《论证符合性》与数据保护原则的一致性论证

Chris Smith计算机科学系，约克大学

Richard Hawkins计算机科学系，约克大学

摘要—**我们展示了组织如何使用符合性论证来证实其符合数据保护原则的主张。使用符合性论证能够提高这些组织、监管机构、认证机构和数据主体评估这些主张真实性时所采用方法的严谨性和一致性。**

关键词： 数据保护、隐私保护、法律、监管、问责、保证、符合性论证

■ 数据保护原则 定义

“个人信息收集、保留、使用和披露的规范” [1]。此类原则是用于规范个人数据处理的法律和自律政策工具的基础。受这些政策工具约束的组织在处理个人数据时，主张其处理活动符合每项原则。组织可以明确提出主张。例如，组织可以在其网站发布的隐私信息中提出主张。也可以仅根据组织处理个人数据这一事实、该组织所在的司法管辖区，以及该组织因此受其约束的政策工具，推断出其主张。

处理个人数据的组织、监管机构、认证机构和数据主体都可能评估其对数据保护原则的符合性声明。要对符合性进行有意义的评估，必须以充分的论证和证据为主张提供支持，使其真实性能够得到有把握的判定。论证和证据不足，会导致评估结果为不符合性（因不确定性所致），或者得出缺乏严谨性和可信度的符合性评估结果。然而，目前可供组织参考的指导文件有限，未能说明其论证和证据的内容、结构与呈现方式。组织可能

因此构建出不足以支持有意义的符合性评估的论证和证据。此外，组织内部以及不同组织之间，论证和证据的内容、结构与呈现方式可能存在显著差异，从而增加符合性评估流程的复杂性和成本，并可能导致结果不一致。

符合安全标准对安全关键系统至关重要，[2] 因为偏离预期行为可能会对个人造成人身伤害。此前已有研究提出，组织可以通过符合性论证来证实其符合安全标准的主张[3]。符合性论证是结构严谨、全面且站得住脚的论证，用于阐明组织对标准的解释。符合性论证以证据为支撑，这些证据足以表明软件流程或工件充分满足标准要求。

在本文中，我们展示了组织如何利用符合性论证来证明其符合数据保护原则的符合性声明；从而提高组织、监管机构、认证机构和数据主体评估符合性时的严谨性与一致性。在整个系统生命周期中，符合性论证都可能对组织发挥关键作用。在部署之前，符合性论证可用于为设计、实施和部署决策提供信息，支持与数据主体的沟通，并为内部和外部评估流程提供依据。在部署之后，符合性论证可用于更好地理解系统变更可能如何导致不符合数据保护原则。此外，如果组织被提出不符合性主张，符合性论证可用于为其决策进行辩护。

数据保护

我们将数据保护视为与个人数据处理相关的隐私。在此上下文中，隐私侵犯源于不符合个人与社会期望的个人数据处理。隐私侵犯可能对个人、组织、群体和社会造成不同类型的伤害 [4] 例如，个人可能因以侵犯其隐私的方式处理其个人数据而遭受声誉损害。例如，组织可能因处理侵犯相关个人隐私的个人数据而被处以罚款，从而遭受经济损失。例如，社会可能因缺乏信任，进而导致其隐私曾遭侵犯的个人不再参与公共系统（如医疗卫生），从而遭受经济损害。因此，个人数据处理可能带来的任何益处，都必须与隐私侵犯可能造成的伤害进行权衡。

隐私已被认可为一种需要保护的个人 [5] 和社会 [6] 价值。处理个人数据且可能侵犯隐私的系统日益普及，因此国家和国际层面制定了政策文书，旨在明确个人数据处理的基本预期。此类文书的例子包括欧洲委员会[7] 和经合组织[8]提出的文书。这些文书围绕一系列原则逐渐趋同，而这些原则构成了全球不同司法管辖区（包括英国和欧盟）数据保护法律文书的基础。监管机构在特定司法管辖区内拥有适当的调查和执法权力，负责监督并确保处理活动符合这些原则。

数据保护原则在英国《通用数据保护条例》（英国《通用数据保护条例》）[9] 中的体现如下：

1. 个人数据应当：

a. 以合法、公平且透明的方式处理，并与数据主体相关（“合法性、公平性和透明性”）；为特定、明确且合法的目的收集，且不得以与这些目的不相容的方式进一步处理；根据第89条第1款，为公共利益的存档目的、科学或历史研究目的或统计目的进行的进一步处理，不应被视为与初始目的不相容（“目的限制”）；

b. 充分、相关，且仅限于处理目的所必要的范围（“数据最小化”）；

c. 准确，并在必要时保持更新；必须采取一切合理措施，确保考虑到个人数据的处理目的后，及时删除或更正不准确的个人数据（“准确性”）；

d. 以能够识别数据主体的形式保存的时间不得超过处理个人数据之目的所必要的期限；如果个人数据仅为公共利益的存档目的、科学或历史研究目的或统计目的而处理，则可保存较长时间，但须根据第89条第1款实施本监管规定要求的适当技术和组织措施，以保障数据主体的权利和自由（“存储期限限制”）；

e. 以确保个人数据得到适当安全保护的方式进行处理，包括使用适当的技术或组织措施（“完整性和保密性”）。

2. 控制者应对遵守第1款（“问责”）负责，并能够证明其遵守情况。

英国的组织，或处理英国境内个人个人数据的组织，其处理活动是否符合这些原则，由信息专员办公室（ICO）监测并执法。ICO 是英国数据保护立法的监管机构，拥有立法中规定的调查和执法权力。

处理活动符合数据保护原则，是数据保护设计与默认（DPbD）的基础。根据英国《通用数据保护条例》第25条，DPbD 本身也是组织的一项义务。DPbD 要求组织“实施适当的技术和组织措施” [9] ，以有效落实数据保护原则、保障数据主体的权利，并确保仅处理各项目的所必要的数据。决定措施是否适当的因素包括：当前的最新技术水平、实施成本、处理的性质、范围、上下文和目的，以及对个人权利和自由的风险。重要的是，随着系统在其生命周期中不断发展，必须持续评估这些因素。

对数据保护原则的符合性，以及由此延伸出的对数据保护设计和默认的符合性，均以问责原则为基础。问责原则要求组织开展的处理符合数据保护原则，并且组织能够证明其遵守情况。在本文中，我们选择使用“符合性”而非“合规性”，因为我们认为，评估不仅由监管机构开展，也由组织自身、认证机构和数据主体开展。

ICO 发布的指导文件 [10，11]概述了其对组织在数据保护审计中如何证明符合数据保护原则的预期。

这些预期也可供组织参考，用于开展内部符合性评估，以进行内部质量控制和改进，或为外部符合性评估做准备。以下摘录自 ICO 发布的《问责框架》中的政策与程序部分 [10]：

> ...贵组织通过政策和程序，阐明了实施数据保护原则和保障个人权利的方法，例如数据最小化、假名化和目的限制
>
> …

已发布指南对证明符合数据保护原则的任何符合性声明所需的证据，提出了高层次的预期。组织必须确定如何构建此类证据，以及如何通过连贯的论证将这些证据与数据保护原则的实施联系起来。组织可以选择通过获批认证方案进行认证，或加入获批的行业专属行为准则，以便根据监管机构批准的、更为细化的预期，对其处理活动进行外部符合性评估。然而，在英国，目前 ICO 发布的获批认证方案登记册中列出的认证方案寥寥无几 [12]，，而且已获批的方案在适用范围上也存在局限。

有助于建立统一的基准，以衡量项目、制定最低标准和最佳实践，并提升系统开发与评估的成熟度。然而，证明符合安全标准并非总是轻而易举。安全标准往往需要加以解释，原因包括：i）标准设定的是高层次目标，而非具体且具规范性的要求；ii）标准有意保留了一定的非特定性（以支持更广泛的适用性）；iii）即使满足了标准的字面要求，也可能未遵循其精神。文档的质量、透明度和可审查性也可能存在显著差异，导致人们难以确切理解符合性主张所代表的含义。

Graydon 等人提出符合性论证[3]，旨在提供一种明确、严谨且结构化的方法，用于生成和传达与安全标准符合性声明相关的证据。符合性论证是一种结构严谨、内容全面且经得起质疑的论证，用以证明所提供的证据足以表明某项制品充分满足安全标准的要求。符合性评估会评估论证结构的有效性，以及用于支持主张的证据的有效性，从而确定整体主张的有效性。符合性论证还可纳入辩证质疑，以呈现系统变化或更广泛的情境变化对现有符合性论证有效性提出挑战的场景。对于开发安全关键系统的组织，以及肩负主张、确保和监管符合性职责的主管机关而言，符合性论证的预期优势包括：明确性、透明度、信心、设计效率、可预测性和可重复性。

符合性论证

符合安全标准对于安全关键系统至关重要 [2]，因为偏离预期行为可能会对个人造成人身伤害。安全标准为开发流程提供指导或加以约束，规定或禁止某些产品特性，并规范评估实践。安全标准

安全关键系统通常会将安全论证作为安全案例的一部分，以证明系统运行时足够安全。安全论证会将一项安全

主张分解为一系列子主张，直至能够用证据加以论证。我们可以采用构建安全论证的相同方法来构建符合性论证。与安全论证一样，符合性论证严谨，但必然属于非形式化的逻辑论证。安全论证可以用任何表达能力足够的论证表示法记录。不过，通常认为，使用图形化论证表示法（例如目标结构化表示法（GSN）[13]）会更容易。GSN 也可用于表示符合性论证。

《论证符合性》与数据保护原则

符合性论证有助于证明符合数据保护原则的主张。使用符合性论证，可以提高处理个人数据的组织、监管机构、认证机构和数据主体评估是否符合数据保护原则时的严谨性和一致性。

为展示这一潜力，我们概述了一个处理个人数据的假设案例研究系统。我们展示了如何针对该系统中的特定处理活动，制定符合性论证，以证明其符合某项特定数据保护原则的主张。我们还展示了以下变化如何表示为可能使符合性论证失效的“挑战”，并且需要通过修订论证、证据和／或系统本身来解决：i）所处理的数据；以及 ii）处理数据的目的。

案例研究

背景

我们考虑一种假设的考勤监测系统（StudentCheck），该系统拟在某学术机构中开发和使用。该机构为注册了学习项目的学生提供教学课程。学生必须参加其注册学习项目中各课程模块对应的教学课程。该机构正在考虑开发并使用 StudentCheck，以识别未参加必修会议的学生，并联系这些学生，为他们提供适当的支持。

系统设计

图 **1** 使用数据流图概述了 StudentCheck 的一项拟议设计。该图展示了 StudentCheck 与外部实体（包括系统和用户）之间的高层级数据流。图中还纳入了外部实体之间的部分数据流，以提供更多上下文。

为准备开设某个模块，排课系统会向 StudentCheck 发送该模块的详细信息，包括模块课程的安排以及已注册该模块的学生名单。每次教学会议开始前，授课协调员会向 StudentCheck 请求一个会话代码，并将该代码发给出席会议的学生。随后，学生将会话代码提交回 StudentCheck，以确认其出勤情况。支持团队使用 StudentCheck 查询某次会议缺席学生的详细信息，并向这些学生发送支持邮件。

在内部，StudentCheck 由若干相互作用的子流程组成。为简洁起见，我们仅关注一个特定子流程：更新考勤。该子流程负责处理学生提交的会话代码，并据此更新其课程出勤记录。我们将此子流程视为单一处理活动，因此，在论证其符合数据保护原则时，它构成单一分析单元。关于在系统内对处理活动进行建模和分析时应采用何种适当粒度的决策，对于构建符合性论证以及更广泛地证明符合性至关重要。图 **2** 使用数据流图概述了更新考勤处理活动的一项拟议设计。

参加会议后，学生向 StudentCheck 提供其用户凭据，其中包括用户名和密码，以及会议

签到代码。身份验证流程使用用户数据库，根据所提供的凭证确认学生的身份。随后，会话管理流程使用会话数据库，根据所提供的会议代码确定会议详情。我们认为会议详情包括：唯一的会议标识符；模块标识符；会议开始时间戳；以及会议结束时间戳。考勤管理流程使用该用户的身份和会议详情更新考勤数据库，然后向学生提供出勤确认。为应对签到代码可能被分发给未参加会议的学生，并由其提交的情况，考勤管理流程对能够确认学生参加会议的时间范围施加了限制。

符合性声明

拟由英国的一家学术机构开发并使用StudentCheck。因此，任何个人数据处理都将受英国的数据保护制度管辖。对于处理活动的任何符合性声明，均将依据英国《通用数据保护条例》中体现的数据保护原则作出。

为简洁起见，我们仅关注与更新出勤活动相关的数据保护原则符合性声明（见图2）。我们认为，更新出勤活动所处理的数据属于英国《通用数据保护条例》第4(1)条所述的“个人数据”定义，因此受数据保护制度管辖。具体而言，我们认为，可以通过随用户凭据一并提供的用户名识别学生。此外，我们进一步将关注范围限定为与数据最小化原则相关的符合性主张：

更新出勤活动中的个人数据处理符合数据

英国《通用数据保护条例》的数据最小化原则

符合性论证

我们使用三个场景来展示符合性论证在支持符合数据保护原则的符合性声明方面的潜力。首先，我们概述更新出勤活动符合数据最小化原则这一符合性主张的符合性论证。然后，我们提出对该符合性论证有效性的挑战，以反映：i）活动处理的数据发生变化；以及 ii）活动处理数据的目的发生变化。我们使用以 GSN 表示的符合性论证片段来阐释每个场景。

场景1：为符合数据最小化原则的符合性主张构建符合性论证

图 **3**展示了一个符合性论证片段，该片段旨在佐证更新出勤活动符合数据最小化原则的主张。

整体的符合性主张是论证的顶层“目标”（G1）。上下文要素用于支持解释，并明确界定该主张适用的范围。C1 引用了对处理活动的性质、范围、上下文和目的的描述。英国《通用数据保护条例》使用这些维度来描述处理活动，并为针对这些活动进行基于风险的决策提供依据。C2 引用了对所处理个人数据的技术描述，其中可能包括数据模型或模式。C3 引用了英国《通用数据保护条例》中的数据最小化原则。C4 引用了英国《通用数据保护条例》中数据保护设计与默认的概念。立法中有关数据保护设计和默认的规定进一步说明了哪些不同因素决定了技术和

用于落实数据保护原则的组织措施是否适当。

我们定义了一种论证策略（S1），说明将如何论证符合性主张（G1）。根据英国《通用数据保护条例》中数据最小化原则的措辞，我们可以将论证分解为三个部分。我们可以分别论证这三个部分的符合性，以共同佐证总体主张（G1）。我们创建了三个“子目标”（G1、G2 和 G3）来表示这三个部分，并构建论证以实现每个子目标。构建子目标的论证需要我们解释所引用的术语：“充分”“相关”以及“与目的相关且限于必要范围”，并证明处理符合这一解释。下面摘录了 ICO 发布的指导文件中的内容 [14]，，我们借此确定了对这些术语的解释：

> 您必须确保所处理的个人数据：
>
> 1. 充分——足以妥善实现您所述的目的；2. 相关——与该目的存在合理关联；3. 限于必要范围——您持有的数据不得超出该目的所需；

需要注意的是，对本指导文件的解释本身也具有主观性。例如，“充分”“恰当”和“合理”意味着什么，都需要经过解释。使用符合性论证有助于说明特定概念是如何解释的、为何采取特定的符合性方法，以及如何论证其充分性。

为证明 Update Attendance 处理的个人数据“足以适当实现所述目的”，论证必须说明所处理的数据如何足以实现“出勤监测”的目的。例如，如果所处理的数据遗漏了任何可用于唯一标识学生的数据项，那么就很难论证这些数据对于该目的而言是充分的。为证明个人数据“与该目的存在合理关联”，论证必须说明所处理的数据在语义上与该目的相关。例如，如果所处理的数据包含与学生所属俱乐部和社团相关的任何数据项，那么就很难论证这些数据在语义上与该目的相关。最后，为证明“你持有的数据没有超过该目的所需的范围”，论证必须说明所处理的任何数据对于该目的而言都是必要的。例如，如果所处理的数据包含与上一学年会议相关的数据项，那么就很难论证持有的数据没有超过该目的所需的范围。

图 **4** 展示了一个与充分性相关的子目标（G2）的符合性论证片段。该目标与上下文（C5）相关联；该上下文通过引用 ICO 指导文件中对“充分”的描述，支持对论证的解释。根据 ICO 指导文件，我们定义了一种论证策略（S2），指出将通过参照数据的充分性来论证符合性。我们将此策略与上下文（C6）相关联，该上下文指出，充分性将从三个维度来表述：1）数据项所涉及的数据主体；2）针对这些数据主体处理的数据项；以及 3）这些数据项的值。我们将论证分解为与这三个维度相关的子目标（G5、G6 和 G7）。我们还展示了如何将 G5 分解为另外两个主张（或子目标），以支持 G5 中的主张。

可以使用不同形式的证据来证实主张，包括政策和程序、自动化测试结果以及形式化证明。在图4中，我们引用了一份论证报告（Sn1）和一份审计报告（Sn2），它们可能分别用于证实 G8 和 G9。

论证报告将概述数据项所涉及处理的数据主体类别（例如，注册学生），并说明为何对这些主体相关数据项的处理足以用于出勤监测。审计报告将评估（最好是

独立评估）论证报告是否合理。作为本项工作的一部分，我们并未编制上述论证或其他相关论证所要求的论证报告或审计报告。我们也未探讨报告的不同形式，或可用于佐证 G5 或其他主张的不同证据形式。为简洁起见，图4中未列出 G6 和 G7 的任何证据节点。不过，我们认为，任何适用于 G5（以及 G8 和 G9）的证据形式也都适用于 G6 和 G7。

数据保护制度及其由包括监管机构在内的不同利益相关方群体所作的解释，可能会随着时间推移而发生变化。因此，应在系统生命周期内定期审查符合性论证，以确保其持续有效。此外，构成该系统的处理活动也可能会随着时间推移而发生变化，例如由于新增功能和错误修复。因而，先前构建的论证可能不再有效且不足以证实符合性声明。符合性论证可以纳入辩证质疑，以明确表示并应对系统以及负责该系统的组织所受政策文书的变化。

现在，我们简要探讨两个场景，在这些场景中，可以使用辩证质疑，对变更后符合性论证的持续有效性提供明确的推理。

场景 2：针对处理的数据发生变化后提出符合性论证质疑

图 **5**展示了一个符合性论证片段，其中针对先前符合性论证的有效性提出了质疑，原因是有人提议更改更新出勤活动所处理的数据。这类更改可能由一系列功能性和非功能性系统需求驱动。为简化起见，我们考虑将用户凭据（包括用户名和密码）从该活动所处理的数据项中删除，以满足安全需求。因此，所处理的数据项可能不再足以实现出勤监测的目的。可以使用针对“数据项足够”这一主张（G6）的辩证质疑（CG1），以明确表示并探讨这一情形及其对符合数据最小化原则的影响。

论证中包含的质疑需要得到适当回应，以确保论证持续有效。回应可能包括反驳质疑（解释为何提出的质疑无效）；对系统设计、实施和/或部署进行变更；以及纳入其他论证 [15]。我们不探讨这些潜在策略的使用，也不探讨它们可能如何适用于上述符合性论证。我们仅希望强调：处理的数据发生变化可能会使符合性论证失效；如何使用辩证质疑表示这种潜在的无效性；有哪些不同策略可用于应对这类质疑；以及采取这些策略应如何通过修订论证、证据和/或系统本身来推动问题得到解决。

符合性论证的优势之一，在于能够更有效地识别潜在挑战，并推动讨论和选择适当的回应。

场景 3：因数据处理目的发生变化而对符合性论证提出质疑

图 **6**展示了一个符合性论证片段，其中包含对先前符合性论证有效性的质疑，原因是活动处理数据的目的发生了变化。这类变化可能再次由一系列功能性和非功能性系统需求驱动，但我们认为，此类变化更有可能由功能性系统需求驱动。

为简便起见，我们认为处理数据的目的已扩展为包括出勤预测。可以通过对说明处理活动目的的上下文（C1）提出辩证质疑（CG2），明确表示并探讨这一情景及其对符合数据最小化原则的影响。该质疑主张，目的的变化意味着其解释取决于目的的子主张及相关证据，以及作为整体的符合性论证，可能不再有效。

如场景 2 所述，我们有多种应对变化的方案。例如，可以尝试构建论证，主张“出勤预测”的处理与“出勤监测”的原始目的“兼容”。不过，我们同样不会探讨此类策略，也不会探讨这些策略如何适用于上述符合性论证。

符合性论证中未包含有关目的有效性的论证或证据。例如，涉及目的合法性和特定性的主张。不过，在为现实场景构建论证时，需要此类论证和证据。例如，与目的限制原则相关的“更新出勤”活动的符合性论证中，可能会包含此类论证和证据。因此，针对给定处理活动的不同原则所作的符合性论证可能相互依赖。这种相互依赖意味着，对某一原则（如目的限制）的符合性论证提出质疑，也可能导致其他原则（如数据最小化）的论证失效。

讨论

局限性

我们针对特定阶段的假设案例研究系统（StudentCheck）中的一项特定处理活动（更新考勤），围绕一项数据保护原则（数据最小化）提出了符合性论证即系统生命周期的设计阶段。针对不同系统中处于系统生命周期不同阶段的处理活动，围绕其他数据保护原则构建论证，将凸显更多需要考虑的因素。我们还仅关注数据保护原则在英国数据保护制度中的体现，并参考了英国特有的立法和指导文件。

所提出的论证和支持性证据仅旨在作为指示性内容。在提出对符合性论证的质疑时，我们没有探讨可用于应对这些挑战的不同方案。我们也没有将使用符合性论证与组织用于证明符合数据保护原则的现有实践进行比较和对照。

益处

构建符合性论证能够使组织在系统生命周期的各个阶段，对其符合数据保护原则的主张的真实性建立更大的信心。组织可以使用论证为设计、实施和部署决策提供信息，支持与数据主体的沟通，并为内部和外部评估流程提供依据。符合性论证还有可能使负责外部符合性评估的利益相关方受益，包括监管机构和认证机构，因为这能够提高不同组织之间论证和证据的一致性与严谨性，并降低成本。

构建和评估符合性论证也可能促使利益相关方发展有关数据保护理论与实践的知识和技能，从而支持他们就更广泛的个人数据处理作出更明智的决策。构建和评估符合性论证也可能凸显组织在实际落实数据保护原则并论证其符合性时面临的挑战，进而推动

数据保护立法的更新，以及监管机构和认证机构发布的指导文件。

挑战

构建和评估符合性论证颇具挑战，尤其是对于缺乏相关经验的个人和团队而言。组织需要了解系统所涉及的所有政策文书，掌握系统相关的技术细节，并具备有效整合与综合这些知识、形成有力符合性论证的技能。组织可能需要多学科团队的参与，其专业知识涵盖计算机科学、法律和伦理学等领域。因此，利益相关方可能需要通过适当的招聘和技能提升，来支持采用符合性论证的方法。

组织还必须能够确定对系统建模并构建符合性论证时适当的细化程度，在最终论证的严谨性与构建和维护论证所需的资源之间取得平衡。

采用符合性论证还会受到利益相关方群体之间相互依赖关系的影响，因此，一个群体（例如组织）是否采用，取决于另一个群体（例如监管机构）是否采用。在采用初期，利益相关方群体之间可能需要开展大量沟通与协作，以确保各方在相互一致的实践上达成共识。

未来工作

由于现有指导文件有限，未能就内容、结构和呈现方式为组织提供充分指引，因此我们认为，组织可能会构建相互矛盾的论证和证据，且不足以支持有意义的符合性评估。不过，还需开展更多工作，以识别并描述组织目前使用的做法来证明符合性，并确定这些做法在组织内部及组织之间的差异程度。

还需要开展更多工作，以确定使用符合性论证是否足以支持监管机构等对符合性的实质性评估，并探讨不同利益相关方群体在采纳方面面临的障碍。针对不同利益相关方群体开展定性研究，深入探讨更详细（且可能是真实场景中的）案例研究，将有助于凸显具体机遇与挑战。

采纳符合性论证可能需要面向各利益相关方群体制定并开展教育和培训。组织将受益于分步指南、标准操作程序和模板；这些材料界定了具有广泛适用性的论证与证据结构。

未来工作还可以探讨，在系统生命周期的不同阶段，哪些形式的论证和证据最适合用于证实与特定数据保护原则相关的主张。

目前已有用于支持构建以 GSN 表示的论证的通用工具。然而，专用于数据保护的工具可以为构建和评估论证的人员提供进一步帮助。也可以开发工具，用于突出显示部署后处理活动的变化（例如组件更新），并支持重新评估论证。符合性论证很可能会作为“持续更新”的制品进行管理，并在整个系统生命周期内不断更新。支持持续管理这些制品的工具和方法，可能会对负责符合性评估的组织及其他利益相关方群体有所帮助。

结论

我们已展示如何使用符合性论证，为符合数据保护原则的主张提供依据；

从而提高组织、监管机构、认证机构和数据主体评估是否符合数据保护原则时的严谨性和一致性。我们的工作还指出了采用这一方法面临的一些挑战，包括构建、维护和评估论证所需的专业知识和时间。未来为支持这一方法开展的工作，应着重于面向数据保护生态系统中不同利益相关方群体的参与、教育和培训计划，以及开发相关工具，以提高构建、维护和评估论证与证据的有效性和效率。

致谢

通讯作者为 Richard Hawkins，地址：英国约克大学计算机科学系，Deramore Lane，YO10 5GH。联系 Richard：richard.hawkins@york.ac.uk。

■ 参考文献

1. C. J. Bennett 和 C. D. Raab，《隐私治理：全球视角下的政策工具》。美国纽约州：劳特利奇，2018年。2 Rierson, L., 2017年。《开发安全关键软件：航空软件与 DO-178C 合规实用指南》。CRC出版社。3. P. Graydon、I. Habli、R. Hawkins、T. Kelly 和 J. Knight，《论证符合性》，《IEEE 软件》，第29卷第3期，第50-57页，2012年2月，doi: 10.1109/MS.2012.26。4 D. K. Citron 和 D. J. Solove。《隐私侵害》，《波士顿大学法律评论》，第102卷第3期，第793-864页，2022年4月。[在线]。网址：https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf [访问日期：10月31日2024]。5. A. Westin，《隐私与自由》，美国纽约州：IG出版社，1967年。6. P. Regan，《隐私立法：技术、社会价值与公共政策》，美国北卡罗来纳州：北卡罗来纳大学出版社，1995年。7. 《关于自动处理个人数据时保护个人的公约》（第108号公约），1981年，法国斯特拉斯堡：欧洲委员会。8. 《隐私保护和个人数据跨境流动指南》，1980年，法国巴黎：经合组织出版服务处。

9. 《欧洲议会和理事会《欧盟第2016/679号条例》》，2016年，c.1，英国伦敦：国王议会法令印刷局。10. 信息专员办公室。《问责框架》，ico.org.uk。[在线]。网址：https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/ [访问日期：5月30日2025]。11. 信息专员办公室。《数据保护审计框架》，ico.org.uk。 [在线]。网址：https://ico.org.uk/for-organisations/advice-and-services/audits/data-protection-audit-framework/ [访问日期：5月30日2025]。12. 信息专员办公室。《认证计划登记册》，ico.org.uk。 [在线]。网址：https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-schemes-register/[访问日期：5月30日2025]。13. ACWG。《目标结构化表示法社区标准》。技术报告 SCSC-141C v3.0，安全关键系统俱乐部，2021年。14. 信息专员办公室。原则（c）：数据最小化。[在线]。网址：https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/data-minimisation/ [访问日期：10月21日2025]15. R. Hawkins。《构建有说服力的安全论证》，arxiv.org。[在线]。网址：https://arxiv.org/html/2502.00911v1 [访问日期：5月30日2025]。

Chris Smith 曾任英国约克大学计算机科学系讲师。他的研究兴趣包括隐私保护、问责和可信度。Smith 获得纽卡斯尔大学计算科学博士学位。可通过领英联系他：https://www.linkedin.com/in/drcjsmith/。

Richard Hawkins 是英国约克大学的副教授。他的研究兴趣包括自主系统和人工智能的安全论证与安全保障。Hawkins 在约克大学获得计算机科学博士学位。联系方式：richard.hawkins@york.ac.uk。

附录A

StudentCheck 系统的设计受到约克大学[1]所用系统的启发。具体而言，该设计使用“会话代码”来表示会议出勤情况。我们推测了此类系统可能涉及的具体处理活动，所呈现的设计正是这一推测的结果。我们并未声称这些推测的活动与约克大学正在使用的系统或任何其他类似系统所包含的活动相符。我们也未声称这些推测的活动涵盖此类系统所需的全部活动。不过，我们认为，这些推测的活动足够贴近实际，能够证明符合性论证适用于与数据保护原则相关的主张

[1] 如需了解更多信息，请访问：
https://www.york.ac.uk/students/support/check-in

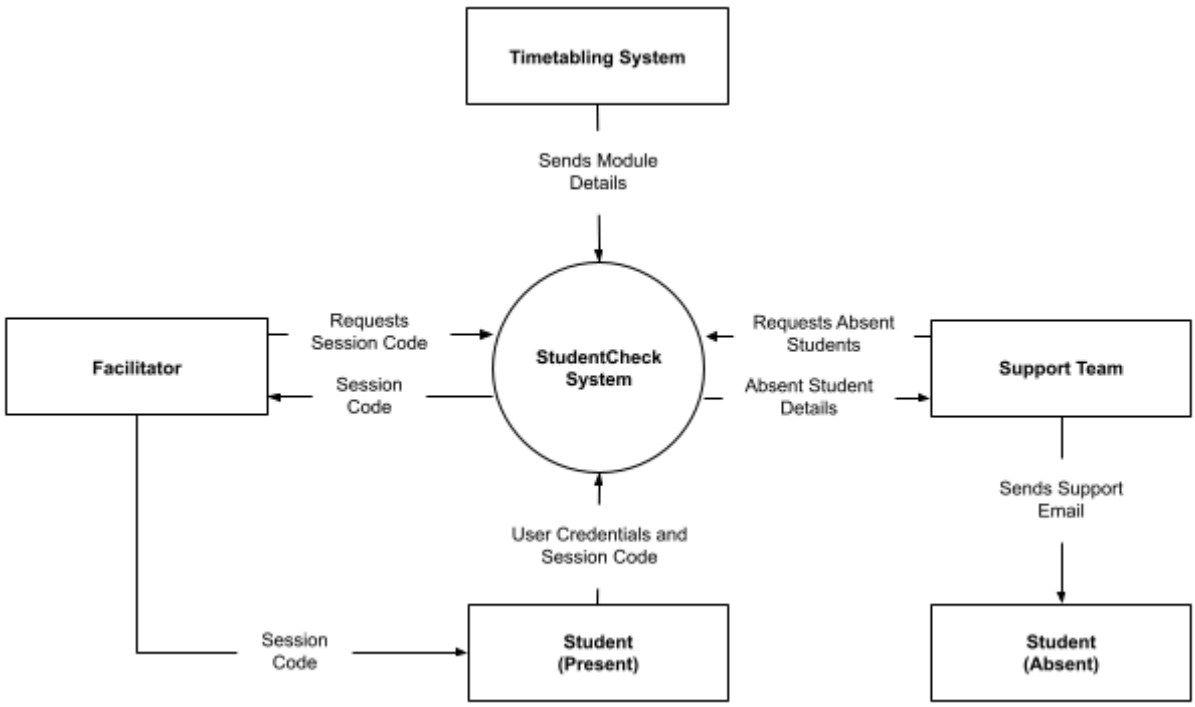


图 1. StudentCheck 系统的数据流图

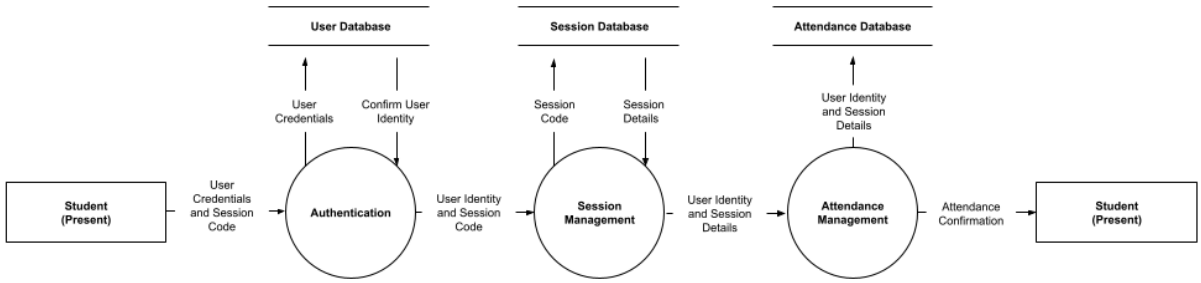


图2. 更新出勤処理活动的数据流图

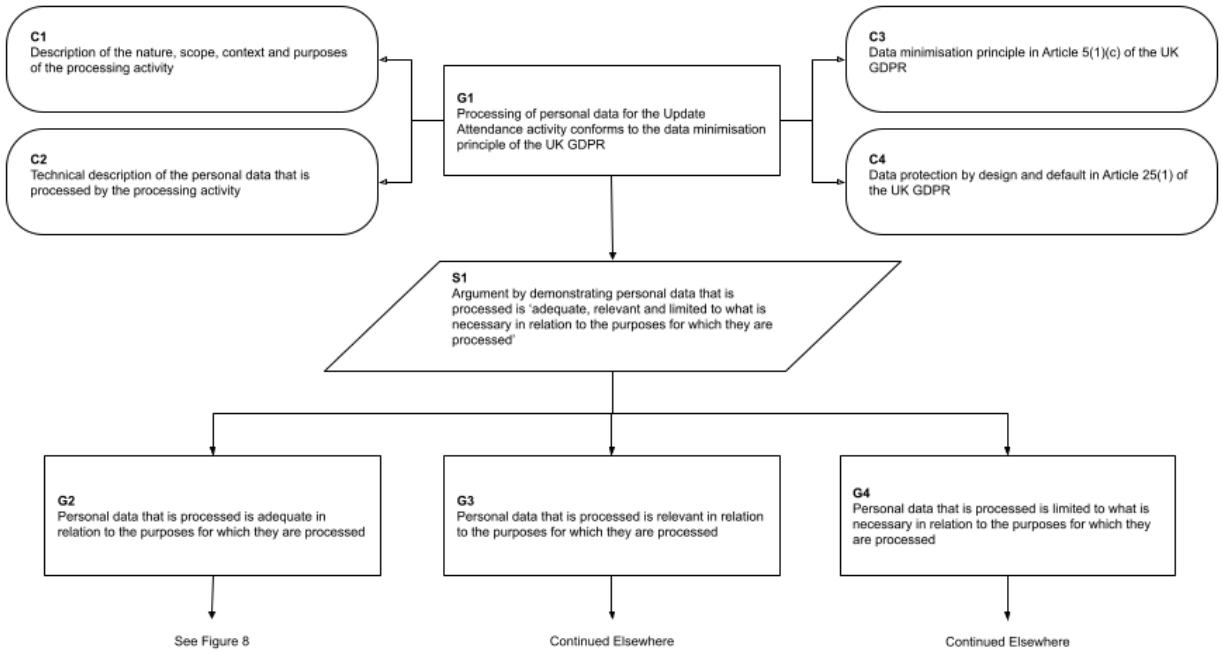


图3. 关于“更新出勤处理活动符合英国《通用数据保护条例》数据最小化原则”这一主张的 GSN 符合性论证片段

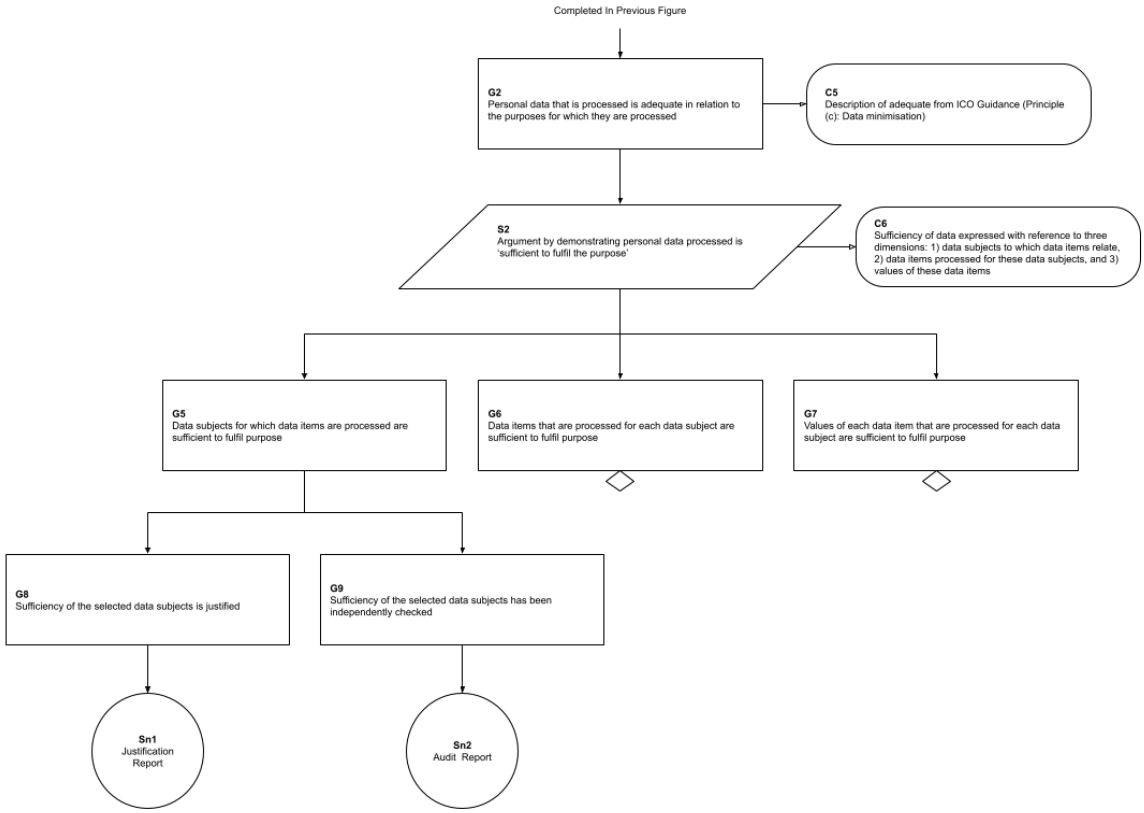


图4. 针对以下主张的 GSN 符合性论证片段：为更新出勤处理活动而处理的个人数据足以满足其处理目的

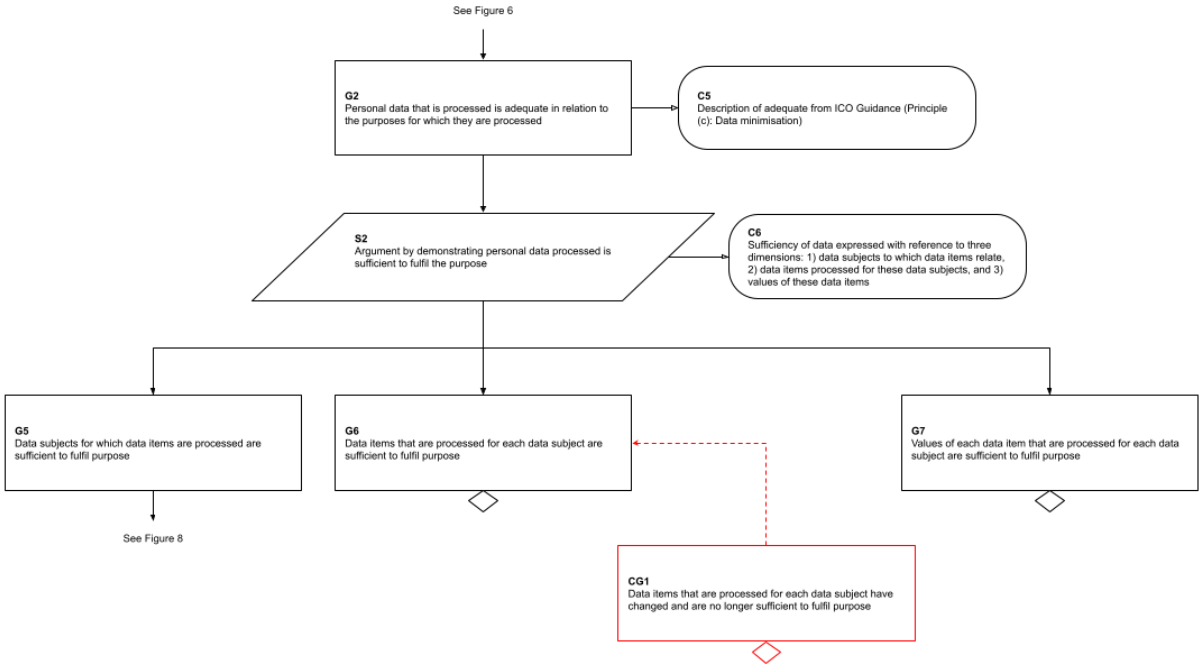


图5。GSN 中的符合性论证片段，其中包含对以下主张的辩证质疑：为更新考勤而处理的个人数据对于其处理目的而言是充分的

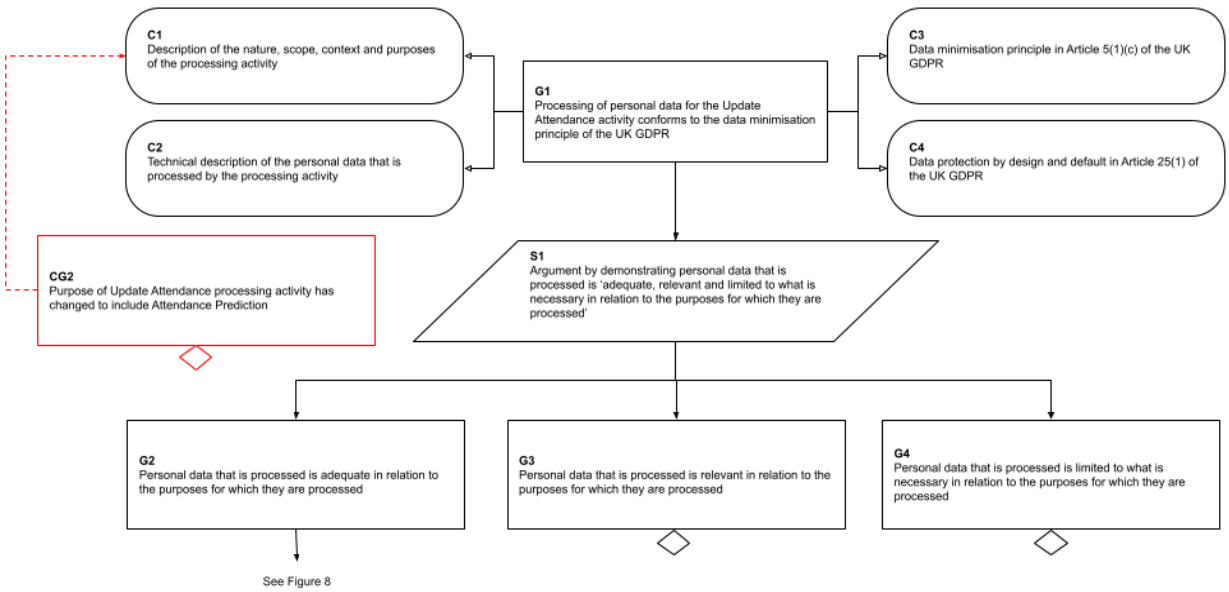


图 6. GSN 中的符合性论证片段，其中包含对更新出勤活动处理个人数据的目的提出的辩证质疑