arXiv:2305.04061v1 [cs.CY] 6 May 2023

我们尚未达到目标：知识管理不足对组织合规的影响

Thomas S.erban von Davier；Konrad Kollnig；Reuben Binns；Max Van Kleek；Nigel Shadbolt 计算机科学系，牛津大学，英国牛津 联系方式：
thomas.von.davier@cs.ox.ac.uk

2023年1月

摘要

自《通用数据保护条例》于2018年生效以来，许多其他数据保护和隐私法规也相继出台。随着新法规的实施，专注于数据保护和隐私的行业专业人士也随之增加。本文基于相关研究——这些研究展示了知识管理在组织合规和隐私工程方面的潜在益处——介绍了一项针对数据保护官和其他隐私专业人员开展的探索性定性研究的研究发现。我们发现，知识管理方面的问题是参与者反馈中所反映的根本挑战。参与者提出了四类反馈：（1）认为法规与实践脱节；（2）普遍缺乏明确的职位描述；（3）数据保护和隐私需要在组织的各个层面得到重视；（4）知识管理工具虽已存在，却未得到有效使用。本文探讨哪些知识管理或自动化解决方案可能有助于建立更完善的计算机支持的工作环境。

1 引言

《通用数据保护条例》于 2018 年首次生效时，Sirur 等人曾就行业遵守新立法的能力发问："我们已经准备好了吗？"[36]他们发现，私营部门对于规模较大、资源充足的组织能否确保合规，顾虑有限；而对规模较小的组织，顾虑则更多。 [36]然而，近年来有关数据隐私和网络安全的法律迅速增多，涵盖《通用数据保护条例》、巴西《通用数据保护法》、加利福尼亚州《消费者隐私法》、计划中的欧盟《人工智能法案》，以及各种拟议中的网络危害立法。因此，科技行业必须跟踪并遵守

大量法律，这促使我们探究相关行业专家的经验。

组织在考虑隐私和数据保护时，往往会让工程师和设计师与律师及政策专家协作。然而，早在21世纪初的研究就表明，负责构建技术的团队并不认为隐私和数据保护是其首要关注事项和义务之一 [26, 6]。对此，研究人员提出了一系列基于价值的软件工程框架[37, 33, 39]。随着隐私和数据保护法律在组织内催生了新的角色，尤其是数据保护官（DPO）和其他隐私专业人员，我们有机会重新审视过去的一些讨论，尤其是结合探讨知识管理（KM）对合规行为益处的文献 [18, 9, 42, 22]。

组织内的数据保护官和隐私专业人员，是立法者制定的法规直接影响的主要群体。他们对于如何实施适用的隐私法律的看法，对于制定未来法规以及改善当前系统面临的挑战和不足，具有不可估量的价值。此外，他们所在的组织和外部各方通常认为，这些行业专业人员有责任确保法规合规。因此，本文旨在探讨知识管理在数据保护官这一角色中发挥什么作用，以及哪些方面仍有改进空间。在本研究中，我们聚焦于以下三个相关的研究问题：

RQ：（知识）数据隐私专家如何在组织内跨不同团队衔接多个知识库？**RQ：**（沟通）数据保护官如何维护并传达组织内部和外部作出的合规决策？**RQ：**（经验）数据保护官在努力确保合规的过程中，目前取得了哪些成功，又经历了哪些失败？

我们与行业内担任数据保护（DPOs）、网络安全或法律岗位的专家进行初步讨论后发现，他们往往在组织内承担审计员和批评者的角色。他们负责改进内部实践，以确保任何数据泄露或其他紧急情境都能得到有效处理，并符合法律规定的标准。他们还需要在内部决策违反相关法律时，偶尔对此提出反对。

最终，我们的访谈揭示了与知识管理及隐私专业人员角色相关的四类挑战。概括而言，这些挑战包括：(1) 人们认为企业的运作方式与法规的实施方式之间存在脱节；(2) 缺乏明确的职位描述；(3) 需要在组织的各个层面纳入并传达数据保护与隐私相关内容；(4) 知识管理工具虽普遍可用，却未得到有效利用。通过将我们的研究置于组织合规与

隐私工程相关态度的现有研究体系中，我们将呈现参与者的观点，揭示推进知识管理的必要性。随后，我们将探讨未来的计算机辅助知识管理工作如何通过进一步遵守隐私法规来改善我们的生活。

2 相关研究

有两个主要的研究领域为我们的研究提供了背景并构成了研究动机。第一个领域是关于组织遵守监管机构要求的现有研究。第二个领域是一系列采用既定方法探讨隐私工程态度的研究。

2.1 知识管理在组织合规中的作用

为应对创新，社会开始制定规则和法规，以尽可能降低潜在风险。数据保护和隐私的历史与技术创新的发展密切相关 [20]。随着技术能力不断提升、数据收集行为日益增多，对审慎且保护隐私的立法的需求也随之增加。这些法规通常包含详细的法律文档及相关标准清单，需要经过处理、理解和实施。此外，确保组织遵守这些法规是一项跨学科工作。

在许多方面，对合规和法规的需求并不是什么新鲜事。制药业和危险行业等特定领域几乎一直受到控制和法规监管 [24, 21, 31, 16]。自然，我们可以观察到，法规的严格程度与受监管领域所带来的危险之间存在一种非正式的相关性。同样，我们也能看到金融市场已有确凿的法规监管历史 [13, 2]。这些领域及相关论文展现了组织合规分析的历史。此外，这些领域还积累了大量关于知识管理对组织员工合规有效性的研究 [18, 9, 42]。研究发现表明，更有效的知识管理可能与合规行为的改善相关。通过对这些领域进行严谨的研究和审查，我们能够更好地理解法规的影响，并继续引导系统远离无效的解决方案。

关于组织合规的研究中，有相当一部分侧重于监管机构需要采取哪些措施，或应如何应对该领域的某些变化 [31, 13, 2, 16]。例如，一些监管理论认为，监管机构在开展监管工作时需要“真正做到响应”，将其所监管组织的行动、框架和态度纳入考量 [5]。尽管将值得关注的问题提请监管机构注意无疑具有重要价值，但对于组织可以采取哪些措施来改善其法规合规，往往缺乏充分分析 [21, 24]。这些分析通常强调

组织在兼顾合规与扩张、改进时所面临的挑战，以及这些决策所涉及的风险。一些文章更进一步，暗示遵守法规的决定相对随意，因而很容易被搁置 [10, 11]。其中一篇文章主张“争取监管机构的支持”，而不是首先努力理解法规的必要性。另一篇文章则强调，合规沦为被动的“清单式”活动所带来的危险。为解决合规可能变成逐项打勾式操作的问题，监管理论认为，通过组织与立法者之间的话语交流，合规与合法性可以成为一个更具互动性的过程，并因此成为更加有效的过程 [8, 28]。鉴于这些组织层面的研究，我们的研究旨在探讨组织内负责法规合规的专业人员所采取的具体行动，尤其是在数据保护和隐私方面。

数据保护与隐私领域已有一些与行业专业人士合作开展的研究，涉及能源公司员工、无人机操作员和制造商 [17, 12]。这些研究进一步证实了知识管理与合规行为之间的相关影响[22]。这些研究项目探讨了如何在各类员工执行个人合规任务时运用知识管理。我们的研究旨在探讨知识管理在特定数据监管和隐私专业人士群体中的作用。

2.2 价值导向的隐私工程

随着数据保护和隐私逐渐成为法规与法律讨论的议题，已有大量研究致力于改进设计与工程中的隐私考量。Lahlou 和 Langheinrich 的早期研究开启了对工程师如何看待自身在确保数据保护与隐私方面所扮演角色的探索 [26, 32]。需要说明的是，本文及后续研究中使用的“工程师”一词泛指参与构建系统的所有技术产品团队成员，例如设计师、系统工程师和需求工程师。这项早期工作促成了一系列设计与工程方法，至今仍在伦理计算领域引发讨论 [25, 37, 30]。然而，对这些框架的有效性和使用情况进行比较与分析，不属于本文的讨论范围。

这些框架已通过多种方法进行探索和检验，旨在了解行业专业人士在数据保护和隐私方面的态度与行为。我们回顾了其中一系列方法，以便将我们的方法置于这一研究体系的背景下。Shilton 在一个学术设计与研究团队中采用参与式观察法，探究哪些经历和互动有助于将伦理融入设计过程 [33]。他们将隐蔽式观察与后续访谈相结合，提供了引人入胜的见解。尽管如此，他们的参与者身处开放的学术环境，而我们关注的群体则是处理专有信息的行业专业人士。针对行业专业人士的一些研究，则通过审查专业讨论论坛上的匿名帖子开展，旨在调查人们的隐私实践，涉及 mo-

移动开发人员 [34]。挑战在于，与组织完善的 iOS 或 Android 论坛不同，科技行业中供我们开展研究使用的隐私专业人员论坛数量有限。

最终，近期一项结合调查数据与访谈数据的研究为我们提供了一种潜在的调查方法。为了更好地了解工程师面临的挑战，研究人员针对 Ubicomp 专业人士以及部分高级工程师开展了一项由两部分组成的研究 [38, 6]。这种混合方法有效揭示了许多工程师对隐私的态度，以及他们所感受到的责任。我们决定采用类似的方法，并进行了一些调整，以契合我们的具体研究兴趣。

在探讨针对行业专业人士的潜在研究方法时，我们受到启发，决定关注一个略有不同的群体。自《通用数据保护条例》于 2018 年生效以来，这一群体不断壮大。这些数据保护官属于以往研究所探讨的技术团队，但其角色正式与法规合规相关。同样，我们可以参考《通用数据保护条例》出台之初开展的研究 [36]。该研究在数据保护官设立之前采访了行业专业人士。研究发现虽持谨慎乐观态度，但指出总体而言，组织对法规合规要求感到安心；不过，不属于科技或安全行业的小型组织仍存在一些担忧 [36]。自 2018 年那篇论文发表以来，仍有必要进一步研究数据保护官在组织内部如何履行其角色。克罗地亚于 2021 年开展的一项调查发现，受访数据保护官中有 82% 表示，他们缺乏胜任该角色所需的教育、知识或培训 [29]。因此，我们的访谈研究旨在揭示有关组织数据保护与隐私态度和做法的具体讨论。

3 方法

本节概述了我们开展定性探索性研究的设计与执行细节。我们借鉴了 Spiekermann 等人和 Bednar 在相关研究中采用的方法，直接了解参与者的态度和想法 [38, 6, 36]。我们希望会见的主要利益相关者包括数据保护官、项目经理，以及任何参与数据法规合规工作的开发人员或法务团队成员。

3.1 招募

为了招募参与者，我们利用专业的在线社交网络，以便接触到在美国和英国各类组织内工作的行业专业人士。我们通过直接发送电子邮件、私信，以及在 LinkedIn 和 Twitter 上发布一则面向更广泛群体的招募公告来招募参与者。我们努力为参与者提供两种选择：一是通过在线方式进行实时讨论，二是通过在线表单填写访谈问题。

表1：本表列出了参与者的编号和性别、当前职位的简要描述，以及其主要运营地点。

编号（性别）	Role	地点	公司规模
P1（男）	数据保护官	USA	250-500
P2（男）	监管负责人	UK	1000+
P3（女）	法律与安全运营人员	UK	50-100
P4（男）	软件公司创始人	UK	50-100
P5（女）	数据保护官助理	EU	1000+
P6（男）	项目经理	USA	1000+
P7（未知）	法律与隐私专业人士	USA	250-500
P8（未知）	隐私副总裁	USA	1000+

我们从八位参与者那里获得了见解，这一人数是在此前研究的基础上增加的 [26, 6]。其中六位参与者接受了访谈，另外两位则通过表单填写了访谈问题。参与者涵盖了从职业生涯早期到高管层的各类数据保护与隐私专业人员（见表1）。他们所在的公司规模各异，从小型初创企业到大型国际组织。

3.2 流程

主要方法是由我们的一名研究人员与一位行业专业人士进行线上访谈。访谈旨在了解这些专业人士如何在其专业岗位上处理法规合规问题（附录 A）。通过半结构式访谈，我们可以提出后续问题，以便深入了解相关情况。第二种方法是在线表单，旨在作为参与本研究的两种方式中相对“轻量”的一种（附录 A）。其内容与访谈基本相同，但无法进行后续提问。此外，在线表单还为参与者提供了更高程度的匿名性。

我们与每位参与者进行了约 30–40 分钟的访谈。在线访谈使用 Microsoft Teams，使我们能够使用自动转录工具。这样便无需对参与者进行任何永久性音频或视频录制，从而确保其匿名性。此外，我们还进一步对访谈文字记录进行匿名化处理，删除所有涉及组织或参与者姓名的内容。我们为确保并维护匿名性所做的工作，是我们能够成功接触到各组织中担任重要职务人士的原因之一。第 6.2 节将探讨我们对匿名性的承诺为何对参与者至关重要。此外，我们坚持说明，我们对专有组织信息并不感兴趣，而是希望了解参与者自身的经历和心得。他们是负责处理内部和外部政策的专家，我们希望听取他们的见解。

3.3 数据分析

在收集参与者提供的信息后，我们开展了一项亲和聚类活动，与其他人机交互方法中的类似活动相仿 [19]。亲和聚类是指将访谈记录拆分成单独的想法或陈述，然后根据相似性对参与者的所有单条陈述进行分组。为每个群组加上标签，形成一个新的层级；随后反复将群组合并分组，直到形成一两个连贯的论点。大约在第六位参与者时，我们达到了较高程度的数据饱和。换句话说，我们开始多次听到相同的反馈和观点，这表明参与者有着共同的经历。

通过对访谈记录进行亲和聚类，我们得以识别出有关如何实践与监管机构保持合规这一主题的三个层次。此方法让我们能够将多位参与者的反馈归纳为一个观点，再与其他观点归为一组，形成更广泛的主题或讯息。综合审视所有主题后，我们得以总结出研究发现的整体论点。

4 研究发现

参与者对自身经历的反馈凸显了四大类挑战。在每个主要类别中，我们记录并整理了他们的想法，并指出知识管理的进步如何应对参与者的这些经历。

4.1 监管脱节

许多行业专业人士表示，他们觉得监管机构并不理解政策在实际实施中的做法。参与者表示，某些法规比其他法规更容易实施。例如，参与者指出，处理 Cookie 是他们工作中最棘手的方面之一。参与者表示，

> P3：法律写得非常好。但如果你在经营一家企业，该如何把这些文字付诸实践呢？我的意思是，这里面有很多模糊地带。Cookie 就是一个很好的例子。
>
> P4：我想举的一个例子是 Cookie……关于 Cookie 的情况，因为这有点混乱。相关规则并不完全明确，而且这些年来一直在变化。

另一方面，同一位参与者提到，建立恰当的隐私声明很容易，并说道：

> P3：隐私声明的数据处理非常直接。

这些选择展现了在实施数据隐私法规时存在的差异。隐私声明和 Cookie 管理是数字体验中的常见方面，但参与者坚持认为，两者的实施难易程度有所不同。尽管面对不同类型的法规时，人们多少感到有些沮丧，但大家仍相信，企业中的其他人有必要了解这些法规。我们接触到的专业人士认识到，持续践行一致的监管实践具有重要价值。

> P3：我认为，数据保护影响评估的关键在于让每个人都真正步入正轨。你知道，这不应该只是打个勾。我认为，在产品开发方面，所有人都需要真正理解数据影响评估。

数据保护影响评估（DPIA）是访谈中常被谈及的话题，因为对我们的参与者而言，它既是法规合规的重要组成部分，也是一项重要的工作职责。正如参与者所说，数据保护影响评估需要组织内多个团队参与，例如负责 Cookie 和隐私声明的团队。尽管如此，有些标准监管实践比其他实践更具挑战性。

不同监管实践所需投入的差异，又因不同国家和地区法律之间的细微差别而变得更加复杂。当前互联网法规面临的挑战在于，网络空间往往跨越国际边界。一位参与者说道：

> P4：我确实认为，传输影响相关事项有些繁琐，因为欧盟基本上是说，你必须自行判断外国法律的情况，而这很困难。举例来说，如果你想把数据发送到印度，就必须自行判断印度法律，这似乎有些荒谬，竟要成千上万乃至数百万人都这么做。

法律和法规因国家而异，这一难题对规模较小的公司尤其棘手，因为它们可能没有聘用国际法规专家。

> P3：我认为，在这些方面，尤其是对小型组织来说，还需要多一些帮助。

对小型企业的担忧反映了《通用数据保护条例》 [36] 开始时相关研究提出的早期担忧。鉴于反馈并未改变，小型组织可能存在一个尚未解决的重大问题，以及确保合规的问题。虽然政策从理论转化为实践时存在模糊之处和各种假设，但我们的参与者指出，他们愿意进一步与监管机构合作，以更好地确立这一从法律到实践的过程。同样，这也反映了先前的访谈研究，该研究发现政府实体对隐私和数据保护实践具有软实力和硬实力 [6]。我们的参与者解释了他们希望与政策制定者合作的原因。

> P2：所以我认为，与标准机构等这类机构互动，也是了解这一领域并帮助推动这些要求形成的方式之一。

隐私专业人员希望加深自身理解，并贡献经验，推动未来的变革。然而，对隐私专业人员来说，合作之路并非总是一帆风顺。一位参与者提到，由于公司只有法务团队负责与监管机构沟通，因此他们无法通过自己的职位直接与任何监管机构互动。相比之下，其他参与者指出，学者和政策制定者往往是他们工作中经常接触的对象。

> P2：在与一所大学合作开展这项工作期间，我们开始与议会委员会接触，回应各类询问和咨询。例如，《调查权法案》出台时，我们参与了相关讨论，就此提供了一些意见，还受邀接受英国内政部的访谈，帮助他们更好地了解可能存在的顾虑。

这些关于与政策制定者互动的不同观点，反映出参与者之间更深层的差异：他们如何界定自己的角色，以及如何在各自的组织中履行职责。

4.2 界定工作

访谈中的一项研究发现揭示了数据保护官或隐私专业人员这一角色具有极大的灵活性，也因此伴随着不确定性。尽管政府和法律力量决定了数据保护官工作的重点，但实际采用的方法、工具和职位描述仍由各个组织自行界定。参与者举出的一个例子涉及如何开展适当的审计。

> P2：对于预期采用的方法，目前缺乏明确说明。我们在不少案例中都看到过这种情况，比如纽约对招聘算法进行审计时就是如此。此类审计实际上并没有统一标准。

他们提到，不同地区的立法所规定的各类指南似乎过于宽泛，以至于每个人都只按自己认为合适的方式，或按其组织认为正确的方式进行审计。这一发现与隐私工程领域以往的研究相呼应；在那些研究中，一些工程师指出了“隐私运营化”的问题 [6]。这项研究强调，监管力量在组织之外确立了有关隐私的价值观和规则，但具体的实施方式和方法主要由员工决定。一位参与者表示，他们的策略是将数据保护和隐私方法与网络安全方法结合起来。这是解决如何正确开展数据审计这一不确定性的一种方法。

> P4：我们会进行内部审查和审计，同时也会与我们的安全团队协作。

此外，隐私专业人员在公司中的整体角色可能会因公司的地位和商业模式而大相径庭。参与者给出了两个截然不同的例子。

> P3：我记得有一次参加会议，会上围绕传输影响评估展开了热烈讨论。我的意思是，究竟需要做到什么程度？你知道，如果你是一家小型企业，要检查所有子流程的话，究竟要做到什么程度？从某种意义上说，这根本不可能。

这位参与者分享了这样一种看法：与资源更充足的大公司相比，在规模较小的公司中，隐私专业人员开展影响评估时，工作的深度和范围可能大不相同。

> P2：在我们的工作中，我们需要确保自己不会采取过于强硬的立场，例如反对某个重要客户的商业模式。

这里可以看到，大型上市公司的商业模式会如何影响隐私专业人员的角色，而这些人员正试图落实法规合规。从这两条反馈中，我们可以看出专业人员所拥有的自主权有所不同。在小型企业中，数据保护官或许能更大程度地主导数据保护与管理理念及政策的实施，但这也意味着资源有限，且所处理数据的整体安全性可能较低。另一方面，大型企业中的数据保护官或许不必过多担心安全和资源问题，但他们不过是庞大股东驱动的机器中的一颗齿轮。数据保护官或隐私专业人员在公司中的明确角色似乎具有灵活性，并在很大程度上由其任职组织以及同事在监管实践中承担的角色所界定。

4.3 我们都身处其中

所有受访参与者都表示，他们在组织内参与多个项目和各项举措。因此，确保数据保护和隐私方面的监管合规工作，需要在多个团队之间进行清晰的沟通。一位参与者描述了一种做法：

> P4：我的意思是，面对不同的受众，确实需要使用不同的语言和表达方式。

大多数参与者的主要受众包括开发团队、高管团队、法律团队和市场营销团队。一位参与者举例说明了面向开发团队时需要如何措辞：

> P3：我不会跑去跟开发人员说，哦，我需要这份数据影响评估。你知道，就是问他们：“你们进行数据处理的法律依据是什么

？”我的意思是，如果你想让他们给出正确的答复，就真的需要用他们的语言把事情讲得简单一些。

同样，高管通常也需要某种形式的简化。一位参与者将这类沟通描述为“非常易于消化的小知识点”。无论涉及哪个团队，数据保护官和隐私专业人员都会与整个组织互动。

由于这种互动几乎无处不在，数据保护官的政策实施成效也取决于组织内其他人的接受程度。在某些情况下，数据保护和隐私已成为公司文化的重要组成部分。

> P4：所以，我们有一套非常完善的内部数据保护政策。我们有正式政策，也会针对这项政策开展培训。每个人每年都必须参加一次相关测试。

然而，并非每个组织都能如此清晰地落实相关实践，或如此积极地接受这些要求。另一位参与者（P1）坦言，他们认为目前所在的组织并没有充分的内部数据治理政策，并表示必须先实施更多网络安全措施和数据访问限制。其访谈揭示了法规合规中一个此前未曾考虑的方面。假设数据结构没有得到充分保护，访问权限也未完全确立，那么这些数据就很容易受到威胁，默认情况下无法达到法规的高标准。因此，组织若要制定法规合规方面的内部政策，首先必须达到一定的安全基准。他们提到，自己不得不花一部分时间倡导公共政策，并强调法规合规的重要性。

无论组织是否已在内部政策中成功落实规则和法规，都需要进行信息传播和入职引导。即使我们目前拥有一套技术协作和数据存储工具，这仍然是一个挑战。

4.4 知识管理失当

每位参与者都表示，无论其从业年限或组织规模如何，知识管理都是一项难题。在此，有必要进一步探讨这些组织当前的知识管理状况。

> P4：我是说，我们确实有维基，也有很多文档，但问题是这些内容会过时。所以我们有一个庞大的 SharePoint 存储库，我们已经用了很多年了，具体多少年我也说不清，但大概有 20 年左右了。

知识管理工具（如内联网和维基）作为文档存储库以及与他人共享信息的方式，已经足够有效。尽管如此，在版本管理、更新和沟通方面仍然存在明显的挑战。特别是，我们的参与者（P1 和 P6）指出，维基内容很容易迅速过时。

目前参与者使用的工具仅实现了知识管理文献 [14, 4] 提出的功能中的三个基本部分（打包、存储和传输）。换句话说，目前的工具更像是信息库，却未能最大限度地促进相关任务的完成。

一种可能的解决方案是转向自动化，处理所有信息并执行数据保护官和隐私专业人员所需的职能。参与者告诉我们，自动化对他们而言仍是一片尚未探索的领域。虽然 OneTrust 等工具已经存在，但参与者表示，他们对此类工具的使用经验有限。真正吸引他们注意的是这类工具的自动化数据映射功能。参与者反复提到，自动化要么是他们工作中的一个目标，要么是一项挑战。

> P3：如果未来由我掌控，我可能会考虑某种自动化系统。我还不知道具体是什么，但主要是希望把一部分手动工作转为自动化。

> P7：我们的数据保护流程中没有使用自动化。

参与者表示，需要改进和扩展目前用于实现法规合规的工具。在一个日益意识到有必要监管快速变化的技术格局的世界里，数据保护官正努力确保每出台一项新法规，都不至于要求组织进行大规模调整。

4.5 研究发现总结：知识管理至关重要

从研究发现来看，四个重要类别都与有效的内部组织和信息处理这一理念息息相关。每位参与者也都表示，知识管理对于法规合规至关重要，但在实践中也是最具挑战性的环节。我们可以看到，每一类反馈都对应着 Despres 和 Chauvel 提出的知识管理分类体系所提供的一种解决方案 [14]。图 1 展示了 Despres 和 Chauvel 所定义的知识管理工具的特征，这些工具可能适用于数据保护官。上方的水平轴显示工具可以发挥的功能，垂直轴则标示实施层级。在第一类反馈中，我们了解到法规与实践之间存在脱节；能够映射并收集组织实现合规所需的全部数据和政策的工具，或许可以解决这一问题（见图 1 左上方）。

第二类反馈揭示了参与者如何看待雇主对其角色的界定较为模糊，尤其是在如何满足政策制定者期望方面。一些参与者表示，处理监管合规需求的内部流程应当立足于组织的工作流程核心，并确保易于获取。在讨论 Bednar 等人的论文时，作者将实践中实现隐私工程所面临的挑战划分为工程师的“负担”、“内心冲突”以及“与律师的斗争” [6]。对参与者的访谈表明，更完善的知识管理工具将使他们能够。

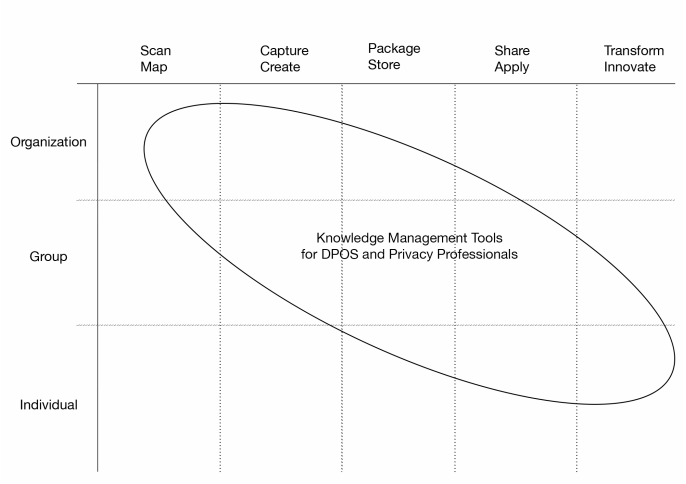

图 1：受 Despress 和 Chauvel 绘制的知识管理实践领域图启发，本图展示了能够回应参与者反馈的知识管理工具所覆盖的领域 [14]。

面临这些挑战。例如，相关文献指出，工程师经常会遇到一种冲突：既需要确保隐私实践得到落实，又需要满足并兼顾雇主的商业模式[38]。一种能够为各个群体或团队打包整理信息的工具，或许能够缓解参与者所表达的这种矛盾（见图 1 中间部分）。

除了界定角色和职责这一挑战外，参与者使用的知识管理系统还需要在多学科团队之间处理和传递信息。报告中一些最显著的挑战是，如何针对不同受众调整隐私和法规合规方面的表述。再一次，这与相关文献中的类似研究发现相呼应：工程师与法律团队之间的沟通并不顺畅[26, 6]。根据以往文献和参与者的讨论，在第三类反馈中，我们认为数据保护和隐私本质上具有协作性。因此，在这一领域使用的任何知识管理工具，都必须能够有效地分享和应用法规，以满足不同团队各自的需求（见图 1 右下角）。

我们的参与者及其同行必须倡导并制定内部政策，使企业能够遵守法规。他们指出，建立与组织流程直接衔接的内部数据保护与隐私政策，将为工程师、高管和法律人员提供统一的参考来源。在我们的讨论中，我们将重点阐述知识管理文献如何主张将这一参考来源融入组织固有的各项任务和职责之中。

5 局限性

本文采用了基于访谈的研究，因此这类研究通常存在的局限性也同样适用。

我们认识到，要针对不同司法管辖区和立法（美国、英国和欧盟）的合规行为得出结论颇具挑战性。然而，需要注意的是，无论参与者最初的背景或培训如何，他们始终都需要在所有这些司法管辖区开展工作。他们所在的组织在全球范围内运营，但通常只有一名正式的数据保护官。

6 讨论

本文所呈现的探索性研究揭示了行业专业人士的亲身经历和态度。他们的陈述有助于学者和开发者构建未来的工具，从而有效应对所凸显的问题。此外，反思文中所呈现的内容，或许能为政策制定者提供一些问题，以促成关于改进数据保护和隐私立法的必要讨论。

6.1 数据保护官知识管理的未来

关于知识管理的挑战，问题在于问题框定和术语。目前对“知识管理”的理解主要描述的是归档和共享工具，这些工具允许用户存放、组织信息，并偶尔对其进行呈现。然而，我们认为，这并未满足该描述中的“管理”部分。二十多年前，一种早期的知识管理分类体系就概述了实现恰当知识管理所必需的其他任务[14]。我们当前使用的工具不会替我们对信息进行优先级排序；它们不会突出显示哪些内容已经过时，甚至可能已无法使用。工具缺乏实际管理功能，导致其潜在可用性不足。这偏离了计算技术改善人类生活的最初目标。

为了进一步直观地理解知识管理，可以用物理世界中的一个类比来说明：目前市场上被宣传为知识管理项目的工具，更像是一座银行金库。我们可以将信息放入其中，并按自己的意愿进行组织；但信息一旦存入其中，而我们离开金库后，在我们再次返回之前，它就会保持原样。我们所期望的知识管理工具，则更像是资产管理者。将与存入金库时相同的资产交由资产管理者保管，提供一些规范，然后让系统以一种很可能在用户返回时使其受益的方式来管理这些资产。

从保险库转向资产管理者，往往需要人类介入，并借助他们能够提供的特定服务，以补充实体存储空间所提供的基本安全保障。早期的知识管理工作也需要代理和人类参与，之后现代软件工具才得以发展。

完全接管了该领域 [40, 27, 15, 7]。然而，在计算方面，我们正处于一个转折点，即将面临类似的跃迁：从大型、相对静态的数据存储库，迈向一个全新的未来。在这个未来，数据的潜在用途不再是存储，而是让数据流通起来，为我们所用。让计算来处理这些新的数据处理任务。

根据我们从参与者那里了解到的信息，我们呼吁进一步开发知识管理工具，以弥补这些工具缺乏“创新杠杆”的问题 [14]。这并非知识管理领域的新议题，但迄今为止我们构建的技术工具主要关注数据存储与共享。即使是近期关于知识管理新能力的研究，也侧重于存储方面 [35, 41, 1]。云存储或许能进一步缓解各类组织面临的挑战，但显然，我们需要灵活响应的自动化知识管理。

要涵盖知识管理可能涉及的全部分类体系，从知识映射到创新与转型，就需要我们的工具承担以往未曾探索过的角色。尽管新型知识管理系统的可能性令人期待，我们仍需考虑自动化对法规合规的影响。若仅仅将合规的作用和必要性简化为自动勾选清单，就毫无价值 [3]。不过，将自动化与参与者的工作相结合，作为计算机支持的工作，或许能缓解我们和文献中观察到的挑战，同时满足政策制定者设定的标准 [23]。这需要采取审慎的以人为中心的设计方法，充分考虑系统中所有利益相关者的需求。因此，我们建议未来开发知识管理软件，使其真正超越具备共享功能的数据存储库。

6.2 对数据保护官角色的思考

合规、网络安全、法律和数据在全球各地的组织中交织呈现，形成了一张精细而常常错综复杂的网络。要确保我们能够满足各领域可接受的要求，需要进行周密规划、开展有效沟通，并对信息进行良好组织。如今，数据隐私与保护领域的行业专业人士正处于这一日益严峻挑战的前沿。

在本书中，我们采访了多位此类行业专家，以了解他们如何平衡公司要求与法律要求。他们表示，尽管有些方面运作良好，但当前软件管理知识的方式也存在明显问题，尤其是在应对这一全新且日益严峻的法规合规挑战方面。

我们的研究发现，目前的知识管理工具主要发挥着文档存储库和共享工具的作用。然而，参与者指出，通过自动化，可以大幅拓展现有工具的功能及其作为数据保护专业人员的能力。这一发现为未来的研究开辟了方向，即探讨如何设计知识管理软件，使其能够更好地满足 Despres 和 Chauvel [14] 提出的完整分类体系。超越文档存储与共享这一主要职能，实现完整的计算机支持的工作，将对这一行业及其他领域产生深远影响。

虽然本文的大部分工作聚焦于将知识管理应用于数据保护与隐私方面的挑战，但研究发现揭示了整个行业面临的严峻挑战。多学科团队需要有效沟通隐私如何影响组织的各个层面。此外，了解正在管理哪些信息和数据，对于制定适当的安全与保障措施至关重要。最后，我们在探索性研究的招募和访谈安排过程中发现了一个明显的挑战。对于少数愿意与我们会面的数据保护官和隐私专业人员，我们必须准确说明为参与者的信息进行匿名化和保护所采取的步骤。这种谨慎究竟源于他们作为数据保护专家的专业知识，还是出于保护其组织实践的需要，目前尚不清楚。尽管如此，接触这一行业专业人士群体颇具挑战，也可能给未来推动政策制定者与专业人士建立联系、促进立法变革的尝试带来问题。

7 结论

接受并采用数据保护和隐私方法仍然具有挑战性。参与者提到，他们日常工作的一部分是努力说服并推动组织内部重视数据保护和隐私。此类说服尝试通常是面向各级高管和经理所作的正式演讲。部分参与者强调，机构施加压力以推动采用合规软件十分重要，这与此前的研究相似 [3]。为了实现数据保护和隐私合规，未来需要开展研究，探索推动企业和机构接受这些方法的有效途径。

归根结底，本研究旨在向行业专业人士和立法者提供范例和证据，展示组织内部为推广和落实数据隐私实践所开展的工作。协作和审慎的知识管理对于探索该领域的解决方案至关重要。随着未来法规的起草，对合作探索的需求很可能会增加。

致谢

本研究通过 RETCON 资助项目获得英国研究与创新署（UKRI）在 PETRAS2（EP/S035362/1）计划下的支持。我们谨向抽出时间与我们交谈并填写在线问卷的参与者表示感谢。他们从繁忙的日程中抽出时间分享见解，使我们得以找到研究问题的答案。我们也要感谢 HCAI 团队的其他成员，以及在整个过程中给予我们的所有支持。

参考文献

[1] Naresh K Agarwal 和 Laila N Marouf。《在学院和大学启动知识管理：一个模板》。载于：*Marouf*国际知识内容开发与技术期刊 4.2（2014），第67页。 DOI：10.5865/IJKCT.2014.4.2.067。 URL：http://dx.doi.org/10.5865/IJKCT.2014.4.2.067。[2] Sharmista Appaya 等。《监管机构如何应对金融科技：评估不同方法——沙盒及其他举措》。技术报告。世界银行集团，2020年。[3] Petra M. Asprion 和 Gerhard F. Knolmayer。《高度监管行业中合规软件的采用：一项实证多理论调查》。载于：夏威夷国际系统科学年会论文集 （2013），第4405–4414页。 ISSN：15301605。 DOI：10.1109/HICSS.2013.107。[4] Gabriela Avram。《知识管理与社交软件的十字路口》。载于：《知识管理电子期刊》4.1（2006），第1–10页。 URL：www.shortcut.nu。[5] Robert Baldwin 和 Julia Black。《真正回应式的法规监管》。载于：《现代法律评论》71.1（2008），第59–94页。[6] Kathrin Bednar、Sarah Spiekermann 和 Marc Langheinrich。《隐私设计工程：工程师准备好迎接挑战了吗？》载于：《信息社会》35.3（2019年5月），第122–142页。 ISSN：10876537。DOI：10.1080/01972243.2019.1583296。[7] F O Bjørnson 和 T Dingsøyr。《软件工程中的知识管理：对已研究概念和所用研究方法的系统综述。信息与软件技术》。载于：《信息与软件技术》50.11（2008），第1055–1168页。 DOI：10.1016/j.infsof.2008.03.006。 URL：https://www.sciencedirect.com/science/article/abs/pii/S0950584908000487。[8] Julia Black。《监管对话》。载于：《法律与社会杂志》29.1（2002年3月），第163–196页。 ISSN：0263-323X。[9] Guido Boella 等。《法规合规中的法律解释管理——时间与论证／可废止逻辑视角；电子商务项目；法规合规中的法律解释管理》。载于：（2013）。 DOI：10.1145/2514601.2514605。 URL：http://www.activiti.org/。[10] Sarah Cannon 和 Lawrence H Summers。《优步和共享经济如何赢得监管机构的青睐》。载于：《哈佛商业评论》（2014）。 URL：
h
t
t
p
s://
h
b
r.
org/2014/10/how-uber-and-the-sharing-economy-can-win-over-regulators/。[11] Hui Chen 和 Eugene Soltes。《合规计划为何失败，以及如何修正》。载于：《哈佛商业评论》（2018）。

[12] Roger Clarke。《民用无人机对行为隐私的影响之法规》。载于：《计算机法与安全评论》30（2014），第 286–305 页。DOI：10.1016/j.clsr.2014.03.005。URL：http://dx.doi.org/10.1016/j.clsr.2014.03.005。[13] Andrew Crockett。评论：金融市场监管机构应如何应对全球经济一体化带来的新挑战？技术报告。经济政策研讨会会议录，2000 年，第 121–128 页。[14] Charles Despres 和 Daniele Chauvel。“知识管理（S）”。载于：《知识管理杂志》3.2（1999），第 110–120 页。[15] Torgeir Dingsøyr。“软件工程中知识管理应用案例研究综述。Agile 2.0 项目观点 TeamIT 项目观点”。载于：《国际软件工程与知识工程杂志》上的文章（2002）。DOI：10.1142/S0218194002000962。URL：https://www.researchgate.net/publication/220344742。[16] Jonathan Drimmer。“人权与采掘业：诉讼与合规趋势”。载于：《世界能源法与商业杂志》上的文章3.2（2010），第 121–139 页。DOI：10.1093/jwelb/jwq001。URL：https://academic.oup.com/jwelb/article-abstract/3/2/121/ 947392。[17] Rachel L Finn 和 David Wright。“民用无人机实践中的隐私、数据保护与伦理：对行业、监管机构和民间社会组织的调查”。载于：《计算机法与安全评论》32（2016），第 577–586 页。DOI：10.1016/j.clsr.2016.05.010。URL：http://dx.doi.org/10. 1016/j.clsr.2016.05.010。[18] Leif Jarle Gressg°ård。“高风险分布式组织系统中的知识管理与安全合规”。载于：《工作安全与健康》5.2（2014），第 53–59 页。ISSN：20937997。DOI：10 . 1016 /J . SHAW . 2014.03.002。[19] Karen Holtzblatt。“情境设计”。载于：《人机交互手册》第 2 版。2007 年，第 942–963 页。[20] Jan Holvast。“隐私史”。载于：《信息安全史：综合手册》。Karl de Leeuw 和 Jan Bergstra 编。2007 年。[21] Andrew Hopkins。“风险管理与规则合规：危险行业中的决策”。载于：《安全科学》49（2011），第 110–120 页。DOI：10.1016/j.ssci.2010.07.014。URL：https://www.researchgate.net/ publication/251615087。[22] Sang Soo Kim 和 Yong Jin Kim。“合规知识与合规支持系统对信息安全合规行为的影响；组织文化研究项目观点 元宇宙项目观点；合规知识与合规支持系统对信息安全合规行为的影响”。载于：期刊文章

《知识管理杂志》（2017）。 DOI：10.1108/JKM- 08- 2016- 0353。URL：https://www.researchgate.net/publication/316099703。[23] John Kingsto。“运用人工智能支持遵守通用数据保护条例”。载于：《人工智能与法律》25（2017），第429–443页。[24] Rony Kubat。“在高度监管行业中平衡合规与持续改进”。载于：《质量杂志》（2019），第48–48页。[25] Saadi Lahlou 和 Fran¸cois Jegou。“ 欧洲消失计算机隐私设计指南，版本 1.1。Ambient Agora-s IST 2000-25134，版本1.1。Ambient Agoras”。载于：Ambient Agoras（2004）。[26] Marc Langheinrich 和 Saadi Lahlou。“D15.3.1——隐私 Troubadour 方法 WP15-隐私”。载于：D15.2.1——隐私专项报告，第1部分（2002）。[27] Maria M¨artensson。“对知识管理作为管理工具的批判性综述”。载于：《知识管理杂志》4（2000），第3–204页。DOI：10.1108/13673270010350002。 URL：http://dx.doi.org/10.1108/13673270010350002。[28] Wendy Mason Burdon 和 Mohamed Karim Sorour。“制度理论与‘合法’合规文化的演变：英国金融服务业案例”。载于：《商业伦理杂志》162（2020），第47–80页。 DOI：10.1007/s10551-018-3981-4。 URL：https://doi.org/10.1007/s10551-018-3981-4。[29] Anamarija Mladini´c、Livia Puljak 和 Zvonimir Koporc。“《通用数据保护条例》实施后对克罗地亚研究机构和非研究机构数据保护官的调查：一项横断面研究”。载于：Biochemia Medica 31.3（2021年10月）。ISSN：13300962。 DOI：10.11613/BM.2021.030703。[30] Helen Nissenbaum。《情境中的隐私：技术、政策与社会生活的完整性》。斯坦福：斯坦福大学出版社，2010年。 URL：http : / / www . nyu . edu / projects / nissenbaum / index . htmlhttp : / / www.sup.org/book.cgi?id =8862..[31] Marisa Papaluca 等。“把关者与推动者：药品监管机构如何通过采取积极主动的态度应对充满挑战且不断变化的环境”。载于：Clinical Pharmacology & Theraputics（2013），第1–8页。 DOI：10.1038/clpt.2013.14。 URL：www.nature.com/cpt。[32] 作者：Saadi Lahlou、Marc Langheinrich 和 Carsten R¨ocker。“隐形计算机的隐私与信任问题”。载于：《美国计算机协会通讯》48.3（2005年3月），第59–60页。 URL：www.junkbusters.com/fip.html。[33] Katie Shilton。“价值杠杆：将伦理融入设计”。载于：《科学、技术与人类价值》38.3（2013年5月），第374–397页。 ISSN：1552825

1.

DOI: 10.1177/0162243912436985.

[34] Katie Shilton 和 Daniel Greene。《连接平台、实践与开发者伦理：移动应用开发中的隐私话语杠杆》。载于：商业伦理学杂志（2017）。 ISSN: 0167-4544。 DOI: 10.1007/s10551- 017-3504-8。[35] Ahmad Shukri 等人。《高等教育机构中基于云的知识管理综述》。载于：*International Journal of Electrical andComputer Engineering (IJECE)* 9.6（2019），第 5420–5427 页。 ISSN: 2088- 8708。 DOI: 10.11591/ijece.v9i6.pp5420-5427。[36] Sean Sirur、Jason R.C. Nurse 和 Helena Webb。《我们准备好了吗？了解遵守《通用数据保护条例》（GDPR）所面临的挑战》。载于：*ACM*计算机与通信安全会议论文集（2018 年 10 月），第 88–95 页。 ISSN: 15437221。 DOI: 10.1145/3267357.3267368。[37] Sarah Spiekermann 和 Lorrie Faith Cranor。《隐私工程》。载于：*IEEE*软件工程汇刊35.1（2009），第 67–82 页。 ISSN: 00985589。 DOI: 10.1109/TSE.2008.88。[38] Sarah Spiekermann、Jana Korunovska 和 Marc Langheinrich。《组织内部：为何隐私与安全工程对工程师而言是一项挑战》。载于：*IEEE*会刊107.3（2019 年 3 月），第 600– 615 页。 ISSN: 15582256。 DOI: 10.1109/JPROC.2018.2866769。[39] Sarah Spiekermann 和 Till Winkler。《面向设计伦理的价值导向工程》。载于：*IEEE Transactions* （2020）。[40] Peter Tyndale。《知识管理软件工具分类：起源与应用》。载于：*Evolution and Program Planning* 25（2002），第 183–190 页。 URL: www.elsevier.com/locate/evalprogplan。[41] Chaoshi Wang、Chun Zhao 和 Lin Zhang。《云环境中海量知识管理框架》。载于：论文集——*2014*年第七届生物医学工程与信息学国际会议（*BMEI 2014*）（2014），第 843–847 页。 DOI: 10.1109/BMEI.2014.7002889。[42] Kamphol Wipawayangkool。《国际多元化中的信息安全合规与知识管理能力》。载于：604（2009）。 URL: http://aisel.aisnet.org/amcis2009/604。

附录 A

A.1 访谈提纲

引言 感谢您今天抽出时间接受我的采访。我们今天的谈话与组织为遵守数据监管法规而开展的记录保存工作有关。您可以在此次访谈前发送的电子邮件中查看项目概要。您是否了解本项目的宗旨和目标？感谢您的关注。提醒一下，本次访谈旨在更好地了解您使用的工具类型。

您日常工作中的情况，以及它们在哪些方面带来价值或造成挑战。我们不会询问您本人或您所在组织的任何个人信息。您可以随时结束本次访谈，也可以根据需要随时要求休息。

您是否有机会阅读并填写知情同意书?

- “是”——太好了，谢谢。继续之前，您有什么问题吗?

- “没有”——请现在花些时间仔细阅读并填写。如果您对其中任何内容有异议或有疑问，请告诉我。如果该文件中的任何内容让您不想继续参加此次访谈，您可以退出。

开始之前，再说明一项数据保护事项：提醒您，从现在到 01/06/22 期间，您可以出于任何原因，在无需说明理由的情况下，要求我们删除您今天提供给我们的数据。如果您对此没有异议，我们就可以开始提问了。

问题——请根据受访者选择合适的问题组介绍/背景

1. 您会如何描述自己在所属组织中的角色?
2. 您如何按规模对贵组织进行分类?
    - 大型企业
    - 成熟企业
    - 小型企业
    - 初创企业
3. 您通常同时参与多少个项目?
4. 您通常会与多少个团队对接?
5. 您能否简要介绍一下这些群组及其角色?

知识管理

1. 您能否介绍一下您的组织用于管理内部知识的工具：

    - 您的组织在内部使用哪些工具来跟踪其大部分知识?

    - 用于管理文档和文件的工具？用于沟通和协作的工具?
    - 项目管理工具？（例如 Asana、Jira、Twilio）？– 如果使用，每周花多少时间在软件中添加和编辑任务?

– 总体而言，使用项目管理软件是有帮助还是有害?

- 还有其他您尚未提及、用于知识管理的工具吗？它们有什么用途?

2. 您觉得自己需要多久整合一次文档，或向他人指出“单一事实来源”?

- 您是否有一个可以信赖的“单一事实来源”?
- 在涉及法律合规或政府法规时，是否需要有一个“单一事实来源”?

组织内部的数据保护

1. 请描述数据保护合规法规的合规要求在您当前职位或角色中发挥什么作用。您是否负责组织数据保护合规的某些方面?

2. 贵组织是否有任何用于跟踪与数据保护合规相关的问题、决策和资源的专用工具?

- 如果是这样，使用了哪些工具，以及如何使用?
- 如果没有，这些问题和决策是如何形成的，又是如何保存和整理的?
- 谁负责维护它们?

3. 您上文描述的系统有哪些优点?

- 想一想你喜欢或经常使用哪些功能.....

4. 上述系统有哪些难点?

- 什么事情会让您感到沮丧？什么因素会拖慢您的工作流程?

5. 您如何在项目管理软件中组织数据保护计划?

- 数据保护（或DPIA文档）是作为独立项目存在，还是对应多个项目?

6. 合规文档和记录的共享方式是怎样的?

- 这些系统在哪些方面能提供帮助，又会在哪些方面造成问题?
- 从贵组织向外部共享信息时，是否还会遇到其他挑战?

7. 与法律顾问或管理机构合作时，您需要如何以不同方式处理相关事项?

8. 贵组织是否有用于数据保护和访问控制的集中式或全球化软件或平台?

- 如果您不知道或没有这类软件或平台，如何跟踪自己可以和不可以访问哪些文件?
- 贵公司是否有专门负责管理权限的团队？您多久与他们互动一次?

9. 您是否清楚了解谁可以访问哪些数据的规则?

    - 对你个人而言?
    - 对于组织中的其他人呢?

10. 您每周需要申请授予访问权限的频率是多少?

数据保护——来自数据保护官的视角（取决于受访者）

1. 您如何开展数据保护审计?
2. 您认为大多数组织在数据保护方面会遇到哪些问题?
3. 您如何支持或与多个组织合作?
4. 您能否详细介绍一下，针对以下事项所需的各种文件，您是如何处理的?

    - 第30条数据处理活动记录
    - 隐私声明
    - 同意
    - 访问请求
    - 数据保护影响评估
    - 合法利益评估
    - 个人数据泄露
    - 《2018年数据保护法》-特殊类别或刑事定罪及犯罪数据

5. 《通用数据保护条例》要求制定的隐私政策文档中，哪一份最难管理或处理？6. 您希望未来 5 年内，数据保护政策和执法方面有哪些变化？7. 如果您有一根魔法棒，您会如何改变或调整确保数据保护的方式?

项目管理（视受访者而定）
如果不是项目管理办公室或组织角色：“您是否与项目经理/项目管理办公室合作？”

1. 所有项目是否都指定了项目经理?
    - 什么样的项目需要指派项目经理?
    - 就您个人而言，您认为项目经理会增加还是减少工作量?

如果是项目管理办公室/组织角色:

1. 您是否负责为团队使用的数据分配权限?
    - 如果是，您会在哪里寻求有关授予权限的指导?
    - 如果不是，您所在组织中负责数据访问角色的把关人是谁?
2. 您是否有一个集中式系统，用于存放项目文件及其中可能包含的数据?
    - 在您访问数据之前，是否需要依赖其他团队?
    - 使用后，您会将数据存储起来以便在其他项目中重复使用吗？如果会，是如何存储的?
3. 您通常使用什么方式与这些团队沟通?

总结/访谈回顾 感谢您抽出时间回答我们的问题，我们对此深表感谢。这些问题旨在帮助我们更深入地了解目前存在的工具生态系统和文档管理器。我们希望了解不同规模的团队和组织之间，记录保存文化有何不同。我们将确保笔记和最终论文草稿中不会收集任何姓名或个人身份信息。不过，如果您有任何问题或疑虑，可以直接通过 **为保证匿名性，邮箱已隐去** 联系我们中的一位。知情同意书中也提供了研究伦理委员会的联系信息；如果您有任何事情想在不让我知情的情况下与他们讨论，可以通过该信息联系他们。