和愈发复杂的业务场景下，技术手段成为企业隐私保护与数据安全治理的必要手段。因此，越来越多的企业开始了隐私科技解决方案的实施，将先前的规划付诸实践。在去年的调研中我们发现，有 65% 参与调研的企业正在实施部分隐私科技解决方案，而到了今年，这个比例增长到了 78% 以上，其中更是有 56% 的参与调研的企业已经实施了部分隐私科技解决方案，显著高于去年的 38%。

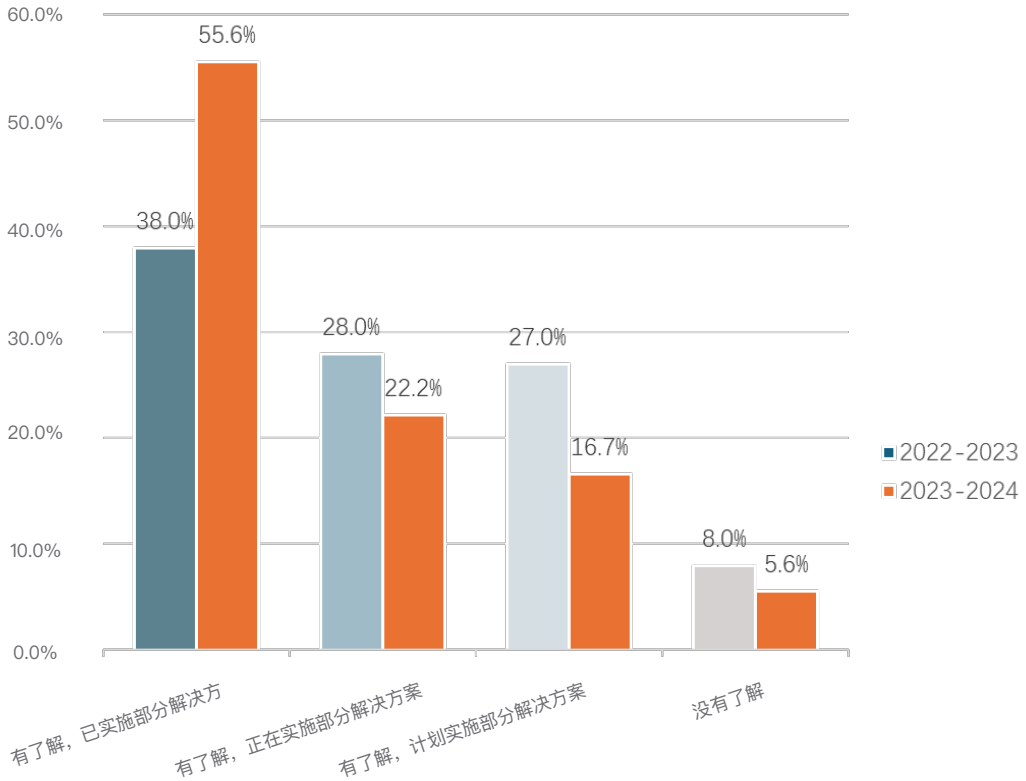



图 3.15 企业隐私科技解决方案实施程度

针对常见的隐私科技解决方案，所调研的十六类隐私科技解决方案的整体实施程度较高的排名前三的有：数据自动化发现、分级分类与标识（61%）、数据流动监控（数据资产态势感知）（50%）、个人信息主体同意授权管理（50%）。另外，隐私事件响应、数据沙箱、数据密态胶囊在今年的调研中为实施程度最低的隐私科技解决方案。综合来看，尽管各类隐私科技解决方案在企业中达到“已较完备实施”的程度仍然都不高（均未超过 18%），隐私科技在企业中的整体实施现状仍然处在起步阶段，但经过了过去一年的实施后，隐私科技解决方案在企业中的整体实施已经取得了长足的发展和进步。

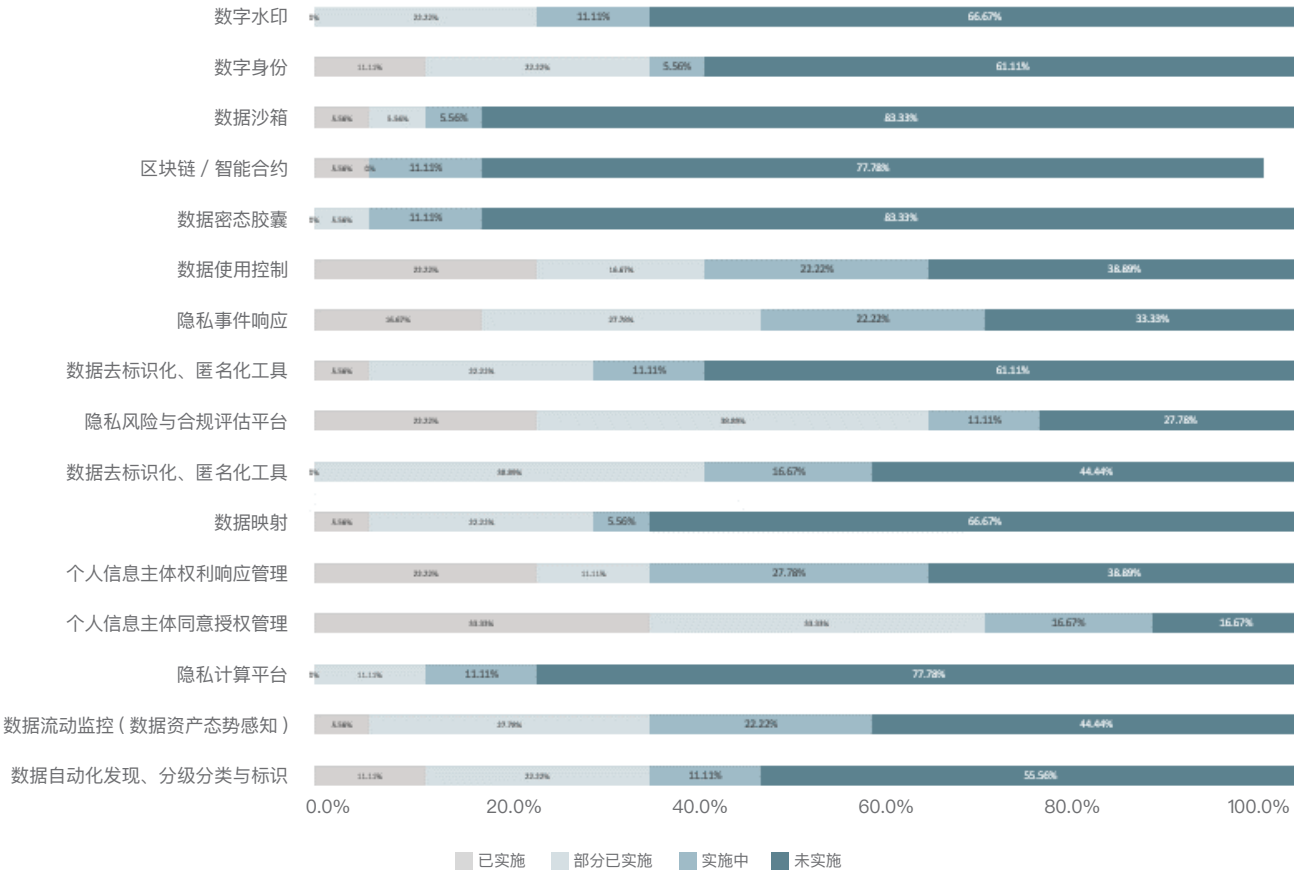



图 3.16 企业隐私科技解决方案实施现状

数据资产管理是同时飘在甲方和乙方头上的一朵乌云。在去年的调研中我们发现，数据自动化发现、分级分类与标识（62%），数据流动监控（51%）仍然是企业最迫切的需求，但数据去标识化、匿名化技术仅排在 23% 的企业最迫切的“三甲”榜单之上。而在今年，数据自动化的实施需求仍高居不下（56%），这与隐私科技解决方案实施现状的调研结果也是吻合的，在今年有 16% 的企业实施了较完备的数据去标识化、匿名化技术，而去年仅有 5%，企业通过近年来的实施，已部分满足了需求。

而相比去年，数据自动化发现、分级分类与标识和数据流动监控的实施程度、需求迫切程度均未明显改善，其中数据自动化发现、分级分类的实施程度（相关产品和解决方案的实施进展，即图表中的“已实施”“实施中”“未实施”等）甚至有显著降低。这说明企业对数据隐私与安全愈发重视的同时，隐私科技市场仍未出现较好的帮助企业识别与监控“有什么数据”和“数据在哪里”等问题。

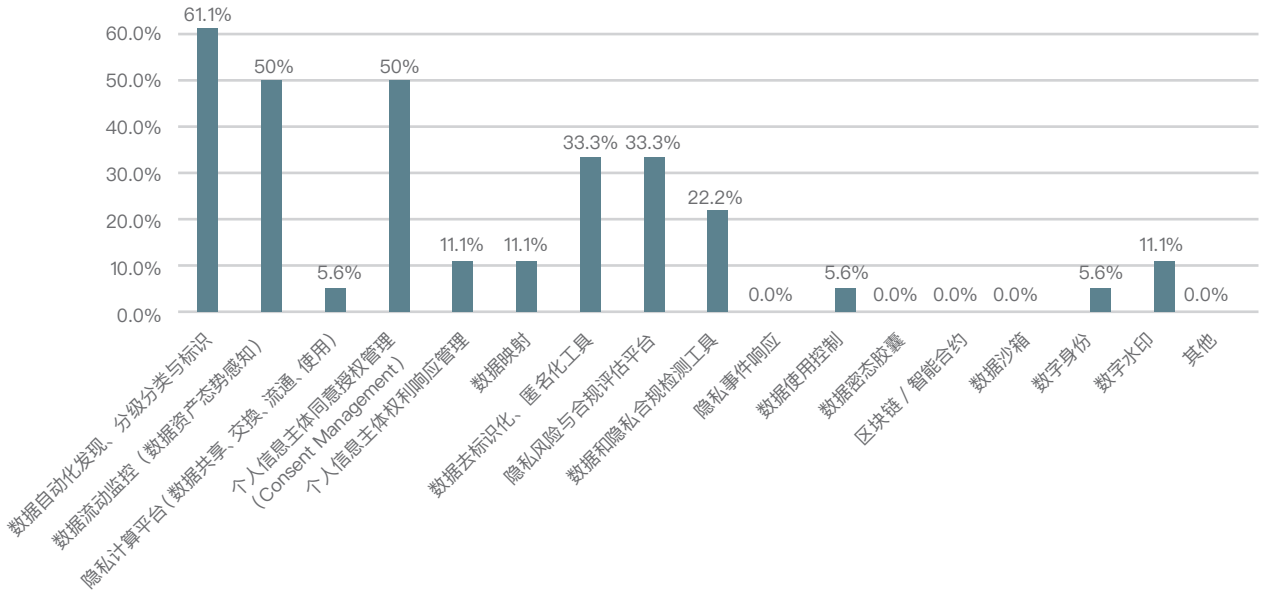



图 3.17 企业隐私科技解决方案需求现状

隐私计算各类解决方案在各行各业行业中有着较大发展潜力。其中，数据自动化发现、分级分类与标识仍是企业最迫切需要的隐私科技解决方案，有 61% 的企业表示迫切需要这类解决方案。

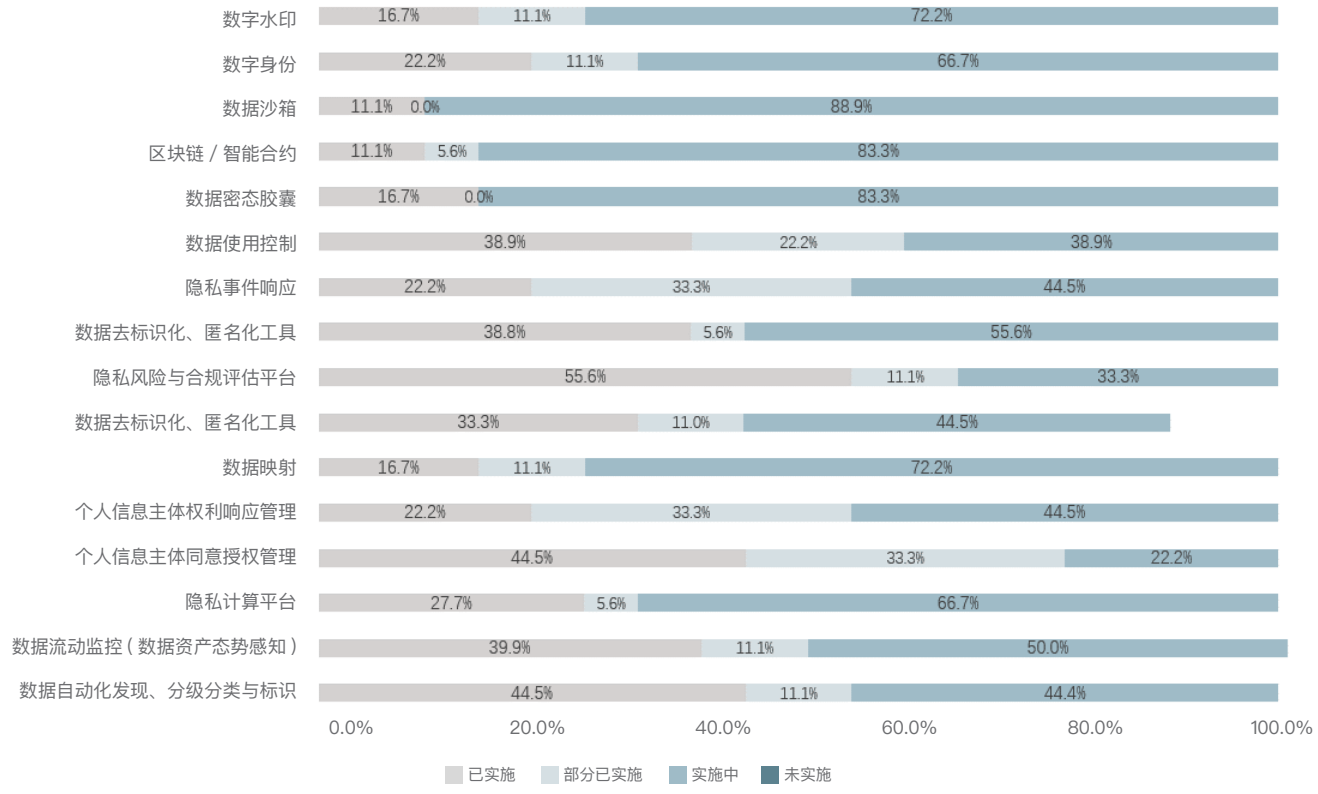



图 3.18 企业已实施的隐私科技技术自研与外采情况

据调研，28% 的数据交易应用的场景在产品优化上，数据交易在产品优化中的应用主要体现在通过数据分析与优化来提升产品的转化率和用户体验，以及通过数据洞察指导产品改进和决策。首先数据交易为产品优化提供了丰富的数据资源，这些数据包括用户行为数据、市场趋势数据等，通过对这些数据的分析，企业可以更好地理解用户需求，从而优化产品功能和用户体验。例如，在移动支付领域，随着移动支付的快速发展，企业需要通过数据分析和优化来提升移动支付的转化率，以满足用户需求和增加商业收益。通过分析用户转化率、竞争情况、用户体验以及安全性等问题，企业可以制定相应的优化策略，如提升用户体验、加强安全性措施等，从而改善产品性能，吸引更多用户使用。其次，数据交易还促进了商业智能的应用，商业智能通过对企业级数据的分析，提供销售、市场、库存等各业务领域的洞察，帮助企业更好地制定商业决策。这种数据分析不仅限于移动支付领域，还广泛应用于各个行业，如通过对供应链数据的分析，优化库存、采购、物流等方面的管理，降低成本并提高效率。

除此之外，数据交易应用的场景还有联合营销（11%）、风险控制（5.6%）、学术科研（5.6%）、产业链优化（5.6%）的等。

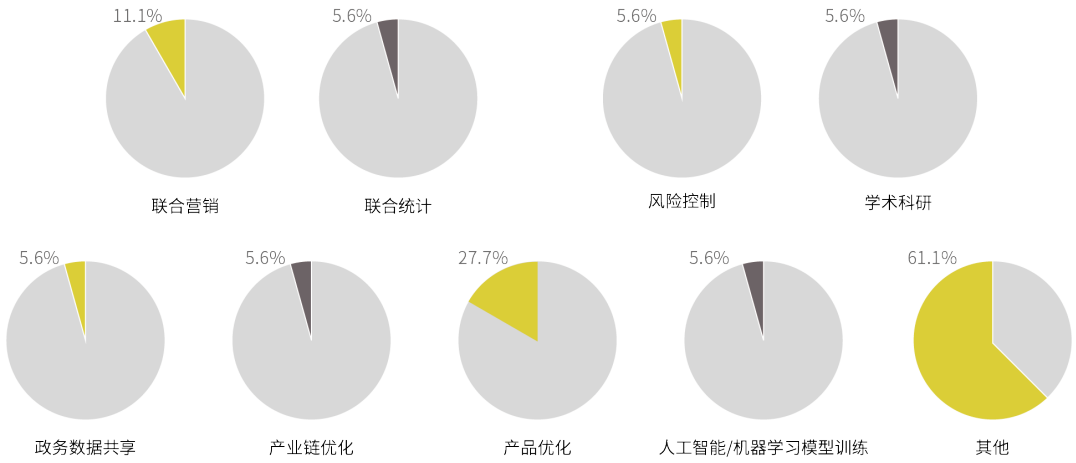



图 3.19 数据交易应用场景分布

## 3.3 企业隐私科技投资趋势

尽管受到经济环境的影响，很多企业都在缩减预算，但很多企业仍然在为数据合规与隐私保护持续投入。在去年的调研中，有 18% 的参与调研的企业认为公司投入无法满足需求，但今年这个比例降低到了 11%，更有 11% 的企业认为投入已经超出需求。

然而，对于数据合规与隐私保护的持续投入也逐步体现在对数据合规与隐私科技的投入上。

据今年的调研结果，企业在过去 12 个月在隐私科技上的投入占比仍然不高，技术投入占公司数据合规与隐私技术方面投入超过 10% 的企业由去年的 22% 上升至今年的 39%。

且在今年参与调研的企业中，表示会在未来 12 个月内增加 5% 以上的隐私科技解决方案预算的占总数的 6%，而表示会降低此方面预算的企业则仅为 27%，超过半数的企业（67%）表示对数据合规和隐私技术投入将保持平稳（预算变化 ±5% 以内）。

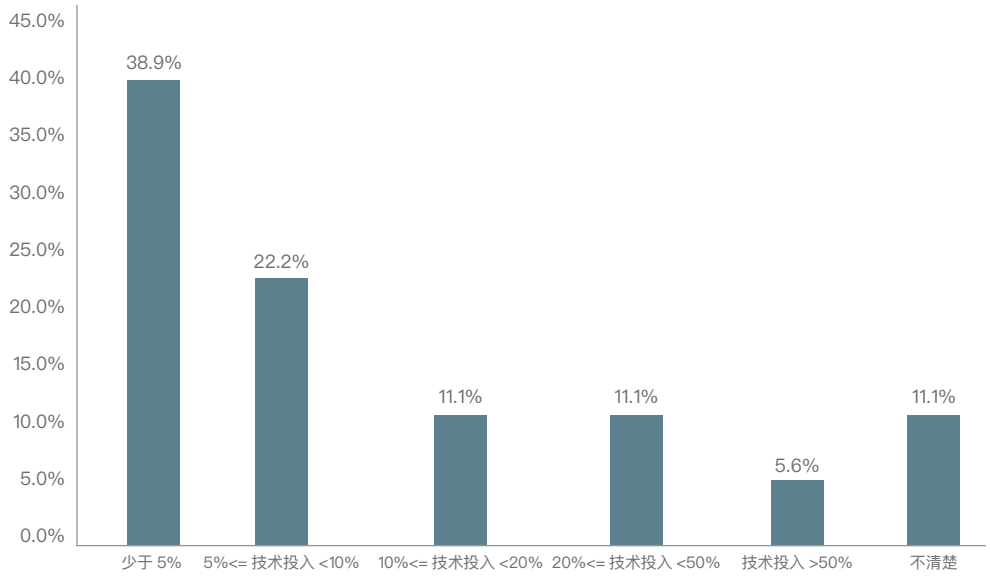



图 3.20 过去 12 个月内公司对数据合规和隐私技术投入

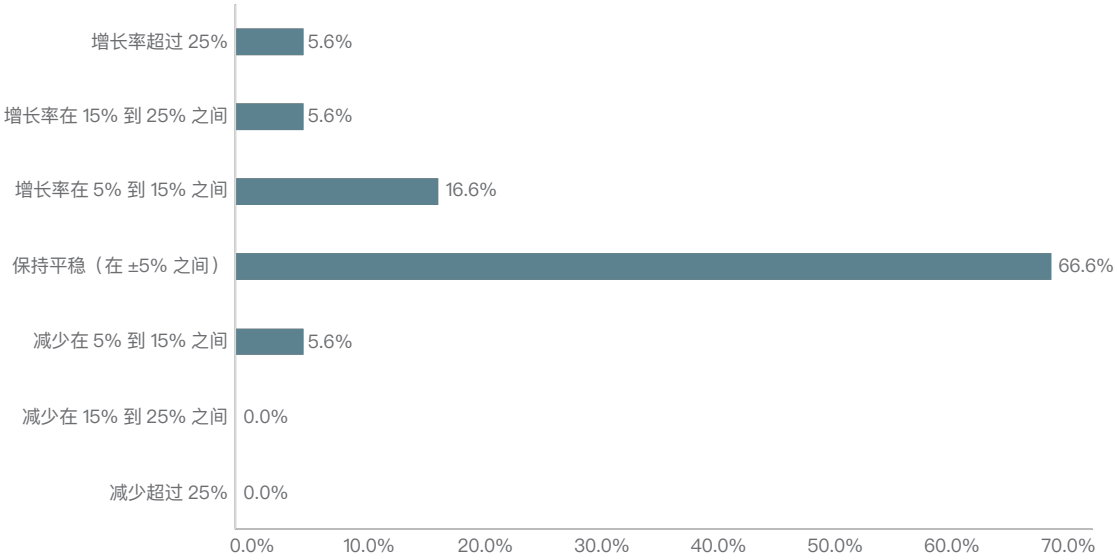



图 3.21 未来 12 个月内公司计划对数据合规和隐私技术投入的调整

## 3.4 企业对国内隐私科技市场的期望

隐私科技投入的停滞原因可能有多种，如过去两年的前期实施让部分产品、方案已进入业务稳态，维护费用低于前期实施费用；企业更多的自研使成本分摊在了信息技术或数字化部门的其他业务预算中；今年新出台的法律要求使得企业花费了更多预算用于合规评估等非技术类工作上等等。但更重要的是，随着国内合规要求日渐成熟且明确，我国数据合规与隐私保护法律提出了诸多相比欧洲、美国、新加坡等地独特的要求，我国的市场环境、业务场景和数字化程度也有着鲜明的特色，因此很多企业在期待更加贴合本地需求的国内隐私科技解决方案。然而，根据今年的调研结果，我们看到国内隐私科技市场仍有待进步。

根据调研，有 24% 的参与调研的企业在未来 36 个月内不会考虑国内的隐私科技解决方案，相比去年的 5% 有显著的增加，仅有 12% 的参与调研的

企业表示会在未来 12 个月内考虑国内的隐私科技解决方案。在全球隐私科技市场成熟度提升的当下，国内厂商面对着不小的来自国际市场的竞争压力。

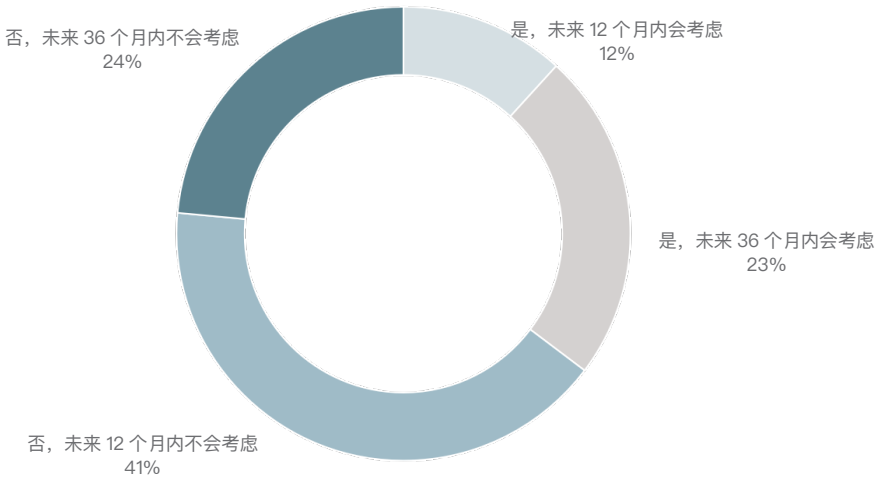



图 3.22 企业对国内隐私科技解决方案的考虑意愿

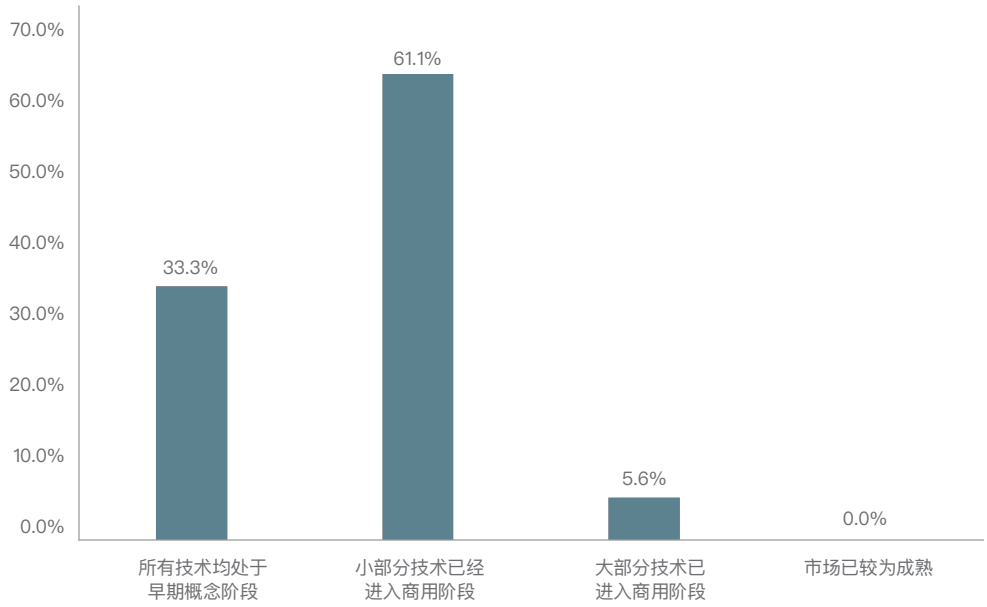



图 3.23 企业对国内隐私科技市场成熟度的评价

对比去年的数据，我们可以观察到国内隐私科技市场成熟度的提高，但提高幅度有限。大部分参与调研的企业均认为目前国内隐私科技市场仍处于早期阶段，仅有不到 6% 的参与调研的企业认为国内隐私科技市场大部分技术已进入商业化模式或认为整个市场已经成熟，90% 以上的企业认为市场仍不成熟，甚至有 61% 的企业认为小部分技术已经进入商业化模式，但仍有大部分产品处于早期阶段。更是有 33% 的企业认为目前国内隐私科技市场的技术均无法有效落地。这些数据既说明目前隐私科技市场仍处于相对早期的阶段，在企业对隐私保护的投资日趋稳定的当下，国内厂商若要提升市场竞争力，应当进一步理解企业需求、对标国际先进产品并结合本土特色，做好企业数据合规与隐私保护的守护者。

## 3.5 企业实施隐私科技所面临的挑战

在企业的数据合规与隐私保护治理中，人员、流程与技术三者均不可或缺且紧密关联。实施隐私科技除了在技术上给企业带来挑战之外，同时也对企业的人员能力与意识、制度流程规范提出了更高要求。在去年的调研中，参与调研的企业表示实施隐私科技最大的挑战是产品无法有效地与现有管理流程或 IT 环境进行整合（84%），用户体验差、导致业务部门对产品的抵制使用（41%）和缺乏相应资质或技能的人员有效支撑运营（36%）。根据今年的调研结果，企业实施隐私科技解决方案的三大挑战分别是产品无法有效地与现有管理流程或 IT 环境进行整合（62%）、缺乏相应资质或技能的人员有效支撑运营（47%）和后期运维成本高、无法及时对产品、规则和流程进行更新（39%）。而隐私科技与数据流通科技对当下的 AI 时代尤为重要，隐私科技与数据流通科技共同作用，不但可以提升数据安全、保护个人隐私，还可以促进数据的高效流通使用，赋能实体经济。这些技术的发展和应用，对于构建一个安全、高效、可持续的数据生态系统具有重要意义。在被调查的企业中，约 61% 的企业认为隐私科技与数据流通科技会对合规工作的开展产生便利，50% 的企业认为其会对数据安全风险管控产生重大影响。无论如何，在未来提高隐私科技与数据流通科技，会极大程度地提升数据安全、保护个人隐私、促进数据高效流通使用，以及赋能实体经济。

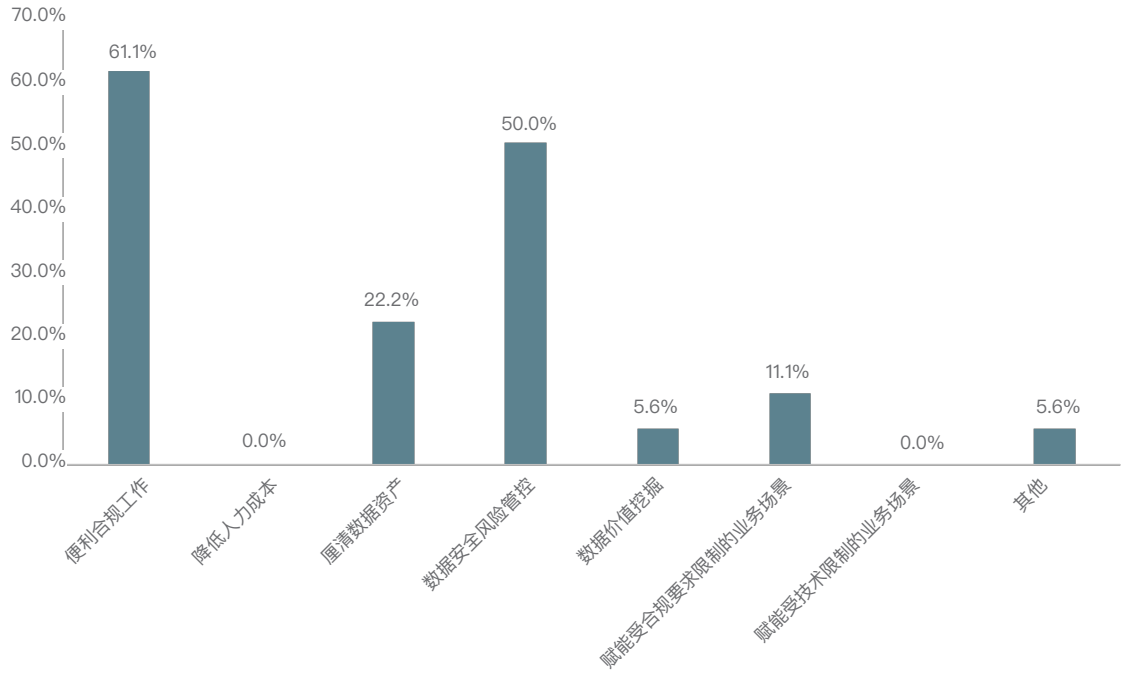



图 3.24 企业认为隐私科技与数据流通科技可以解决哪些问题

# 04

## 第四章 CHAPTER 4

# 产业发展洞察与典型实践

EY安永 Building a better working world
SICSI CYBER RESEARCH INSTITUTE 赛博研究院

# 04 第四章 CHAPTER 4 产业发展洞察与典型实践

目前，隐私科技产业正站在一个新的历史起点上，它不仅关乎技术的创新与迭代，更关乎如何在保障数据安全和隐私的前提下，促进数据的合规流通与高效利用。在这一进程中，隐私科技通过提供一系列的工具、服务和技术解决方案，支持企业在 IT 架构和业务场景中实现数据合规和隐私保护。同时，隐私科技的应用场景也在不断扩展，从金融、政务、通信到医疗、教育等多个行业，隐私科技都在助力企业实现数据的安全、合规和高效利用。随着技术的成熟和市场需求的增长，隐私科技正逐渐从理念走向规模化应用，成为推动数据要素市场化配置的重要力量。

## 4.1 隐私科技产业发展

隐私科技产业的发展是一个从理念构建到规模化应用的过程。在个人信息权益保护、数据流通、共享与开放、个人信息合理开发利用的全球性需求下，隐私科技产业即将步入快车道，以愈发成熟的隐私设计理念为基础，依托快速迭代的技术、产品及服务占据市场份额，形成广泛协作的生态圈，从而完成规模化行业应用，构建未来的数据智能网络。

数字化时代，随着全球范围内对数据保护和隐私权益日益重视，全球隐私科技产业正经历快速发展。同时，各国政府数据保护相关法规陆续实施，企业在合规性和安全性方面的压力不断增加，隐私科技的需求也随之上升。无论是在国际市场还是国内环境中，隐私科技的创新与应用正在为各行业提供新的解决方案，以应对日益复杂的隐私挑战。

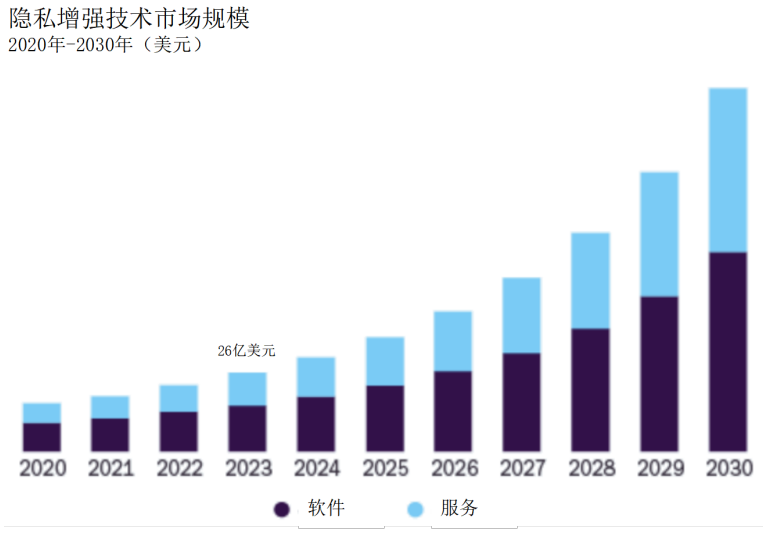



图 4.1 2020 年 –2030 年全球隐私增强技术市场规模及预测情况（Grand View Research[6]）

在全球范围内，隐私科技产业的发展受到了数据保护需求增加和合规性要求加强的推动。在这个过程中，隐私增强技术（Privacy Enhancing Technologies，简称 PET）作为隐私科技的一个重要组成部分，扮演着至关重要的角色。PET 包括了一系列的技术手段，如数据加密、匿名化处理、去标识化、安全多方计算等，它们旨在在数据的收集、处理、存储和传输过程中保护个人隐私，防止数据泄露和滥用。因此，结合 PET 这一细分市场的动态，可以进一步观察和预测整个隐私科技产业发展趋势，展望隐私科技板块的未来方向和利用潜力。

根据 Grand View Research 的报告，全球隐私增强技术市场在 2023 年的估值为 26 亿美元，并预计从 2024 年到 2030 年将以 25.3% 的复合年增长率增长。这一增长可以归因于对 GDPR 和 CCPA 等严格法规的遵守推动了企业采用隐私增强技术解决方案，以确保在保护隐私的同时安全地使用数据。此外，数字化转型的兴起，以及对网络安全威胁和数据泄露的日益关注，也增强了对先进隐私保护技术的需求，如同态加密和差分隐私，以在不损害功能的情况下保护敏感信息。

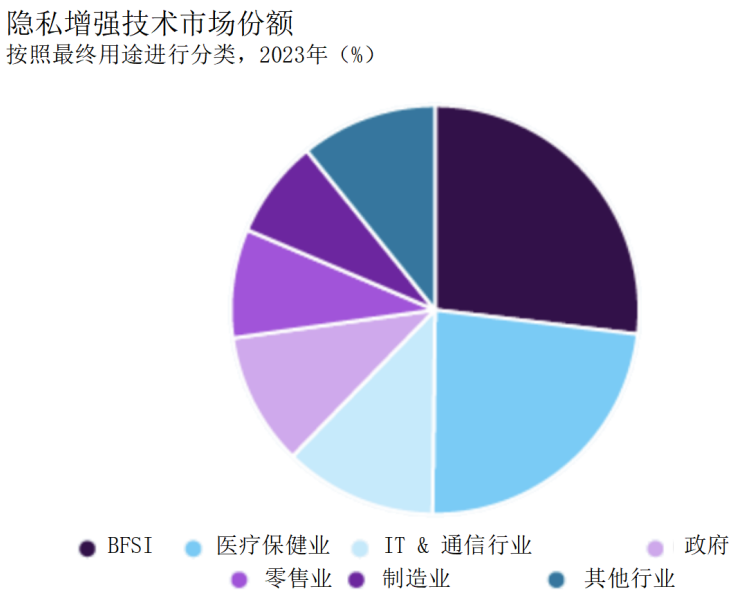



图 4.2 2023 年全球隐私增强技术不同行业市场份额（Grand View Research[6]）

对比不同行业的市场份额可以发现，银行、金融服务和保险（BFSI）行业的细分市场在 2023 年占据了最大的市场份额（27%）。金融机构处理大量敏感的个人和财务数据，使其成为网络攻击和数据泄露的主要目标。因此，人们更加重视保护这些信息，以维护客户信任并满足严格的管理法规要求。隐私增强技术（例如数据匿名化、加密和安全多方计算）正在成为这些组织保护敏感数据同时仍支持有价值的数据分析和业务运营的重要工具。

同时，由于智能制造和工业 4.0 计划的兴起，物联网、人工智能和大数据分析等先进技术正在逐步集成到生产流程中，这些技术生成和处理大量数据，这引发了对数据隐私和安全的担忧。而隐私增强技术可以通过提供保护数据的机制来解决这些问题，同时支持将其用于洞察和决策。因此，预计制造业中的隐私增强技术市场份额将在预测期内以最快的复合年增长率增长。

在中国，随着《个人信息保护法》等相关法律

法规的实施，隐私科技产业也迎来了新的发展机遇。国内对于隐私计算技术的需求不断增长，特别是在金融、政务、医疗等数据敏感性较高的行业。隐私计算技术如多方安全计算、联邦学习、同态加密等，已经在多个行业中得到应用，以支持数据的安全共享和分析，同时保护个人隐私。此外，中国政府在数据安全与算法应用方面的立法进程加快，推动了公共数据授权运营平台的建设，促进了数据要素的流通与循环，有效释放数据要素价值，增强数字经济发展效益。隐私计算作为其中的关键技术模块，将全方位助力公共数据授权运营安全有序开展，促进公共数据与社会数据融合。

## 4.2 典型案例 1：金融行业<br>数据要素 × 金融服务提高金融抗风险能力

随着金融科技的快速发展，金融机构在享受数字化转型带来的便利的同时，也面临着日益严峻的数据保护挑战。如何在保障客户隐私和数据安全的前提下，实现数据的高效利用，已成为金融行业亟需解决的问题。隐私科技，作为解决这一问题的关键技术，通过隐私计算、数据加密、安全多方计算等技术手段，为金融行业提供了数据保护与利用的新思路。

**（1）金融行业数据保护痛点**

金融行业拥有海量的用户数据，包括交易记录、账户信息、信用评分等敏感数据。这些数据不仅对金融机构至关重要，也极易成为黑客攻击的目标。同时，金融行业还存在一些特殊的业务场景。例如，金融行业越来越多地采用生物识别技术（如指纹、面部识别、声纹等）进行支付或身份认证，这些生物特征数据具有唯一性和不可更改性，一旦泄露或被滥用，将对用户隐私造成严重威胁；在对账过程中也会涉及大量敏感的财务信息，需要严格控制数据访问权限，并确保对账数据的访问范围最小化，同时对敏感信息进行脱敏或加密处理，以防止数据在对账过程中被泄露。

此外，风控系统在金融交易中用于识别和预防欺诈行为，但同时也涉及大量用户数据的处理。这些数据需要严格的权限管控和行为审计，确保风控数据的安全性和合规性。在使用用户数据进行风控模型训练时，也必须对数据进行去标识化处理，以保护用户隐私，防止个人敏感信息被泄露。尤其是金融机构在与其他机构进行联合风控时，需要明确各方在数据处理和保护方面的责任，确保数据在整个风控过程中的安全。

**（2）金融行业隐私科技核心应用：数据要素与金融服务的深度融合**

金融行业的服务不仅依赖于传统的金融数据，还需要融合来自环保、工商、税务、气象、消费、医疗、社保、农业农村、水电气等多个领域的数据。这种跨行业的数据整合，能够为金融机构提供更全面的用户画像和风险评估，从而优化信贷业务管理和保险产品设计。

通过隐私科技，金融机构可以在不泄露个人信息的前提下，利用多方数据进行主体识别。这种技术手段使得金融机构能够更准确地识别客户的信用状况和风险特征，从而提高信贷审批的效率和准确性。同时，隐私科技支持金融机构间共享风控类数据，融合分析金融市场、信贷资产和风险核查等多维数据。这种数据的集成和分析能力，能够有效提升金融机构的反欺诈和反洗钱能力，增强金融抗风险能力。此外，隐私科技还鼓励电子商务企业、现代流通企业和数字贸易龙头企业在安全合规的前提下，

融合交易、物流和支付数据。这种跨境数据的流通能力，能够支撑提升供应链综合服务、跨境身份认证和全球供应链融资等能力，为国际贸易提供更为安全和高效的金融服务。

**（3）金融行业隐私科技解决方案：基于联邦学习的隐私计算平台**

某大型银行采用联邦学习技术，克服了数据共享的障碍，整合了多种来源的数据，如金融保险信息、位置信息和社交网络数据，共同构建模型。这一举措旨在构建一个既保护数据隐私又激励数据共享的生态系统，服务于信贷风险评估、跨机构的反洗钱和欺诈检测，以及金融产品的个性化推荐。同时，该银行还解决了内部子公司间的数据安全共享问题，促进了银行业务的数字化转型和智能化升级。

该银行的隐私计算平台具备分布式计算能力，其隐私计算引擎通过多方安全计算和联邦学习技术，支持隐私查询、数据的协同计算和可视化建模。此外，平台还提供了全面的服务，包括系统管理、用户管理、数据管理、项目管理、任务调度和日志记录等功能，构建了一个完整的系统架构。该平台可以确保数据在不被泄露的前提下进行协同处理，实现数据的保密性和可用性。平台提供了包括联邦学习和多方安全计算等多种隐私保护功能，满足了银行内部数据挖掘、用户身份验证和监控等需求。它还确保了银行集团内部机构和子公司之间的数据安全流通，并且能够与外部合作伙伴进行数据的联合应用。

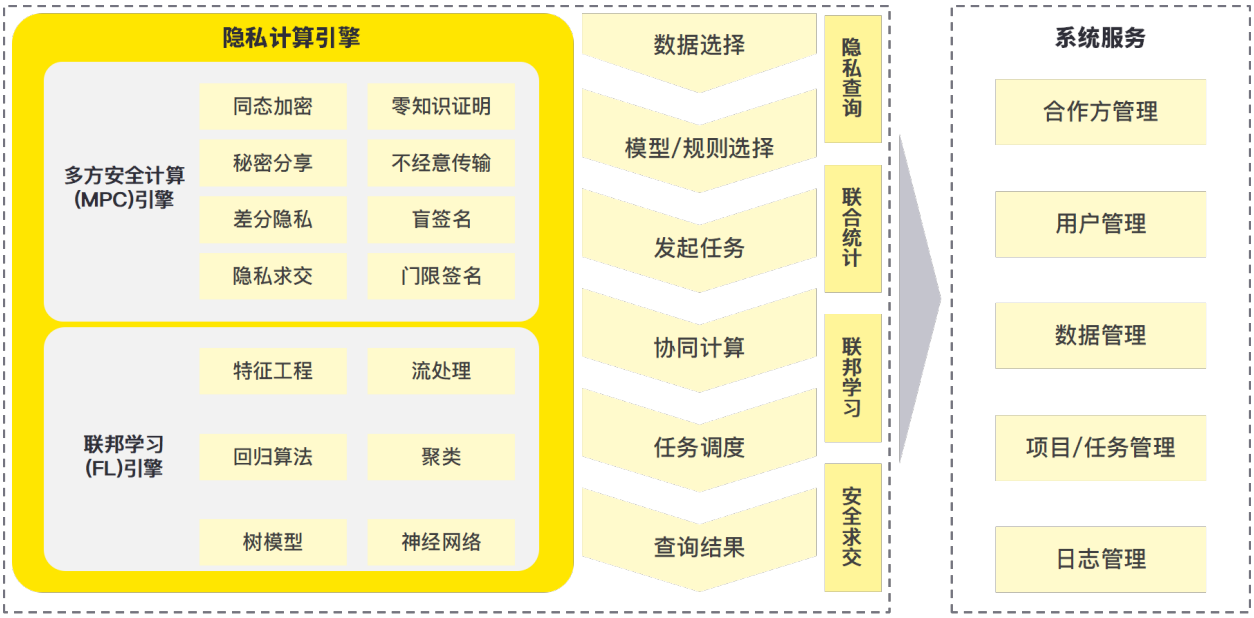



图 4.3 隐私计算平台系统架构

同时，为了在不直接共享敏感数据的前提下，实现数据价值的最大化，金融机构也开始探索与其他行业进行跨领域的联邦合作。以金融机构 + 运营商的合作为例，基于银行联邦学习平台，利用隐私计算技术，在安全隐私及合规的前提下，可以为银行引入通信运营商数据，共同开展在手机银行登录场景反欺诈模型的联邦学习建模和应用，为银行对风险账户提前管控提供模型依据，进一步减少银行客户的资产损失。

该银行的联邦学习系统保证了数据源和银行的数据安全存储在本地数据库中，计算过程仅在本地节点上执行，同时，所有计算过程中的加密信息仅在经过验证的节点间传递，实现了“数据可用不可见”“数据不动、模型动”。此外，平台还通过数据使用授权和精确的用量控制，确保了数据不会被未授权的第三方再次利用。

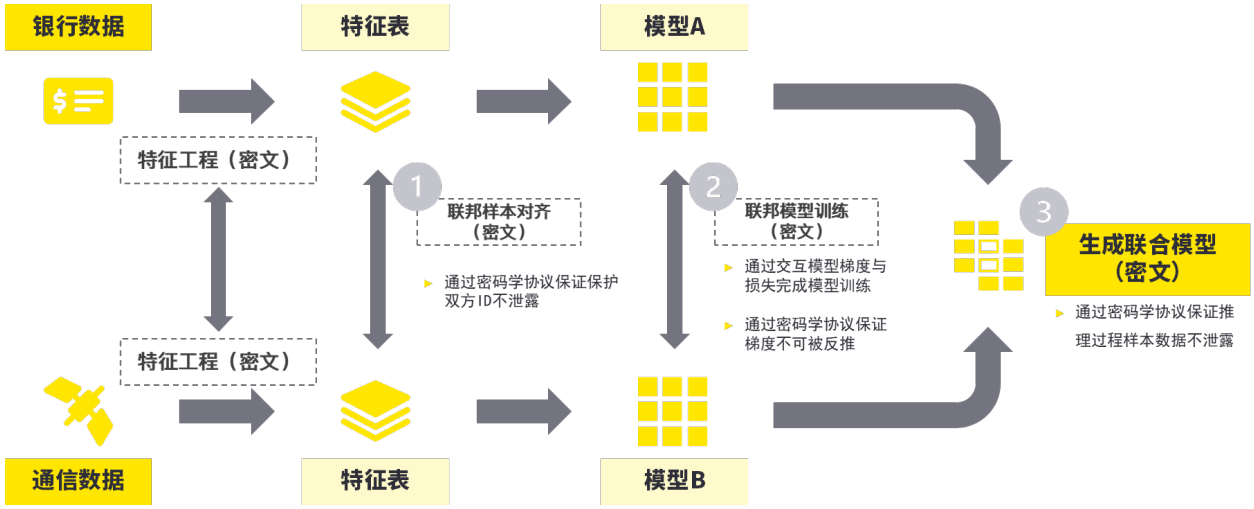



图 4.4 银行 – 通信联邦学习技术方案

## 4.3 典型案例 2：医疗行业数据协作网络促进安全高效的数据共享平台

在医疗行业中，数据的保护和利用一直是一对难以平衡的矛盾。随着医疗信息化的深入，个人健康数据的电子化存储带来了前所未有的便利，同时也带来了隐私泄露的风险。如何在确保患者隐私安全的基础上，充分利用这些数据进行临床研究和疾病预防，是医疗行业面临的重大挑战。

**（1）医疗行业数据保护痛点**

医疗数据包含了患者的敏感信息，如个人身份、病史、诊断结果、治疗方案等。这些数据的泄露不仅侵犯个人隐私，还可能导致严重的后果。对于医疗机构需要建立有效的数据安全事件应对机制，包括安全事件的监测、预警、应急响应和事后处理。这要求医疗机构具备相应的技术和管理能力。

此外，医疗机构之间的数据共享存在障碍，容易导致数据孤岛现象。这不仅影响了医疗资源的有效利用，也限制了医疗大数据在临床研究、疾病预防和健康服务等方面的应用。传统的数据共享模式存在诸多风险，包括数据在传输和存储过程中的安全性问题，以及数据使用过程中的合规性问题。因此，在推动数据共享和开放的同时，如何确保数据在流转过程中的安全，防止数据被滥用或泄露，也是医疗机构需要面对的问题。

**（2）医疗行业隐私科技核心应用：数据安全共享与跨境合作**

通过构建一个基于隐私计算技术的科研协作网络，可以实现数据的安全共享和高效利用。科研协作网络的核心是一个分布式的数据平台，它允许联盟内的医疗机构在保护患者隐私的前提下，进行数据的联合分析和研究，并采用严格的数据治理流程，对所有数据进行去标识化处理，确保个人隐私不被泄露。同时，还应建立完善的数据治理体系，包括数据清洗、归一化处理和质量控制，以保证数据的准确性和可用性。此外，还可以利用隐私计算技术，如多方安全计算、联邦学习和同态加密等，实现数据的安全共享。这些技术确保了在不直接共享原始数据的情况下，医疗机构能够进行联合数据分析，从而在保护患者隐私的同时，实现数据的价值挖掘。

在数据跨境方面，隐私科技的应用也展示了其

在国际合作中的价值。通过与国际医疗机构的合作，可以实现数据价值的跨境流通，而不涉及原始数据的跨境传输。这种数据价值跨境的方式，不仅符合各国的数据保护法规，也为全球医疗研究合作提供了新的可能性。

**（3）医疗行业隐私科技解决方案：智能预警与合作研究平台**

在实际应用中，该平台成功支持了一项针对传染病预警的研究项目。通过整合来自不同医疗机构的匿名化医疗数据，平台利用机器学习模型预测了特定症候群的发展趋势。当模型预测到症候群人数异常增加时，系统会自动触发预警，提示可能的传染病爆发，从而为疾病预防和控制提供了有力的数据支持。

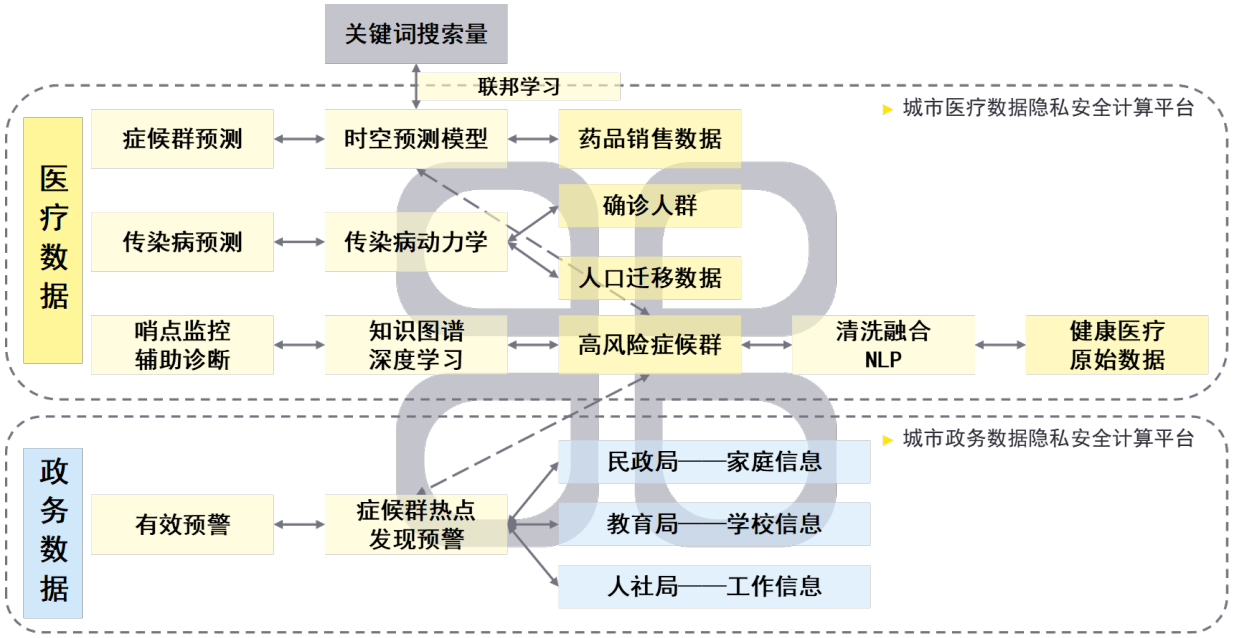



图 4.5 多点触发预警系统技术框架

该平台还支持了多中心的临床研究。研究人员可以在保护患者隐私的前提下，跨机构访问和分析大量临床数据，从而加速了医学研究的进程。这种跨机构的数据共享和协作，不仅提高了研究效率，也为医疗行业带来了新的研究思路和方法。

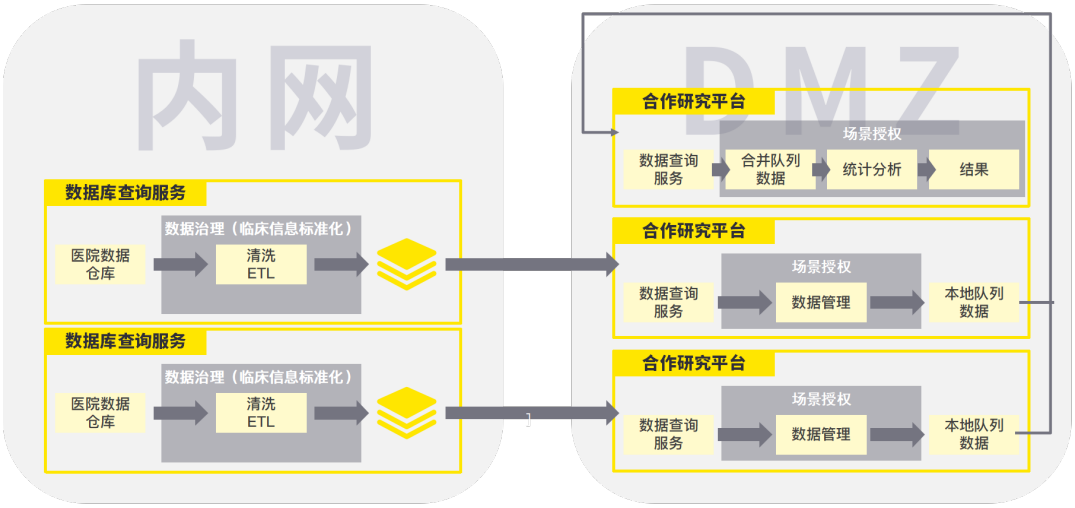



图 4.6 多中心临床研究网络框架

## 典型案例 3：政府和公共部门公共数据融合助力新市民服务应用

在数字化转型的浪潮中，政府和公共部门正面临着如何利用数据资源提供更高效、更精准的公共服务。特别是在金融服务领域，如何通过数据要素与金融服务的深度融合，提升服务的质量和效率，成为政府和公共部门亟需解决的问题。本案例聚焦于上海市如何通过公共数据的融合应用，助力新市民服务应用，提高金融服务的可得性和便利性。

**（1）政府和公共部门数据保护痛点**

政府和公共部门在跨部门、跨地域、跨层级的数据共享中存在难题。数据管理各自为政，导致数据共享纵强横弱，部门获取地方信息容易，而地方获取部门信息困难。同时，数据共享开放的法律法规亟待完善，数据平台组网难和数据应用缺乏高效整合共享也是当前面临的挑战。

公共数据的有效治理和高效运营能够最大限度地挖掘价值红利。然而，目前公共数据治理在合规性、标准化水平、授权机制等方面存在不足，亟需构建更加完善的数据治理体系。

**（2）政府和公共部门隐私科技核心应用：公共数据要素流通与保护**

公共数据要素的流通是市民服务的核心。通过整合和治理多源数据，包括人口户籍、教育、人社、企业注册登记等信息，政府可以构建一个全面的数据资源库，为新市民提供更加精准和便捷的服务。这些数据不仅用于金融服务，还涉及到社会管理、城市规划等多个方面，能够极大提高政府服务的效率和质量。此外，政府还可以通过数据服务接口的开放，支持金融机构开发创新金融产品，解决传统金融服务模式中对中小微创新企业服务不足的问题。

在公共数据要素流通过程中，可以通过加强数据治理、实施数据加密、访问控制等安全措施，以及建立统一的数据开放平台，确保数据在流通过程中的安全。同时，通过隐私计算技术的应用，如联邦学习，可以实现数据的协同计算，使得数据在不出本地库的情况下，仍能为金融机构提供服务，从而在保护数据安全的同时，发挥数据要素的价值。

**（3）政府和公共部门隐私科技解决方案：新市民服务应用**

在实践中，新市民服务应用的实施，体现了政府如何利用公共数据资源来提升市民的生活质量。政府通过提供新市民数据服务产品，使得金融机构能够更准确地识别和满足新市民的金融服务需求。这些服务产品不仅包括信贷风险评估，还涉及到个性化金融产品的设计和推广。通过这种方式，政府和金融机构共同为新市民提供了更加全面和贴心的服务，帮助他们更好地融入城市生活，同时也推动了城市经济的发展和社会的繁荣。

新市民群体通常包括外来务工人员、新就业大学生等，他们对金融服务的需求与本地市民有所不同。为了更好地服务这一群体，政府需要收集和处理大量个人数据，这就必须在确保数据安全和隐私的前提下进行。通过建立新市民服务应用，不仅提高了金融服务的可得性和便利性，还通过数据的合理利用，增强了对新市民群体的服务能力。例如，通过分析新市民的就业、居住和消费数据，政府能够更准确地评估他们的信用状况，从而提供更符合他们需求的金融产品和服务。

公共数据要素的流通在新市民服务应用中发挥了关键作用。政府通过整合各部门的数据资源，构建了一个跨部门的数据共享平台，使得数据能够在

保护个人隐私的前提下，为新市民提供更精准的服务。这一平台不仅包括了人口基本信息、教育背景、社保缴纳等数据，还涵盖了企业的注册信息、财税信息、年报信息等，为金融机构提供了全面的客户画像。通过这些数据的融合应用，金融机构能够更好地评估新市民的信用风险，提高信贷审批的效率和准确性。


图 4.7 新市民服务应用概览图

新市民服务应用的实施，不仅提升了金融服务的质量和效率，还促进了政府服务的创新。政府通过新市民服务应用，能够更有效地响应新市民的需求，提供更加个性化和便捷的服务。例如，政府可以通过分析新市民的消费习惯和信用记录，为他们提供定制化的金融产品，如个人贷款、信用卡服务等。同时，政府还能够通过数据的分析和挖掘，发现新市民群体中潜在的市场机会，促进经济发展和就业。此外，新市民服务应用还能够帮助政府更好地进行社会管理和城市规划，如通过分析新市民的居住分布和交通出行数据，优化城市基础设施建设和公共服务供给等。

# 05

## 第五章 CHAPTER 5

# 未来展望

EY安永 Building a better working world
SICSI CYBER RESEARCH INSTITUTE 赛博研究院

05

# 第五章 CHAPTER 5
# 未来展望

隐私科技的产业发展是一个从理念构建到规模化应用的过程。由于这一概念在不同国家、地区有着区域性特色，在不同行业的应用场景中也有着显著差异的技术和业务需求方向，所以隐私科技仍然是一个百家争鸣的领域，各方角色在相应的赛道中沿着不同的方向向前摸索。然而，在个人信息权益保护、数据流通与共享、个人信息合理利用的全球性需求下，隐私科技产业已获得蓬勃发展。隐私科技产业发展将以愈发成熟的隐私设计理念为基础，依托快速迭代的技术、产品及服务占据市场份额，通过开源形成广泛协作的生态圈，从而完成规模化行业应用，构建未来的数据智能网络。

《2023–2024 全球数据流通与隐私科技发展报告》根据近一年的洞察，对产业未来提出几点展望，对《2022–2023 全球数据合规与隐私科技发展报告》年的洞察结论予以补充。

## 5.1 应用：从满足合规要求到破除数据流通障碍

随着全球主要经济体数据安全与隐私保护的合规体系日益完善，法律法规日渐明确，监管行动成为常态化，企业的合规工作也日渐成熟。隐私科技在数据合规中的应用也得以发展，尽管仍存在诸多有待提高的地方，但隐私科技在合规工作中的支撑作用已不可替代。

但与此同时，随着数据要素市场的建设与发展，我们已经看到联邦学习、数字身份等技术在合规以外的领域崭露头角。可以预见，隐私科技在进一步破除数据流通障碍，挖掘数据价值，完善数据要素市场中将扮演基础设施的重要角色。

## 5.2 人才：安全合规与业务并重的“全能型”人才缺口增长

根据 Gartner 的数据，到 2025 年，50% 在中国开展业务的大型跨国公司将设置专职的数据安全负责人，具备本地法律专业知识和语言技能，以满足中国市场相关的数据保护需求。而在数据流通需求日渐增长的当下，对企业相关人员的能力要求也会更高。隐私科技等技术将不仅限于保护企业的数据，而将“破圈”成为赋能业务的利器。因此，对人员的技术能力、业务理解均将是巨大的挑战，前台业务部门与中后台安全技术部门之间的距离将进一步被拉近，业务、技术与安全合规的稀缺全能人才将会是企业的重要需求。

## 5.3 标准：技术通用性与行业性标准亟待制定

企业对于数据流通的关注聚焦于安全性、技术成熟度、业务价值和落地可实施性四个方面。诸如隐私计算等新型理念与技术将被引入数据流通领域，为数据流通增加创新力和完善性。未来，隐私科技厂商、云提供商、电信运营商、数据交易所、政务平台等将进一步提供可信的交易环境与平台，帮助越来越多企业、公民、组织获得可信、有价值的数据。隐私计算等新型理念与技术进一步从小范围的应用过渡到行业性、跨行业解决方案，被积极应用于更多业务领域。

与此同时，聚焦隐私科技中的关键技术，利益相关方需要合力制定多方安全计算、联邦学习、同态加密、差分隐私等技术应用标准，建立技术成熟度模型，进一步推动技术快速成熟与市场化。目前，已有相关隐私计算系列标准制定完成，如《基于多方安全计算的数据流通产品技术要求与测试方法》《基于联邦学习的数据流通产品技术要求与测试方法》《基于可信执行环境的数据计算平台技术要求与测试方法》《区块链辅助的隐私计算技术工具技术要求与测试方法》，后续技术安全性的标准还将进一步统一和规范；技术成熟度需要加强计算效率和性能的重视；通用性则涉及不同行业、不同企业、不同业务场景之间，相关技术是否通用。这些都是隐私科技发展必须思考的问题，只有持续性推动隐私计算技术成熟度和通用性的标准化，才为数据合规流通夯实技术基础，加快隐私科技产品市场化阶段的可复制性。

## 5.4 产业：政府与企业携手共进推进数据流通

中央《数据二十条》的发布与实施为深化数据要素市场化配置改革，释放数据要素价值，推动数字经济高质量发展提供了政策引导和方向指引。 作为数字经济发展的新引擎，我们可以预见，未来会有更多的中央与地方性政策进一步为数据要素市场的供需匹配、价值评估、交易模式、信任机制、数据确权等方面进行规范、引导与激励。与此同时，隐私科技作为数据要素市场基础设施中的重要技术，也将从企业和平台侧进一步深化与挖掘数据流通场景与价值。政企双方将共同培育出一批示范性场景和案例，携手推动数据流通，持续推动数字经济的增长与繁荣。

# 附录
# APPENDIX

## 常见隐私科技解决方案类型

**1）数据发现、分级分类与标识**

定义：通过自动化的数据扫描和策略识别的方式定位数据、分级分类数据，以进一步实现分级保护。在数据发现过程中基于正则表达式、关键字、UDF等模式或者机器智能学习模式，自动将库、表中的数据进行识别和分级分类，并可视化分级分类结果。基于分级分类结果对字段或表级别打标签。

**2）数据去标识化、匿名化工具**

数据去标识化工具在个体基础上，采用技术手段如假名、哈希、加密等替代对个人信息的标识，保留了个体的颗粒度，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体。数据匿名化工具通过对数据进行随机映射、统一泛化等操作，使其发布的数据无法关联到任何具体个体。

**3）数据映射**

采用手动或自动的方式帮助企业确定整体数据流，识别企业处理的个人信息，个人信息的来源和去向，存储、传输或处理数据的系统或流程。

**4）个人信息授权管理**

帮助企业收集、跟踪、展示和管理用户的个人信息授权同意，保证数据在不同阶段的处理活动均给予“告知 – 同意”的原则。

**5）数据主体权利管理**

帮助企业为个人行使数据权利提供更便捷的方式，包括响应个人关于行使访问权、更正权、可移植权和删除权等权利的请求。

**6）数据流动监控**

通过技术来实现对数据真实流转情况的可视以保证数据资产分布及访问行为态势的清晰度、透明度和可控性，并通过对数据流转路径和敏感数据访问行为的分析，预测数据资产可能面临的泄露风险、丢失和滥用。

**7）隐私事件响应**

提供符合法律要求的合规应急事件自动化处理，包括向相关方提供隐私事情详情和需履行的事件通知义务，帮助企业应对法律风险。

**8）隐私风险与合规评估平台**

帮助企业基于线上流程和评估模板开展隐私影响评估、数据出境安全评估、第三方合规评估、风险隐患定位等评估工作，高效规模化完成需要电子表格、数据输入和报告的任务，为企业提供合规性证明的平台。

#### 9）数据和隐私合规检测工具

针对网页、安卓 App、iOS App、小程序、IoT 设备等进行自动化隐私合规检测的工具，以确保企业的网页 cookie、APP、小程序等遵守相关法律法规和政策。

#### 10）隐私计算平台

基于一种或多种隐私计算技术，如联邦学习、多方安全计算、隐私求交、可信执行环境、差分隐私等技术，在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算，实现数据在流通与融合过程中“可用不可见”的数据处理平台。

## 常见数据流通管控保障技术

#### 1）数据使用控制

数据使用控制技术主要用于在数据流通过程中，确保使用方按照设置的权限或方法来访问、使用或处理数据，实现对数据全生命周期内按需受控的跨域使用控制。通过定义不同的角色和权限级别，确保只有授权的用户或实体能够访问和使用特定的数据，同时也支持设置访问和使用控制策略的设置和实施，在数据接入、处理、流通、使用全过程进行管控，防止数据未经授权的访问和使用。

#### 2）数据密态胶囊

数据密态胶囊是一种复合技术，结合了数据加密、数据血缘等技术，将密态数据、数据血缘和数据的权限管理能力进行绑定，组合成数据密态胶囊，使得密态数据在离开数据提供方的安全区域后，仍然被有效地管控。数据密态胶囊内的授权规则是被强制验证的，外界既无法篡改该规则，也无法绕开该规则使用密态数据。

#### 3）智能合约

智能合约有助于保障提供方的数据控制权。它是内置于代码中、在满足某些触发条件时自动执行某些功能的程序，具有预防违约、保证业务逻辑自动强制执行的特点。在数据流通场景下，智能合约可以自动拦截非经许可的数据传输行为，实现数据要素价值变现的自动分配机制，在交易完成后自动删除特定数据库内的数据。

#### 4）数据沙箱

数据沙箱通过在可信计算环境上执行外部程序的方式，保障数据安全可控。它将调试环境和运行环境隔离，数据需求方相关人员以及数据分析师只能在调试环境中使用基于原始数据抽样的数据进行代码调试，同时保证代码在隔离环境中运行，全流程各参与方均无法接触到全量数据。

#### 5）分布式数字身份

分布式数字身份技术为数据流通用户和数据本身提供可追溯、不可伪造、不可篡改的数字身份，并支持身份的颁发与校验。基于区块链的分布式数字身份认证方案可以将用户身份管理权限交给用户自身，不需要中心化的第三方参与，由用户持有和控制其身份标识，并通过数字签名等技术保证身份的可验证性。此外，数据流通供需双方可以自由选择与哪些对象共享自己的哪一部分身份信息，进而保护数据流通交易当事人的隐私。

#### 6）数字水印

数字水印技术能够在不破坏原有数据内容和对象可用性的前提下，通过一定的规则与算法将标识信息隐藏在结构化数据中。水印信息可以是数据权利人的身份信息、作品序列号等，用以证明真实权利人，并作为主张他人侵害数据权益的证据。在发生数据泄露事件后，可以通过提取嵌入在被泄露数据中的水印信息，准确定位数据泄露的风险发生主体，从而解决数据泄露时数据无法追溯的难题。

## 主流隐私计算技术

### 1）差分隐私

差分隐私是密码学中的一种手段，当从统计数据库进行查询时，提供了一种最大化数据查询的准确性，同时最大限度减少识别其记录的机会。它可以通过对数据引入随机性，添加噪声，从而防止数据被推测。差分隐私能够做到在利用数据来满足业务需求的同时，抵抗外部攻击和实现隐私保护。在差分隐私技术的实践中，实现差分隐私保护的机制通常包括拉普拉斯机制和指数机制。拉普拉斯机制实现了对数值型结果的保护，指数机制则是实现对离散型结果的保护。如今，差分隐私已经应用到各行各业的业务场景中，比如医疗行业用于患者电子健康档案的保护、医疗传感器如可穿戴设备的地理位置信息的保护等。

### 2）同态加密

同态加密是一种特殊的密码学技术，它可以通过对加密的数据进行计算得到密文计算结果，后对其进行解密得到与原数据计算结果相同的结果。同态加密能够真正做到数据的“可算不可见”，在得到正确 结果的同时保证了数据安全和隐私保护。在实践中，同态加密根据加密方式可以分为部分同态加密和全同态加密。部分同态加密是指仅支持对密文进行部分的计算，全同态加密是指对密文进行任意的计算。

近几年，同态加密的应用场景较广泛，在云计算、区块链和物联网中都存在同态加密的运用。如在云计算场景下，通过同态加密实现数据的流通，保证数据在流通的全过程中是密文的形式，确保数据安全。又如在区块链场景下，同态加密帮助实现了链上数据的保密性。同态加密的运用为数据的流通提供了安全保障，因此它已逐渐渗透到了医疗、金融、法律业等高度监管的行业。

### 3）联邦学习

联邦学习是隐私计算中最常见的一项技术，它本质上是一种分布式机器学习技术，通过中央服务器来实现对加密数据的流通与处理，最后完成多方分布的机器学习框架。联邦学习能够在确保数据合规与隐私保护的前提下，多方共同参与完成联合建模。在整个过程中，既保证了数据安全，又实现共同学习的目标，协助企业解决数据孤岛、数据不可用、数据泄露等问题。实践中主要运用在企业风控评定、安全防控检测、医疗诊断等方面。

联邦学习在使用过程中，根据参与方之间的样本分布，分为横向联邦学习、纵向联邦学习和联邦迁移学习，不同的分类在实践中对应解决了不同类型的问题。

横向联邦学习适用于参与方特征相同，但是样本重叠较少的情景。横向联邦学习主要通过增加样本数量，达到了提升模型的准确性和泛化能力的目的。

纵向联邦学习则适用于参与方样本相同，但是特征重叠较少的情景。纵向联邦学习主要通过丰富样本来优化学习模型。

联邦迁移学习适用于参与方特征和样本重叠度都较低的情景，是对横向联邦学习和纵向联邦学习的补充。

### 4）隐私集合求交

隐私集合求交指的是，在保证互相之间不透露原始数据集的情况下，求得多方数据集之间的交集。隐私集合求交的用途十分广泛，如广告效果追踪、多方安全计算等。在前面联邦学习的介绍中，纵向联邦学习需要较高的参与方样本重合度，那么如何

才能在不向其他联邦学习参与方透露自己有哪些数据的情况下仍能找出重合的数据样本呢？答案便是隐私集合求交。隐私集合求交有多种实现手段，如将数据进行哈希处理后进行求交，便可以迅速找到交集，并使得对方无法获得原始数据；当然，哈希仅仅是比较简单的手段，且安全性不佳。目前，常见的隐私集合求交方法包括不经意传输、基于密钥的方案、基于混淆电路的方案等，不同方案在安全性、计算成本、通信成本等方面有着不同的优劣势。

**5）多方安全计算**

多方安全计算是指，各参与方在互不信任的场景下，共同计算一个联合函数，并保证参与方仅能获得自己的计算结果，不泄露其他任何信息。它既能够确保数据的保密性，还能够确保各参与方都收到原有计算函数的正确结果。多方安全计算主要可以分为混淆电路和秘密分享。混淆电路能够在保证不泄露参与方数据的情况下进行计算，并且指定计算结果的所属者。秘密分享是通过拆分秘密信息，来实现数据安全，防止信息被丢失、破坏和篡改。近几年，多方安全计算陆续开始也应用到各类行业，其中混淆电路通常用于各类计算，而秘密分享在身份认证、密钥管理等方面有重要的作用。

**6）零知识证明**

零知识证明同样是一种特殊的密码学技术。一般来说，若需证明一个事实，如自己的身份、对某权益的所有权，验证者需与证明者掌握同样的信息才可进行验证，如口令、证书；但利用零知识证明技术，证明者能够在让验证者掌握任何被验证的具体信息的情况下，验证者仍可以进行有效的验证。“色盲游戏”是一个经典的零知识证明的例子：假设你有红绿两个小球，两个小球除了颜色之外完全相同，但你的朋友是红绿色盲，无法区分两个小球，那么为了证明这两个小球颜色的确是不同的，你的朋友双手各持一个小球并将手藏在身后，然后随机交换双手的球并询问你双手的球是否交换过，那么由于你每次都能答对，你的朋友最终相信了这两个球的颜色的确是不同的，尽管他最终也无法知道两个球分别是什么颜色。

目前，零知识证明被较多用于加密货币中，用于保护交易中的隐私，确保匿名支付的情况下仍然能够在区块链上验证交易。主流协议包括 zk-SNARK,zk-STARK 等。但除了加密货币中的匿名支付之外，零知识证明的特性使其能够用于更加广泛的场景，

包括：

资产管理：如在 NFT、元宇宙的应用中，通过零知识证明在不泄露具体资产信息的情况下证明自己对资产的所有权；

身份认证与访问控制：在不泄露申请人的具体身份信息、口令的情况下，进行身份认证、权限管理；

合规证明：在不泄露合规详情的情况下，如纳税记录，证明自己对法律法规的遵从情况。

**7）合成数据**

顾名思义，合成数据即通过计算机来生成的“假”数据，而不是从客观世界收集到的可以反映真实事件、环境、人物的数据。在很多数据使用场景中，受限于数据获取的困难、成本的限制以及隐私合规的要求，真实数据无法满足使用要求，如在模拟自动驾驶路况时，通过合成数据模拟出大量现实中较难出现的极端工况数据；训练机器学习模型时，通过合成数据模拟出样本不足的数据集；在涉及个人信息相关的研发、测试中，通过合成数据模拟出符合业务需求的个人信息，从而避免使用真实的个人信息；

**8）可信执行环境**

可信执行环境，即在中央处理器内预制特定、

隔离的安全区域，有着独立的硬件资源和软件程序，在该区域内加载的程序和指令均以既定的形式运行，除授权信道外，可信执行环境中的信息无法被外部访问，且在可信执行环境内部中的可信应用也是相互隔离的。通过这种机制，有效地保护了可信执行环境中数据及可信应用的机密性和完整性。

除了保护交易、内容保护等安全使用场景外，可信执行环境在联邦学习中也有其用武之地。在联邦学习中，为了保护聚合各方模型数据的参数服务器的数据安全，通常会采用同态加密等密码学手段进行保护，但同时也带来了极高的运算成本，降低了联邦学习的效率，而在可信执行环境中进行参数聚合，则可以较好地平衡安全与效率。

## 文末引用

[1] 中国信息通信研究院安全研究所《数据要素流通视角下数据安全保障研究报告》

[2] IBV,Prosper in Cyber Economy

[3] TrustArc, 2024 Global Privacy Benchmarks Report

[4] 欧盟委员会 ,Working Programme 2024, COM

[5] Numbers and Figures | GDPR Enforcement Tracker Report 2023/2024 (cms.law)

[6] Privacy Enhancing Technologies Market Size, Share & Trends Analysis Report By Component (Software, Service), By Type (Cryptographic Technique, Anonymization Technique), By Application, By End-use, By Region, And Segment Forecasts, 2024 – 2030

EY安永
Building a better working world

建设更美好的商业世界

安永的宗旨是建设更美好的商业世界。我们致力帮助客户、员工及社会各界创造长期价值，同时在资本市场建立信任。

在数据及科技赋能下，安永的多元化团队通过鉴证服务，于 150 多个国家及地区构建信任，并协助企业成长、转型和运营。

在审计、咨询、战略、税务与交易的专业服务领域，安永团队对当前最复杂迫切的挑战，提出更好的问题，从而发掘创新的解决方案。



APAC no. 03021126
ED None

关注安永微信公众号，
扫描二维码，获取最新资讯。

ey.com/china

SICSI
CYBER RESEARCH INSTITUTE
赛 博 研 究 院
Shanghai Institute of Cyberspace Security Industry

上海赛博网络安全产业创新研究院（以下简称赛博研究院）是在上海市经信委和上海市社团局共同指导下的民办非企业，是国内从事数字经济、网络安全、数据合规的专业智库。

赛博研究院秉持专业、诚信、创新、合作的精神，已经为各级党政部门和各类企事业单位提供了包括战略规划、合规咨询、人员培训、技术平台等综合服务，并是上海市通信管理局、国家计算机网络应急技术处理协调中心上海分中心等监管部门的专业支撑单位，积极推动我国数字经济发展和网络强国建设。

成立至今，赛博研究院已发布《全球数据跨境流动政策与中国战略》《人工智能赋能网络空间安全：模式与实践》《数据安全治理白皮书》《云平台安全责任与治理》《智能网联汽车产业趋势与安全挑战》《人工智能数据安全风险与治理》《人工智能时代数字内容治理的机遇与挑战》等数十份具有较高影响力的专业报告。

2023-2024

# 全球数据流通与隐私科技发展报告

GLOBAL DATA CIRCULATION AND
PRIVACY TECHNOLOGY DEVELOPMENT REPORT

EY安永
Building a better working world

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院