隐私计算联盟
Privacy Preserving Computing Alliance

隐私计算技术应用合规指南

（2022 年）

隐私计算联盟

2022 年 12 月

版权声明

免责声明

本报告的内容和观点不构成任何相关问题的法律意见。因隐私计算及其他数据流通技术仍在快速发展，业务模式不断迭代，法律规范和行业标准不断更新，企业实际业务中产生法律意见或专业分析需求时，建议咨询相关专业人士。

编写委员会

❖ **牵头单位**：

隐私计算联盟

❖ **编写单位**（排名不分先后）：

上海市方达（北京）律师事务所、世辉律师事务所、德恒律师事务所、上海富数科技有限公司、深圳市洞见智慧科技有限公司、华控清交信息科技（北京）有限公司、上海零数众合信息科技有限公司、北京腾云天下科技有限公司、杭州趣链科技有限公司、星环信息科技（上海）股份有限公司、神州融安数字科技（北京）有限公司、蚂蚁科技集团股份有限公司、天翼电子商务有限公司、OPPO 广东移动通信有限公司、浙江吉利数字科技有限公司、深圳国家基因库。

❖**编写组主要成员**（排名不分先后）：

王丹阳	吕艾临	侯　宁	闫　树
张斯睿	王泽宇	袁　博	韩　璐
王新锐	刘晓霞	王一楠	周　望
万千惠	全婉晴	卞　阳	方　竞
杨天雅	李　倩	曾钰涵	王湾湾
姚　明	殷宝玲	薛　婧	靳　晨
时　代	王云河	张嘉熙	林　乐
兰春嘉	杨　珍	胡豫皖	李仲平
葛梦莹	南钰彤	徐　静	汪小益
张延楠	江　涛	彭海祥	杨一帆
李登峰	刘　伟	宁立君	昌文婷
彭　晋	白晓媛	贺　伟	徐　潜
喻　博	付艳艳	李晨龙	薛　勇
吴　凯	游丽金	王伟文	韦振勇

引　言

近年来，随着数字经济的发展和数字化转型的深入，企业逐渐积累大量数据，需要与外部数据进行融合以充分释放价值。但是，全球数据安全事件频发，数据保护合规监管日趋严格，企业在数据流通和协作方面的风险及合规成本大大增加。在此双重背景下，企业亟须探索出一条数据安全流通的新道路，在保证数据安全的前提下挖掘数据价值。隐私计算技术因其“数据可用不可见”的特点，为上述困境提供了解决思路。

隐私计算是一类在提供隐私保护的前提下，实现数据价值挖掘的技术，是人工智能、密码学、数据科学等众多领域交叉融合形成的跨学科技术[1]。应用隐私计算，原始数据不出域，参与方也难以逆推原始输入数据，降低了原始数据泄露的风险，进而帮助企业履行安全保障义务，降低数据滥用风险。

近几年，隐私计算发展迅速。据统计，2016 年至 2022 年第一季度，中国隐私计算企业的累计融资额超 30 亿元人民币，资本热度持续提升[2]。根据隐私计算联盟 2022 年发布的《隐私计算产业图谱 1.0》，互联网、大数据、金融科技、AI、区块链、云服务和信息安全等行业的企业都入局隐私计算技术服务产业，金融、政务、通信、互联网、工业及能源、医疗等行业领域均有应用需求。此外，国务院、各中央部委出台的一系列政策文件，如发展改革委等四部委发布的《全国一体化大数据协同创新体系算力枢纽实施方案》等，以及《上海市数据条例》等地方性法规等也开始将隐私计算作为一种数据流通过程中的

[1] 闫树，吕艾临：《隐私计算发展综述》，载《信息通信技术与政策》，2021 年第 6 期，第 1 页。
[2] 艾瑞咨询 2022 年《中国隐私计算行业研究报告》第 13 页。

安全保障技术来鼓励使用。

然而，在火热的发展势头下，隐私计算的应用也面临着一些挑战，在合规方面尤为明显。一方面，近年来我国的数据合规监管趋严，立法愈发频繁，企业的数据合规意识也逐渐建立，对数据合规问题的关注度提升。另一方面，随着《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》”）的出台和生效，个人信息的处理行为面临着更严格的法定义务和法律责任约束，隐私计算应用于处理个人信息时也必须考虑如何遵守相应要求。而在现阶段，企业对于授权同意、个人信息保护影响评估以及个人信息权利保障等合规义务如何落地仍然存在一些疑惑，如何在匹配《个人信息保护法》合规要求的同时尽可能降低合规对业务的影响，仍有待探索。因此，在相关实施细则出台和监管执法案例出现之前，很多需求方对隐私计算技术应用持谨慎的观望态度，行业内对于隐私计算应用的合规性展开了一些讨论，对于法律规定的合规要求也产生了一些理解和认识上的偏差。

对此，隐私计算联盟、中国信通院云计算大数据研究所和多家企业共同完成了《隐私计算技术应用合规指南（2022 年）》。在期待立法不断完善、实践不断创新的同时，我们尝试在我国现有立法框架下，对隐私计算技术应用的合规问题进行探索和梳理，对隐私计算技术面临的合规挑战进行分析，并提出一些合规要点，希望对现阶段的隐私计算技术应用提供一些合规指引和参考、为未来行业的规范和立法的完善提供一些思路。

目　录

表 目 录

图 目 录

第一章

概述

(一) 隐私计算技术的概念和原理

隐私计算是指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，实现数据在流通与融合过程中的“可用不可见”[3]。**主流的隐私计算技术可以分为三大方向：**一是以**多方安全计算**为代表的基于密码学的隐私计算技术，二是以**联邦学习**为代表的人工智能与隐私保护技术融合衍生的技术，三是以**可信执行环境**为代表的基于可信硬件的隐私计算技术[4]。

多方安全计算可以在各方不泄露输入数据的前提下完成多方协同分析、处理和结果发布，因此广泛应用于联合统计、联合查询、联合建模、联合预测等场景。**联邦学习**能够在本地原始数据不出库的情况下，通过对中间加密数据的流通与处理来完成多方联合的机器学习训练，因此广泛应用于联合建模，也可与可信执行环境配合使用，提供安全性、应用性更强的综合解决方案。**可信执行环境**通过软硬件方法在中央处理器中构建一个安全的区域，保证其内部加

[3] 隐私计算联盟、中国信通院云大所《隐私计算法律与合规研究白皮书（2021 年）》。
[4] 隐私计算联盟、中国信通院云大所《隐私计算白皮书（2021 年）》。

载的程序和数据在机密性和完整性上得到保护，可以完成对多方数据完成联合统计、联合查询、联合建模及预测等各种安全计算[5]。

(二) 隐私计算技术合规讨论的产生原因

在我国，隐私计算技术应用的合规在行业内引发了热烈的讨论，原因主要有以下几点：

多主体参与导致法律关系复杂。从法律主体看，隐私计算技术应用往往会涉及多个参与方共同协作，数据提供方、技术提供方、结果使用方是最为常见的三类主体。**数据提供方**一般是指在隐私计算技术应用过程中提供数据的主体。**技术提供方**一般是指提供数据处理平台、算法工具、解决方案等技术支持的主体。**结果使用方**一般是指获取隐私计算最终输出的数据结果并进行场景应用的主体。在实践中，还存在数据提供方本身不只一方、各参与方角色重合等情况。因此，一个隐私计算应用场景中往往包含多对法律关系，各参与方角色的重合还会带来数据合规义务的竞合或抵消。倘若不能准确判断各方之间的法律关系或明确法律义务或法律责任，就会引发一些合规问题。

受疫情影响，某快递公司“先寄后付”业务深受客户追捧，但仅依靠快递公司内部用户数据无法准确判断客户是否为低风险用户，若判断失误，容易引发坏账风险。故在第三方隐私计算技术提供方的协助下，该快递公司引入某大型银行信用卡中心掌握的用户在金融业务中的个人信用相关行为和跨行数据，通过联合建模建立散单客户风险识别模型。

在上述案例中，银行信用卡中心为数据提供方，快递公司同时为数据提供

[5] 隐私计算联盟、中国信通院云大所《隐私计算白皮书（2021 年）》。

方和结果使用方，技术提供方为第三方隐私计算技术服务方。

隐私计算技术在我国的合规价值缺乏背书。隐私计算技术包含多种数据处理行为，各参与方应当遵守我国数据合规相关法律法规。尽管目前我国数据合规法律的基本框架已初步建立，但配套的实施细则尚不完备，可供参考的司法和执法案例较少。相比之下，国外在立法和监管方面提供了更明确细致的指引。欧洲数据保护委员会（EDPB）发布的《关于第 25 条的设计和默认数据保护指南》在建议部分指出，有条件的使用隐私增强技术可以作为满足欧盟《通用数据保护条例》（GDPR）第 25 条规定的保护措施[6]。这在某种程度上从监管的角度赋予了隐私计算技术能够帮助履行合规义务的法律地位[7]。但目前在我国，隐私计算技术的合规价值尚未得到类似的背书。**实际上，隐私计算技术的合规价值会因法律体系、社会和经济背景的不同而有所不同。在立法方面，**尽管我国的《个人信息保护法》在立法原则上与欧盟《通用数据保护条例》有共通之处，但具体的法律规定存在很多差异。因此，隐私计算技术在欧盟得到认可的合规价值，放置在我国的法律体系下并不天然成立。**在社会和经济背景方面，**隐私计算在欧洲的推广主要得益于隐私保护问题亟待解决，其本身就带有一定的合规属性；而隐私计算在我国的快速发展主要是因为能够促进数据流通，

[6] 见 Guidelines on Article 25 Protection by Design and by Default 第 30 页。EDPB 指出，最先进的隐私增强技术（Privacy-enhancing technologies）可以被视为 GDPR 第 25 条要求采取的措施（如果适用于基于风险的方法）。使用隐私增强技术本身不一定能完全履行 GDPR 第 25 条规定的义务，数据控制者应当评估该措施在实施数据保护原则和数据主体权利方面是否适当有效。

[7] 欧洲数据保护委员会 （EDPB）是根据《通用数据保护条例》（GDPR）的规定设立的独立机构，其任务和职责包括提供一般指导（包括指南、建议和最佳实践）以澄清法律并促进共识或推动欧盟的数据保护法律的实施等。

其价值更多的体现在促进社会经济发展层面。基于以上差异，隐私计算技术在我国的合规价值，需要基于我国的具体情况进行研究和讨论。

技术与法律对于相同问题的认知存在差异。隐私计算技术的合规分析，涉及技术与法律两大专业领域的碰撞与融合。对法律专家而言，判断隐私计算技术的合规性，需要理解通过技术语言描述的数据处理行为，将其与法律条文的规定相对应，进而判断相关行为属于何种法律行为，会触发何种合规风险。对技术专家而言，了解隐私计算技术应用合规性，也需要经历从技术到法律的认知转变。这种涉及跨专业的沟通往往会引发一些认识和理解上的偏差，进而导致关于合规问题的一些争议和讨论。

(三) 隐私计算技术的法律适用

讨论隐私计算技术应用的合规问题，首先需要明确法律适用，厘清法律关系。尽管我国数据保护领域的相关立法尚不完备，但现有法律框架基本可以涵盖隐私计算应用所涉及的法律行为。各参与方需根据隐私计算应用的场景进行具体的判断和分析。

隐私计算技术应用本质上是一种数据处理行为，各方在隐私计算技术应用涉及的数据提供、加工、传输、使用等环节的数据处理行为，均适用相关法律法规对于数据处理的要求。

首先，应用隐私计算技术应当遵守《中华人民共和国民法典》[8]

[8] 《中华人民共和国民法典》第四编“人格权”第六章“隐私权和个人信息保护”。

《中华人民共和国刑法》[9]等**综合性立法以及相关司法解释**[10]中对于个人信息保护和数据保护的相关要求，违反相关规定将视情节承担相应的民事或刑事责任。

其次，应用隐私计算技术应当遵守数据合规领域的专门规定。2021 年，《中华人民共和国数据安全法》（以下简称“《数据安全法》”）和《个人信息保护法》相继正式出台并生效，与此前的《中华人民共和国网络安全法》（“《网络安全法》”）共同构成了**我国数据合规领域的基本法律架构。**2022 年 9 月 12 日，国家互联网信息办公室发布了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》，拟修订后的《网络安全法》与《个人信息保护法》《数据安全法》的衔接更加严密合理。违反《网络安全法》《数据安全法》和《个人信息保护法》的相关规定将根据不同情节承担暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照、高额罚款等行政责任。

同时，应用隐私计算技术应遵循相关国家标准、行业标准中对于数据处理行为的细节要求，如《信息安全技术 个人信息安全规范（GB/T 35273-2020）》《信息安全技术 个人信息去标识化指南（GB/T 37964-2019）》等。

此外，若隐私计算技术应用涉及特殊监管行业，如金融、医疗、

[9] 《中华人民共和国刑法》第二百五十三条之一、第二百八十五条、第二百八十六条、第二百八十七条之二等。

[10] 《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》等。

汽车、地图测绘等，**也应当符合相关行业对于数据处理行为的具体要求**。以隐私计算技术应用最广泛的金融行业为例，行业相关要求包括《征信业管理条例》《征信业务管理办法》《中国人民银行金融消费者权益保护实施办法》《银行金融机构数据治理指引》《金融信息服务管理规定》《银行保险机构信息科技外包风险监管办法》等等，还包括《个人金融信息保护技术规范（JR/T 0171-2020）》《金融数据安全 数据生命周期安全规范（JR/T 0223-2021）》《金融数据安全 数据安全分级指南（JR/T 0197-2020）》等金融行业的相关标准。

(四) 隐私计算参与方法律关系认定

如前所述，隐私计算技术应用主要涉及**数据提供方、技术提供方、结果使用方**三类主体。在实际应用场景中，通常是由技术提供方为数据提供方或结果使用方部署隐私计算平台（包括软件、硬件或软硬件一体机），提供技术服务或软件开发服务，并负责隐私计算平台的日常运维，并不直接参与处理数据。除为数据提供方和结果使用方量身打造隐私计算平台之外，技术提供方也可以将自己的隐私计算平台部署在数据提供方或结果使用方本地，技术提供方作为平台方寻找掌握数据资源的数据提供方入驻平台，数据提供方将节点部署在技术提供方平台。

隐私计算技术应用涉及的各参与方之间的法律关系需要进行**个案分析**，在不同的应用场景中判断其所扮演的角色属于数据合规法律法规中的哪些义务方，确定所适用的法律法规，进而判断具体应当遵

守的合规要求。**在我国现行法律下，隐私计算技术的参与方可能被认定为如下法律主体，包括但不限于：**

1. 个人信息处理者

《个人信息保护法》第七十三条规定，个人信息处理者是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。根据《个人信息保护法》第二十条，两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，属于“共同处理个人信息”，若侵害个人信息权益造成损害的，应当依法承担连带责任。

一般情况下，**数据提供方和结果使用方**决定隐私计算过程中对个人信息的处理目的和方式，**基本可以被认定为个人信息处理者。技术提供方**一般仅提供技术支持，例如提供算法逻辑、技术解决方案、数据存储工具等，并不会对数据处理的目的和方式产生决定性影响，因此**被认定为个人信息处理者的可能性较低。**但若技术提供方与数据提供方和/或结果使用方构成委托处理关系，仍应当根据《个人信息保护法》的规定配合委托方履行相关合规义务。

2. 委托人和受托人

《个人信息保护法》第二十一条提到了委托人和受托人的概念。委托人更具决定权，会对受托人进行审慎监督，确保其按照约定来处理个人信息。受托人则需要严格按照约定来处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息，同时需采取必要措施来保障个人信息安全，合作结束后，受托人应当将个人信息返还或者予

以删除，不得保留。

在隐私计算技术的应用场景中，**数据提供方和结果使用方**往往对于数据有更多的控制权，**可能会被视为委托人；技术提供方**不决定个人信息处理的目的和方式，只是提供技术支持，所以**可能被认定为受托人。**

值得注意的是，目前在法律层面仅针对“个人信息的处理”对委托处理中双方权利义务进行了明确规定，但委托处理是一种常见的数据处理方式，可以理解为民法中委托合同关系在数据处理方面的应用。实践中，对非个人信息的委托处理也可以参考上述合规逻辑，在该等合规要求的基础上具体约定双方的权利义务。

3. 个人信息的提供方与接收方

《个人信息保护法》第二十三条规定，个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照《个人信息保护法》的规定重新取得个人同意。

根据《个人信息保护法》第二十三条的表述，个人信息的提供和接收发生在个人信息处理者之间。如前文所述，在隐私计算技术应用场景中，通常认为技术提供方不属于个人信息处理者；通过隐私计算技术，**数据提供方**以“可用不可见”的方式将个人信息提供给**结果使用**

方使用，因此二者可能被认定为个人信息的提供方和接收方。

表 1：隐私计算技术各参与方之间的法律关系

法律关系 / 参与方	共同处理	委托处理	提供个人信息
数据提供方	共同处理者	委托人	提供方
技术提供方	/	受托人	/
结果使用方	共同处理者	委托人	接收方
法定义务	❑ 应当约定各自的权利和义务。个人可以向任何一方要求行使《个人信息保护法》规定的权利。 ❑ 对共同处理侵害个人信息权益造成损害的，应当依法承担连带责任。	委托人： ❑ 应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。 ❑ 对受托人的个人信息处理活动进行监督。 ❑ 进行个人信息保护影响评估。 受托人： ❑ 应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息。 ❑ 委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。 ❑ 未经个人信息处理者同意，受托人不得转委托他人处理个人信息。 ❑ 应当依照《个人信息保护法》和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行《个人信息保护法》规定的义务。	提供方： ❑ 向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。 ❑ 进行个人信息保护影响评估。 接收方： ❑ 应当在提供方告知并取得同意的处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照《个人信息保护法》的规定重新取得个人同意。

第二章

隐私计算技术的合规价值

隐私计算技术本质上是一种保护数据安全，促进数据流通的技术。随着我国数据保护领域的立法不断完善，保障数据安全成为数据处理者的法定义务，保护个人信息主体的合法权益也成为监管关注的重点。在此背景下，隐私计算技术也在合规层面被赋予了新的价值。

(一) 隐私计算技术有助于遵守最小必要原则

《个人信息保护法》第六条规定，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。这包含两方面内容，**一是“目的限制”**，即处理目的明确合理+处理行为与处理目的直接相关，**二是“最小必要”**，即不得超出实现目的的最小范围过度收集个人信息。**隐私计算技术有助于遵守最小必要原则的体现主要是第二方面。**

首先，隐私计算技术可以通过技术手段限定初始的数据处理目的和使用范围，使得各参与方基于最初共同商定的范围来落实最小必要原则。例如，各参与方可以通过事先签订合约等方式，基于最小必要原则来设计可信执行环境中的代码执行规则，明确进入可信执行环境的具体数据类型、使用次数、算法规则等信息，从而实现从设计之初

就纳入最小必要原则；在具体的计算过程中，因为可信执行环境内的数据处理均是基于最初商定的技术方案进行运作的，所以在执行过程中各参与方很难超出最初约定的目的来使用数据。又如在隐私求交场景下，各参与方只会利用隐私求交所识别的交集的数据来进行建模处理，非交集的数据始终被排除在外，从而使数据处理符合最小必要原则。**其次，对于结果使用方而言，隐私计算技术可以使其从数据提供方处收集更少的数据来达到相同的数据处理目的，将“实现处理目的的最小范围”进一步缩小。**

例如，在个人向银行申请贷款时，银行希望了解个人目前在其他银行的贷款总额。通过隐私计算中的秘密分享技术可以在不泄露个人在其他各个银行的贷款数额的前提下，计算出个人贷款总额。如下图 1 所示，如果使用传统方式，结果使用方需要从银行 A、B、C 直接采集贷款信息，然后求和；相比之下，如通过秘密分享对原始数据进行计算，银行 A、B、C 并不需要将贷款信息直接传输给结果使用方，便可以直接计算出贷款总额，且结果使用方获得的输出结果只有贷款总额数值，并无法知悉各家银行分别发放的贷款数额。与传统方式相比，结果使用方获取的数据更少，也减少了数据流转，进而更加符合最小必要原则。

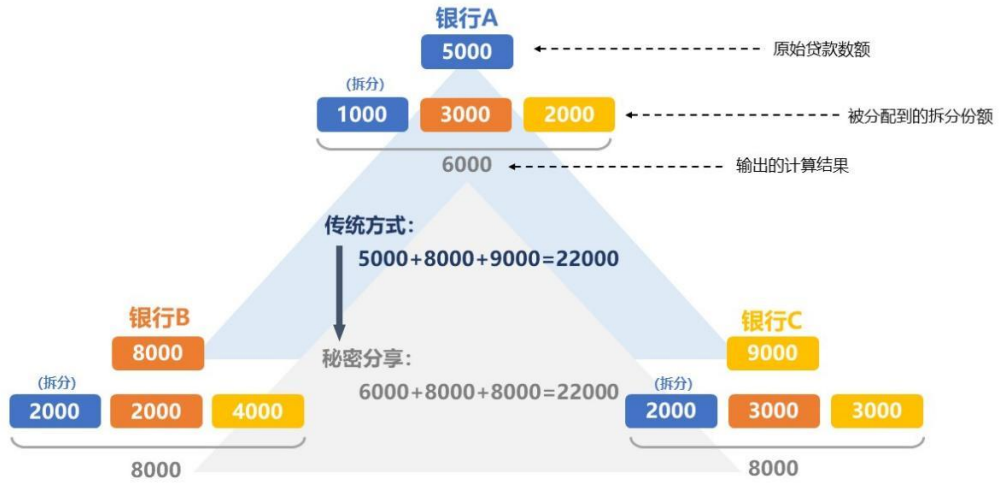

图 1：通过秘密分享计算个人贷款总和

(二) 隐私计算技术有助于提升数据处理的安全性

《数据安全法》第二十七条规定，开展数据处理活动应当依照法律、法规的规定……采取相应的技术措施和其他必要措施，保障数据安全。《个人信息保护法》第五十一条规定，个人信息处理者……应当采取相应的加密、去标识化等安全技术措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。**隐私计算技术可以保证原始数据不出域，从源头上减少数据泄露的可能性。**原始数据是企业在运营和提供产品和服务的过程中所积累的重要数据资产，尤其是用户个人信息的原始数据与个人信息权益紧密相关，一旦泄露会对个人权益造成严重损害，并承担相应的行政、民事甚至刑事法律责任。因此，在数据处理或数据开发利用过程中保证原始数据不出域，对于提升安全性意义重大。**在进行数据安全风险评估或个人信息保护影响评估时，采用隐私计算技术可**

被认定为安全风险相对更低。

隐私计算技术中的联邦学习是减少原始数据流转较为典型的例子。联邦学习是一类分布式的机器学习，各方参与者通过约定的算法协议来进行机器学习，数据仅在本地进行处理，只交换中间结果值来优化各方的模型，不直接共享原始数据，有效保障各方联合处理数据过程中的数据安全。此外，与传统的加密、去标识化单一技术相比，隐私计算通过将数据脱敏、差分隐私、同态加密等多种安全技术手段融合，为降低原始数据泄露风险提供多重技术保障。

隐私计算技术中的可信执行环境还可以通过硬件来提升数据处理的安全性。可信执行环境通过硬件 CPU 芯片来创造一个受保护的“飞地”（可以理解为是一个独立的安全操作系统），不同的程序可以在硬件环境中隔离运行，从硬件层面来保障数据安全，避免其遭受外界恶意程序或非授权第三方的干扰。

(三) 隐私计算技术有助于减少合作方的数据滥用

合作方的数据滥用本质上属于超出授权或未经授权使用数据的行为，如在合作过程中对获取的相关数据超出授权范围开发利用，或在合作结束后未经授权对数据进行后续的开发利用。对于个人信息而言，除了满足《个人信息保护法》第十三条规定的例外情形，处理个人信息应当取得个人同意。对于非个人信息而言，合作方通过签署协议获得数据上游方的授权从而有权将相关数据用于特定目的，也应当遵守与数据上游方之间关于授权的约定。实践中，企业通常会通过约

定违约责任的方式来限制合作方的数据滥用行为，但这是一种事后补救的思路，对于企业损失的挽回十分有限，也大大降低了企业将数据投入流通的意愿。

隐私计算技术恰恰可以在事前帮助降低合作方滥用数据的可能性。例如，**联邦学习**并不会直接共享原始数据，而仅仅是交换梯度值，即一种机器可读且难以复原为原始数据的数据碎片，通过这些数据碎片难以识别到具体的个体。各参与方都是获取此类数据碎片进行算法处理，优化模型。因此，参与方无法直接获得原始数据，也就降低了合作方滥用数据的风险。而**秘密分享**技术则通过对数据进行切片化处理，使得各参与方在仅获取密文碎片数据的情况下进行数据共享和使用；各方只能将相关数据用于已达成共识的特定技术方案所约定的使用目的；超出约定的使用目的，此类密文碎片数据很难进行复用。因此也就降低了合作方超授权范围使用的风险。

隐私计算技术可以减少数据被合作方滥用。例如联合风控的应用场景中，传统方案需要银行将个人用户的样本信息分别加密输入到合作数据源掌握的模型中，得到各自的评分后进行交叉评估，汇总得出评价结果；而在联邦学习方案中，各方数据不出域，各自在本地建模，只交互中间结果，各方各自在本地进行迭代训练，避免原始数据的泄露，也大大降低了合作方滥用原始数据的可能性。

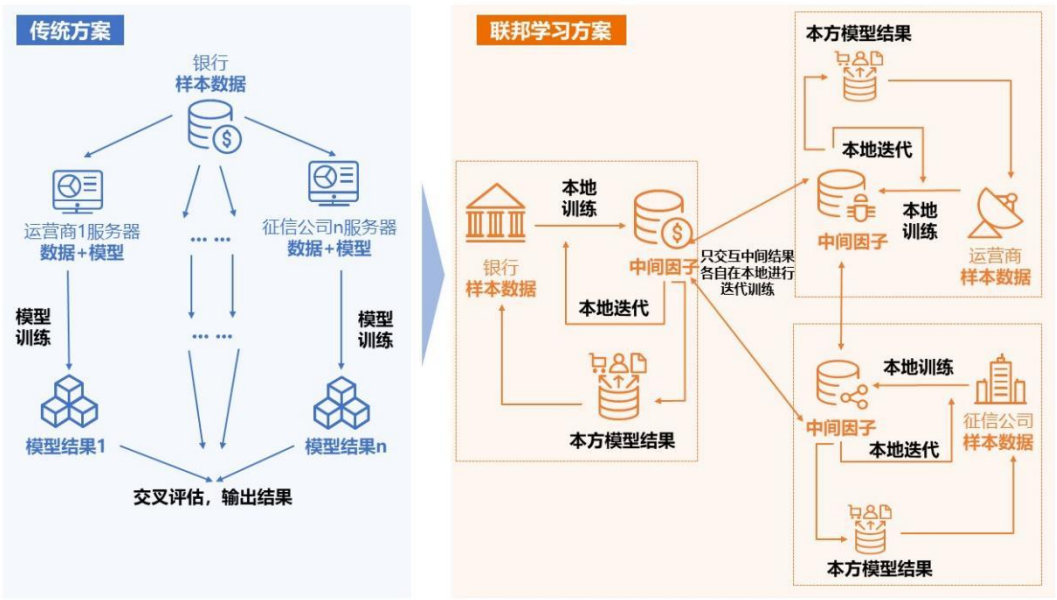

图 2：联邦学习实现“数据不动模型动”

第三章

隐私计算应用面临的合规挑战

随着我国关于数据合规的相关立法不断出台，对数据（尤其是个人信息）使用的监管要求也越来越严格，人们对隐私计算技术应用的合规以及其能带来的合规价值越来越关注。需要注意的是，隐私计算技术能够在一定程度上帮助保护个人信息，但其本质上是保护数据安全流通的一类技术，而非专为保护个人信息而设计的合规工具。与此同时，现有立法的配套实施细则尚不完备，监管执法案例尚不明确。因此，行业内关于如何在趋严的监管形势下合规应用隐私计算技术的讨论逐渐火热，隐私计算应用所面临的一些合规挑战也逐渐浮出水面。

(一) 挑战一：授权同意问题

一些观点认为，在不符合《个人信息保护法》第十三条规定的例外情形的前提下，使用隐私计算技术处理个人信息无需取得个人同意。理由有三类，或是认为在隐私计算技术处理个人信息的过程中，个人信息未出域，因此无需取得个人同意；或是认为尽管存在数据出域情况，但出域的数据经过处理后不再是个人信息，而是无意义的数据切片，因此无需取得个人同意；或是认为即使数据切片可以逆推还原为原始个人信息，但需要耗费极大的算力和时间代价，不具有实践可行

性，因此无须取得个人同意。这些观点中存在对《个人信息保护法》的两个误解。一是将“个人信息是否出域”当作判断“是否应当取得个人同意”的标准，二是通过隐私技术处理后的个人信息不再属于个人信息。

针对误解一，《个人信息保护法》的规定是除了《个人信息保护法》第十三条规定的例外情形，只有取得个人的同意才能处理个人信息。**因此，只要认定隐私计算技术属于处理个人信息的行为，在不满足例外情形的情况下，就应当取得个人同意。**根据《个人信息保护法》第四条第二款，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。隐私计算技术并非是对数据进行单一处理的行为，而是涉及各参与方之间的多次数据交互。尽管目前对于前述定义中列举的具体行为没有进一步的解释，但结合我国对于个人信息较为严格的监管态度，我们倾向于认为**隐私计算技术包含对个人信息的使用、加工、传输、存储，属于处理个人信息的行为。**故在不符合法定例外情形的情况下，使用隐私计算技术处理个人信息应当取得个人授权同意。

> **《个人信息保护法》第十三条　符合下列情形之一的，个人信息处理者方可处理个人信息：**
>
> **（一）取得个人的同意；**
>
> **（二）为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需；**
>
> **（三）为履行法定职责或者法定义务所必需；**

（四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；

（五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；

（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；

（七）法律、行政法规规定的其他情形。

依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。

误解二实际上是对我国立法中“匿名化”的理解存在偏差，我们将在下节中一并讨论。

(二) 挑战二：匿名化问题

一些观点认为，通过隐私计算技术处理个人信息，处理后的个人信息无法被还原，或虽然存在被还原的可能性，但还原该等信息将付出大量的时间和金钱成本，基本仅属于一个理想化的假设。因此，该观点将隐私计算技术处理个人信息的行为等同于将个人信息进行匿名化，进而得出对经过隐私计算技术处理（即匿名化）后的数据进行使用不再适用《个人信息保护法》。

对于匿名化的讨论和争议并非我国独有。以欧盟为例，第 29 条工作组（Article 29 Working Party）在 2007 年和 2014 年对于匿名化的解读就存在不一致[11]。2021 年 4 月 27 日，欧盟数据保护监督员

[11] A guide to the EU’s unclear anonymization standards (iapp.org).

（European Data Protection Supervisor, EDPS）和西班牙的数据保护机构（Agencia Española de Protección de Datos, AEPD）联合发布报告《与匿名化相关的 10 个误解》（“AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation”[12]），解释了人们对于匿名化认识上一些的误区，包括假名化和加密都不等同于匿名化，但加密是一种有效的假名化手段；随着时间的推移和新技术的不断发展，现有技术水平下达到的匿名化可能被推翻；百分百的匿名化不一定总能实现，现实中要考虑重识别的剩余风险；匿名化是一个二元概念，很难通过绝对的是或否去衡量，等等。

在我国，《个人信息保护法》对匿名化的定义是“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。”[13]对此，我国立法或监管机构并未进行进一步的解读，目前也尚无司法案例对匿名化进行判断，但首先可以肯定的是隐私计算技术与匿名化之间的关系不能一概而论。隐私计算技术是基于密码学、统计学及硬件实现等不同技术的统称，各类别的技术基于不同原理实现，其在不同场景中能够达到的数据保护程度有所差异。**在使用隐私计算技术的某些场景下，计算结果本身就包含标识符，或者计算的目的就是要输出某些带有个人标识的结果（如隐私求交）。**在这些情况下，隐私计算技术对个人信息的处理并不满足“无法识别”的要求。

对于“不能复原”，隐私计算使用加密方法对原始数据进行保护，

[12] AEPD-EDPS joint paper on 10 misunderstandings related to anonymisation | European Data Protection Supervisor (europa.eu).
[13] 《个人信息保护法》第七十三条（四）。

无论是采用同态加密的数据，还是多方安全计算（秘密分享）的碎片数据，理论上都可以进行解密或复原，**可以说目前没有哪种技术对于数据的处理被证明是绝对不可被复原的。**但对该等解密和复原行为客观所需要的时间和成本的考虑并未通过立法体现。因此，**目前隐私计算技术的处理行为所达到的效果更类似于《个人信息保护法》定义的“去标识化”，**即“个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。”[14]故从立法文本角度出发无法做出隐私计算技术等同于匿名化的判断，对于相关数据的使用仍然要遵守《个人信息保护法》的相关规定。

(三) 挑战三：目的限制问题

如前文所述，隐私计算技术对于最小必要原则的实现主要体现在不超出实现目的的最小范围过度收集个人信息，即《个人信息保护法》第六条中的第二个方面。但是，**隐私计算技术通过技术手段限定初始的数据处理目的和使用范围，一个必要的前提是各参与方事先已经约定达成了一个数据处理目的和使用范围，**而对于这个处理目的是否明确合理，处理行为是否与处理目的直接相关（即是否满足《个人信息保护法》第六条中的第一方面），是依靠各参与方主观判断决定的，并无法通过隐私计算技术来实现。

A 公司在获得用户授权同意收集用户的浏览和搜索记录时所告知的使用目的是向用户展示商品或服务信息。但 A 公司与 B 公司达成商业合作，使用 A 公司收集的用户浏览和搜索记录信息帮助 B 公司优化营销策略。尽管 A 公司和 B

14 《个人信息保护法》第七十三条（三）。

公司在合作过程中使用隐私计算技术，可以保证双方合作过程中使用的数据仅限于求交后的交集部分，但对于 A 公司对该等信息的使用行为是否与所获得授权时告知的使用目的直接相关，需要另行判断。

因此，在希望通过隐私计算技术帮助实现最小必要原则的目的时，还应当注意考虑数据提供方将数据用于特定目的的数据处理行为是否与获得授权同意时告知的处理目的直接相关。

尽管隐私计算技术无法彻底解决或实现授权同意、匿名化或目的限制，但这些隐私计算技术无法实现或满足的条件，目前也没有其他技术能够实现或满足。从某种程度上讲，关于授权、匿名化的相关问题需要未来从立法、司法、监管和实践层面依靠多方探索和推动解决，寄希望于现阶段通过隐私计算技术的应用彻底解决这些问题是不切实际的。相反，在数据安全愈发受到重视的今天，隐私计算技术本身在提升数据处理安全性、减少数据滥用等方面的优势不应当被忽略。

第四章

隐私计算技术应用的合规要点

上文我们从宏观层面对于隐私计算技术本身所能带来的合规价值进行了探讨，接下来我们尝试从微观的角度对于**各参与方在具体应用隐私计算技术过程中应当关注的合规要点**进行梳理，希望能够在现有法律法规的框架下，为隐私计算技术的合规应用提供一些思路和参考。

(一) 合规分析思路

在我国现行法律法规下，隐私计算技术的各参与方在考量隐私计算技术应用合规性时，可以参考如下思路：

1. 判断数据类型

我国现行数据合规法律体系下的数据类型大致可以分为：个人信息，重要数据，国家核心数据，国家秘密等，以及一些涉及金融、健康、地理测绘等特殊监管数据。处理不同类型的数据将适用不同的法律，也对应不同的合规要求。

2. 判断适用法律

首先，隐私计算技术作为一种数据处理行为，普遍适用《网络安

全法》《数据安全法》等关于数据合规的一般性法律法规。**其次，**根据隐私计算技术拟处理的数据类型，可以进一步判断其特别适用的法律。以隐私计算技术应用最广泛的金融场景为例，涉及个人信息的，特别适用《个人信息保护法》；因涉及金融行业监管，还需要注意《征信业务管理办法》《中国人民银行金融消费者权益保护实施办法》等的要求。**此外，**一些国家标准也可以作为参考提升合规性，如《金融数据安全 数据生命周期安全规范（JR/T 0223-2021）》《个人金融信息保护技术规范（JR/T 0171-2020）》等。

3. 判断法律关系

最后，根据各方之间约定的合作模式，结合各方在隐私计算技术应用过程中承担的角色，以及适用的法律法规，判断各方之间的法律关系，进而判断各方应当承担的具体合规义务。

(二) 数据提供方的合规要求

1. 数据源合规

数据来源的合法性一直是数据合规的重点。若数据来源的合法性无法保证，则后续的数据处理和使用就如同食用“毒树之果”，将带来重大的合规隐患。因此，数据提供方在获取数据时应当注意满足法律法规对于数据源合法性的要求。不仅如此，考虑到风险传递，技术提供方和结果使用方也会不同程度地向数据提供方确认其数据来源的合法合规性，数据提供方需要对此配合提供相关证明文件等。

数据提供方可能通过以下几种渠道获取数据，不同的数据获取方

式对确保数据来源合法合规的要求有所不同。

直接收集，指基于合法业务需要或依法定职权而向特定信息主体直接收集或因特定信息主体使用产品或服务而由网络系统或其他记录载体自动采集数据。如通过 App 收集个人信息，通过问卷形式收集企业相关数据等。

间接获取，指通过授权使用或采购等间接方式获取数据。如将政务数据授权运营，银行采购外部数据完善风控模型等。

公开收集，指通过人工下载或爬虫等自动化手段收集对一般公众开放的数据。

自行产生，指企业自身在经营、科研、生产过程中产生数据，如运营数据、业务数据等。

（1）一般性要求

a. 经营范围

首先，应当考察主体获取数据所依托的业务经营行为是否在经营范围内。如 2022 年 10 月 9 日中国人民银行发布的《金融领域科技伦理指引（JR/T 0258—2022）》指出，坚持金融科技的本质是金融，涉及金融业务的按照相关规定取得金融牌照和资质，规范开展经营活动，杜绝以“科技创新”的名义模糊业务边界、交叉嵌套关系、层层包装产品、实施无证经营或超范围经营等行为。因此，数据提供方应当确保其自身以及数据上游方获取相关数据的行为未超出经营范围。

b. 特定资质

其次，对于开展特定经营活动需要特定资质的，应当注意是否获取相应资质并在有效期内。《数据安全法》第三十四条规定，法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。相关资质如《中华人民共和国测绘法》规定拥有测绘资质才能开展相应的测绘活动收集相关地理信息[15];《征信业务管理办法》规定依法取得中国人民银行个人征信机构许可，才可以从事个人征信业务[16]，金融机构不得与未取得合法征信业务资质的市场机构开展商业合作获取征信服务[17]等等。因此，数据提供方应当确保自身或数据上游方具备开展相关业务并获取相关数据的资质。

c. 保证数据来源合法合规

对于直接收集的数据，应当确保获得相关主体的同意。**通过授权使用的方式获得数据，**则应当确保数据提供方所获取的授权涵盖了将相关数据通过隐私计算技术处理，向结果使用方输出计算结果并用于特定目的。**通过采购获得的数据，**应当确保卖方获得相关数据的方式合法合规且有权交易，如要求其提供相关协议或授权文件等。**通过公开方式获取的数据，**若使用了爬虫等自动化手段，应当注意从数据类型、获取方式和使用目的等方面判断是否存在合规风险（参考本节下文“**（2）处理个人信息的要求**”“**a. 授权同意和告知**”中关于**公开收集**

15 《中华人民共和国测绘法》第五章。
16 《征信业务管理办法》第四条。
17 《征信业务管理办法》第五条。

的内容）。

（2）处理个人信息的要求

隐私计算技术应用于处理个人信息的场景，应当遵守《个人信息保护法》的专门规定。

a. 授权同意和告知

除了满足《个人信息保护法》第十三条规定的例外情形，数据提供方应当确认所提供的数据已经取得个人合法有效的同意，并依法履行了告知义务[18]。

对于**直接收集**个人信息的情形，授权途径通常为直接获得个人同意。因此，数据提供方应当判断其是否已经获得个人授权同意或单独同意、授权范围、以及是否已充分履行告知义务；符合法定例外情形的，还需判断是否符合无需获得同意和无需告知的情形。

对于**间接获取**个人信息的情形，获得授权的具体方式包括：

（1）个人直接授权数据提供方可以出于特定目的从第三方处获得相关个人信息，如信贷业务中为评估借款方的资信状况，借款方授权贷款方从司法、工商、征信等部门获取借款方的相关个人信息。这种情况下数据提供方要判断第三方获得的授权是否合法合规，以及自身从第三方获取相关个人信息是否符合授权涵盖的特定目的；

（2）数据提供方并未获得授权，而是第三方从个人获得授权，

[18] 取得个人同意和履行告知义务的具体要求，详见《个人信息保护法》第十四条至第十八条、第二十二条、第二十三条和第三十条。

即第三方有权收集相关个人信息并可以出于特定目的提供给其他方（即此处的数据提供方）使用，如信贷业务中贷款方为建立风控模型而向第三方采购外部数据，贷款方并未直接获得个人的授权，而是由第三方获得授权。这种情况下，应判断第三方所提供的数据是否在授权范围内且有权将该等数据对外提供和使用。

在间接获取的情况下，数据提供方也需要向数据流转的上游追溯并判断数据来源的合法性。数据经过多次授权的，应当关注每个授权环节的合法合规，判断授权链是否完整。

对于**公开收集**的个人信息，主要判断是否存在不当使用爬虫等自动化手段获得数据的情况。可从以下几个角度判断使用爬虫的合法性：

（1）**数据类型。**对于明确需要授权才可使用的个人信息，或由于数据本身的性质表明数据主体不愿随意流通公开的商业秘密、非开放数据等，通过爬取方式获得将构成未经授权收集的行为。

（2）**获取手段。**若数据主体设置访问控制、反爬取措施，或 Robots 协议中明确不允许第三方爬取数据，则突破、避开、绕开该等措施的爬取行为将被认定为未经授权的收集行为，或引发刑事风险。

（3）**使用目的。**即便爬取的数据类型和获取手段都合法合规，但如果将爬取的数据用于非正当合理的目的，如实质性替代被爬取方经营的部分产品或内容，妨碍对方正常经营、不合理增加运营成本、破坏网络系统的正常运行，非法出售或提供公民个人信息等等，则也会触发相应的法律责任。

自行产生的数据若不包含个人信息一般不涉及授权同意的要求。

b. 最小必要

根据《个人信息保护法》第六条第一款，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。因此，数据提供方应当结合隐私计算应用具体场景中的个人信息处理目的判断所使用的个人信息类型、体量是否符合最小必要原则，同时在符合最小必要原则的前提下尽量不影响处理目的的实现（尤其是可能影响个人权益的应用场景）。

2. 处理目的合规

数据提供方应当要求结果使用方确保其使用隐私计算处理后的计算结果所用于的目的合法正当。

3. 使用限制

数据提供方应当对技术提供方的数据处理行为进行监督，确保其按照约定及时删除或销毁相关数据，防止后续的数据滥用。

数据提供方可以要求结果使用方不能尝试逆推、还原或用其他手段获取数据提供方的原始数据信息。

4. 安全合规

（1）一般性要求

开展数据处理活动应当采取相应的技术措施和其他必要措施，保

障数据安全[19]；加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告[20]。

数据提供方向技术提供方采购隐私计算服务的，应当向技术提供方确认其所提供的隐私计算产品或服务符合相关网络产品和服务的国家标准的强制性要求[21]。

数据提供方应当确保技术提供方建立了适当的数据安全能力，落实必要的管理和技术措施，防止数据的泄露、损毁、丢失和篡改[22]。

（2）个人信息保护影响评估

根据前文所述，数据提供方与技术提供方之间可能被认定为委托处理个人信息，数据提供方与结果使用方之间可能被认定为向其他个人信息提供者提供个人信息，那么根据《个人信息保护法》第五十五条，数据提供方应当在提供数据前进行个人信息保护影响评估，评估内容应当包括：个人信息的处理目的、处理方式等是否合法、正当、必要；对个人权益的影响及安全风险；所采取的保护措施是否合法、有效并与风险程度相适应。个人信息保护影响评估报告和处理情况记录应当至少保存三年[23]。

（3）跨境传输合规

19 《数据安全法》第二十七条。
20 《数据安全法》第二十九条。
21 《网络安全法》第二十二条。
22 《信息安全技术 个人信息安全规范（GB/T 35273-2020）》第 9.1 条 b）项和第 11.5 条。
23 《个人信息保护法》第五十六条。

若隐私计算技术的处理过程涉及数据跨境传输，则应当遵守《数据出境安全评估办法》的相关规定，涉及个人信息出境的，还应当遵守《个人信息保护法》第三章“个人信息跨境提供的规则”。具体可参考《数据出境安全评估申报指南》《个人信息跨境处理活动认证技术规范 V2.0》《个人信息出境标准合同规定(征求意见稿)》等相关要求。

（4）涉及关键信息基础设施运营者采购隐私计算服务的要求

若数据提供方是关键信息基础设施运营者并且向技术提供方采购隐私计算产品或服务，则应当与技术提供方签订安全保密协议，明确安全和保密义务与责任[24]；若采购隐私计算技术产品或服务影响或者可能影响国家安全并落入网络安全审查的范围，还应当依照《网络安全审查办法》的规定依法进行申报。

5. 保障个人信息主体的权利

数据提供方将个人信息用于隐私计算主要涉及个人信息主体的知情权、决定权、限制或拒绝权，更正、补充权，以及删除权。

（1）知情权、决定权、限制或拒绝权

根据《个人信息保护法》第四十四条，个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。因此，这部分权利的保障主要体现在，对于将个人信息用于隐私计算的事宜，数据提供方应当得到授权

[24] 《网络安全法》第三十六条。

并充分履行告知义务。

（2） 更正、补充权

《个人信息保护法》第八条规定，处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。《个人信息保护法》第四十六条规定，个人发现其个人信息不准确或者不完整的，有权请求更正、补充。个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。因此，对于更正、补充个人信息的请求，数据提供方除了对其个人信息予以核实并及时更正、补充之外，还需要及时告知技术提供方和结果使用方同步配合进行更正、补充。

需要说明的是，《个人信息保护法》第八条对于个人信息质量的要求主要为了保护个人的相关权益，而在技术层面对数据质量的要求主要是为了保证模型的准确性和有效性，二者的侧重点略有不同。例如，自然人 A 向银行申请贷款，银行希望了解 A 的信贷状况，但却错误地输入自然人 B 的身份信息，通过风控模型计算最终输出了 B 的信贷状况，得出拒绝向 A 提供贷款的结论，侵害了 A 的个人权益，属于因违反《个人信息保护法》第八条而损害了个人权益。而在技术层面对数据质量的要求，如数据提供方对数据进行预处理，或通过校验规则等定位或排除无效数据等，主要是为了保证模型本身的准确性和有效性。在自然人 A 申请贷款的例子中，如果输入的身份信息是正确的，但因训练模型的数据不准确，导致银行使用的风控模型出现问题，进而对 A 的资信状况做出错误的判断，得出拒绝向 A 提供贷款的结论，损害了其个人权益，则属于没有符合技术层面对数据质量的要求而损害了个人权益。

（3） 删除权

若个人对用于隐私计算的个人信息请求删除的，数据提供方除应当依法删除或停止存储并采取安全保护措施之外[25]，还应当及时告知并同步要求技术提供方和结果使用方采取删除或相关措施。

(三) 技术提供方的合规要求

1. 数据源合规

技术提供方应当确认数据提供方提供的用于隐私计算的数据来源合法合规。

2. 安全合规

1) 一般性要求

开展数据处理活动应当采取相应的技术措施和其他必要措施，保障数据安全[26]；加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告[27]。

技术提供方应当确保其提供的隐私计算产品或服务符合相关网络产品和服务的国家标准的强制性要求[28]。

技术提供方向关键信息基础设施运营者提供隐私计算技术产品或服务的，应当配合签署保密协议[29]，并协助其履行关键信息基础设

[25] 《个人信息保护法》第四十七条。
[26] 《数据安全法》第二十七条。
[27] 《数据安全法》第二十九条。
[28] 《网络安全法》第二十二条。
[29] 《网络安全法》第三十六条。

施运营者的安全合规义务；涉及网络安全审查的，配合进行网络安全审查申报。

2) 处理个人信息的要求

在处理个人信息的应用场景下，若技术提供方与数据提供方或结果使用方构成委托处理的关系，则作为受托人，技术提供方应当依照《个人信息保护法》和有关法律、行政法规的规定建立适当的数据安全能力，采取和落实必要的管理和技术措施，保障所处理的个人信息的安全，并协助个人信息处理者履行《个人信息保护法》规定的义务[30]。

3. 存储合规

技术提供方不应当擅自存储相关数据，缓存数据在计算完毕后应当及时删除。在处理个人信息的场景下，除法律、行政法规另有规定外，技术提供方对其所处理的数据的保存期限应当为实现隐私计算处理目的所必要的最短时间[31]。

尽管从技术提供方的角色出发，其合规要点主要包含以上几点，但在实际应用场景中，采购隐私计算产品和服务的一方通常会要求将自身需要履行的合规义务通过隐私计算产品和服务中的功能来实现，这种情况下，技术提供方也应当适当关注数据提供方和结果使用方的相关合规要点，以更好地了解和完善隐私计算产品和服务的相关功能，协助数据提供方和结果使用方更好地提升合规性。

[30] 《信息安全技术 个人信息安全规范（GB/T 35273-2020）》第 9.1 条 b）项和第 11.5 条，《个人信息保护法》第五十九条。
[31] 《个人信息保护法》第十九条。

(四) 结果使用方的合规要求

1. 数据源合规

结果使用方首先应当确认数据提供方获得合法有效授权收集相关数据，且有权提供给结果使用方使用。结果使用方可要求数据提供方确保数据来源合法合规，如通过提供营业执照、资质证照、与数据上游方签署的相关协议条款等证明。若提供的数据包含个人信息的，则结果使用方应当注意确认数据提供方获得的授权涵盖了可将相关个人信息进行处理并提供给结果使用方，如要求提供相关隐私政策、通过系统、后台展示用户勾选同意授权留痕、与用户之间的授权文件或授权条款等。

结果使用方还应当确认自身有权引入相关数据并用于特定目的。在提供信贷产品和服务的场景中，获得用户授权引入外部数据方面比较容易实现，因为产品和服务本身会设置和用户直接交互的界面，并与用户签署相关贷款协议，如单独设置授权书或在贷款协议中设置相应的授权条款等，从而告知用户其可能会从第三方收集的个人信息类型和使用目的。但在一些通常不会直接触达用户的场景，如用于优化营销策略或风控模型，因用户无法直接对此有所感知，因此目前主要通过隐私政策的相关条款实现授权和告知。

具体而言，隐私计算本身并不是数据处理的目的，而是一种手段，因此在隐私政策中通常不会直接表明通过隐私计算技术处理数据，而是对具体的使用目的或场景进行相关描述，如用于营销、个性化展示、风险评估、优化产品和服务等等。此外，隐私计算技术本身较为复杂，在隐私政策中详细说明隐私计

算原理和复杂的数据交互过程并不现实，用户难以理解，也不符合监管对隐私政策的展示要求。因此，目前隐私政策中能涵盖隐私计算处理和使用个人信息的告知和授权条款通常还是用比较简洁的语言描述相关使用场景和数据类型。

2. 结果使用目的合规

1) 一般性要求

结果使用方应当保证其对隐私计算技术的计算结果数据的使用遵守法律、法规，尊重社会公德和伦理，遵循合法、正当、必要和诚信原则，遵守商业道德和职业道德，不得危害国家安全、公共利益，不得损害个人、组织的合法权益[32]。

2) 使用个人信息的要求

隐私计算处理个人信息后，输出结果若仍包含个人信息的，结果使用方应当确保其使用行为不属于非法收集、使用、加工、传输他人个人信息，不属于非法买卖、提供或者公开他人个人信息；不属于危害国家安全、公共利益的个人信息处理活动[33]。若对隐私计算技术计算结果数据的使用导致个人信息权益造成损害，结果使用方不能证明自己没有过错的，应当承担损害赔偿等侵权责任[34]。

3. 安全合规

1) 一般性要求

开展数据处理活动应当采取相应的技术措施和其他必要措施，保

[32] 《数据安全法》第八条。
[33] 《个人信息保护法》第十条。
[34] 《个人信息保护法》第六十九条第一款。

障数据安全[35]；加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告[36]。

结果使用方向技术提供方采购隐私计算服务的，应当确认隐私计算产品或服务符合相关网络产品和服务的国家标准的强制性要求[37]。

2) 处理个人信息的要求

结果使用方可以参考《信息安全技术 个人信息去标识化效果分级评估规范（征求意见稿）》对计算结果的数据进行去标识化程度评估，并根据去标识化程度确定相关计算结果的敏感程度，以及后续的处理和存储方式。对于评估后发现计算结果中存在未进行去标识化处理的个人信息或重标识风险较高的数据，宜进一步进行去标识化处理，并采取技术和管理方面的措施，将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理[38]。结果使用方不应尝试逆推、还原或用其他手段获取数据提供方的原始数据信息。

3) 涉及关键信息基础设施运营者采购隐私计算服务的要求

若结果使用方是关键信息基础设施运营者并且向技术提供方采购隐私计算产品或服务，则应当与技术提供方签订安全保密协议，明确安全和保密义务与责任[39]；若采购隐私计算技术产品或服务影响或

35 《数据安全法》第二十七条。
36 《数据安全法》第二十九条。
37 《网络安全法》第二十二条。
38 《信息安全技术 个人信息安全规范(GB/T35273-2020)》第 6.2 条。
39 《网络安全法》第三十六条。

者可能影响国家安全并落入网络安全审查的范围，还应当依照《网络安全审查办法》的规定依法进行申报。

4. 存储合规

若隐私计算输出的计算结果包含个人信息，则除法律、行政法规另有规定外，结果使用方对隐私计算技术处理结果数据的保存期限应当为实现处理目的所必要的最短时间[40]。隐私计算输出结果不包含个人信息的，结果使用方存储计算结果数据的期限应当符合与数据提供方之间的约定。

(五) 合规风险综合评估

由于不同企业应用隐私计算技术的场景和目的各不相同，隐私计算技术合规要求及法律风险需要具体问题具体分析。企业可结合自身的商业需求，参照上述列举的核心合规要点逐一评估相关风险，同时酌情考虑参与方既往的数据安全保障能力、技术能力测评结果等，对隐私计算技术应用的数据合规风险进行综合评估。与此同时，在我国数据保护相关立法及执法较为频繁的背景下，**企业还应当定期跟进立法和监管的最新要求，**以便及时更新隐私计算技术应用的风险评估工作，为企业商业可持续发展保驾护航。

[40] 《个人信息保护法》第十九条。

第五章

结语

作为一项新兴技术，隐私计算在发展壮大和落地应用的过程中，必然会经历从野蛮生长到趋于规范的过程。相应的，随着人们对隐私计算的认识和理解逐渐深入全面，国家的数据保护立法和监管不断细化完善，隐私计算技术本身及其应用持续创新发展，隐私计算技术的应用合规也会经历一个从模糊到清晰的过程。这一过程需要从理论与实践、技术与法律等多维度来探索实现。

(一) 正确认识原理与特点，减少合规价值误区

随着隐私计算技术的不断发展，在数据合规立法和监管活动趋严的背景下，越来越多的人开始关注这一新兴技术。但目前人们对于隐私计算的技术原理、特点和优势等的了解还不够深入，对于隐私计算技术应用在不同场景下能够实现的效果理解还不够准确，对于隐私计算技术能够发挥什么样的合规价值存在误解和疑问。对此，需要加强对隐私计算技术的宣贯，让市场更加准确深入地了解隐私计算技术及其优势，引导市场将隐私计算技术应用在最能发挥其合规价值的场景中，以达到事半功倍的效果。

(二) 加强领域间交流碰撞，促进技术法律适配

隐私计算技术的合规应用需要技术和法律两个领域不断交流碰撞。随着科学技术的不断发展，单纯的法律专业知识已经无法满足企业的合规需求，技术与法律的融合已经成为技术应用合规的必然趋势。一方面，隐私计算技术的技术从业人员需要尝试了解一些基本的数据合规法律知识以及立法和监管逻辑，理解法律法规最终希望保护哪些合法权益，并将其融入到技术应用和创新过程中；另一方面，法律相关从业人员也应当更深入地了解隐私计算技术的发展历史和技术原理，进而更准确地在个案中判断分析法律适用和法律关系，评估合规风险。只有在技术和法律之间架起桥梁，让技术了解法律，让法律更懂技术，才能推动隐私计算技术的合规应用和有序发展。

(三) 兼顾合规与业务发展，理性开展技术应用

尽管隐私计算目前无法解决个人信息的授权问题、匿名化问题，但其在实现最小必要原则和提升数据处理安全性、防止数据滥用方面的合规价值是毋庸置疑的，如果能够在充分认识隐私计算技术的技术特点和合规价值的基础上，有的放矢地进行落地应用，它的合规价值也将在应用的过程中被进一步放大。但需要明确的是，合规价值仅仅是隐私计算技术所拥有的价值中的一小部分。提升数据处理的安全性、减少数据滥用不仅仅是数据合规的要求，更是商业上的需求；合理有效的应用隐私计算技术是企业在数字经济中有更强的商业竞争力的表现，是协助企业在降低合规风险的前提下最大化对数据的开发利用

并为企业创造价值的一种手段。

站在更宏观的角度，隐私计算技术为数据流通提供了安全保障，降低了企业参与数据流通的顾虑，有利于解决了目前数据流通的痛点，从而推动数字经济的发展。只有充分认识到隐私计算技术在提升合规性、提升商业竞争力和促进数据流通方面的优势，才能够有效发挥它的价值。我们希望与业界携起手来，共同建设合规应用隐私计算的产业生态，共同促进隐私计算大规模落地实践与规范发展。