This document was translated from English by machine and may contain mistakes. The English original is at https://www.novaracg.com/2026/08/30/the-procurement-file-is-the-governance-system/.

采购档案就是治理体系

Heather Grizzle · August 30, 2026

AI governance becomes real in the procurement file, where an institution records the evidence behind a deployment that affects disabled people.

1. 目录

1. 执行摘要
2. 治理最终必须触及交易本身
3. 作为问责工具的采购档案
4. 1. 预期用途与禁止用途
5. 2. 受影响人群分析
6. 3. 供应商声明记录
7. 4. 独立保障
8. 5. 故障与后备机制架构
9. 6. 性能边界与已知的未知
10. 7. 日志记录、可追溯性与事件重建
11. 8. 投诉、可争议性与救济
12. 9. 模型变更与重新验证
13. 10. 暂停与退出权限
14. 从人工智能政策到机构层面的证据
15. NCG政策立场
16. 结语立场

作者：Heather Grizzle，Novara Consulting Group

2. 执行摘要

人工智能治理越来越多地通过政策、委员会、原则、清单和风险分类来体现。这些结构固然重要。但当一家公共机构真正采购并部署一套人工智能系统时，治理最终必须变成远没那么抽象的东西。它必须变成一份记录。

Someone has to describe what the system is allowed to do. Someone has to decide what evidence is sufficient to support the vendor's claims. Someone has to identify the people who may be harmed when the system fails. Someone has to determine which failures require human intervention, which changes require reevaluation, and which conditions require the system to be suspended. If those decisions are not documented before deployment, an AI governance policy does not cure the omission. The procurement file is where institutional principles become operational commitments.

摘要

对于影响残障人士的人工智能系统而言，采购档案应当包含足够的证据，以便在出现问题之后能够回答一个基本问题：机构有何合理依据相信该系统适用于这一用途、这一人群和这些条件？如果无法从记录中还原出这一答案，那么在系统上线之前，治理体系就已经是不完整的。

---

3. 治理最终必须触及交易本身

> 备用机制只有在需要的人真正能够使用它时，才称得上是一种保障。
>
> Heather Grizzle

Organizations are building increasingly sophisticated AI governance structures. They establish responsible AI principles, create review committees, maintain inventories, and classify systems according to risk. They adopt policies requiring fairness, transparency, accountability, privacy, accessibility, and human oversight. Then procurement begins. A vendor responds to a solicitation. Product demonstrations are scheduled. Accessibility

documentation is collected. Security questionnaires are completed. Legal terms are negotiated. Business owners describe the efficiencies they expect. The technology clears the institution′s established gates and enters service.

这些关卡的存在可以带来相当程度的机构信心，但信心并不等同于一项站得住脚的决定。关键的治理问题不仅仅在于该系统是否通过了必要的流程，而在于由此形成的记录中是否包含足以证明所批准的具体部署合理性的证据。

That distinction becomes especially important when AI mediates access for disabled people. A system may summarize information, communicate with patients, evaluate applicants, translate language, generate instructional material, prioritize cases, assist employees, authenticate users, answer questions, or, increasingly, act on behalf of an institution. In each case, accessibility is not simply a characteristic of the interface. It is part of the decision architecture. A disabled person may encounter a system differently from the population on which it was primarily designed, tested, or validated, and an accessibility failure may alter the information that person receives, the choices available to them, their ability to respond, or the institution′s interpretation of their behavior. The procurement record therefore needs to establish more than whether accessibility was considered. It needs to establish what was considered, what was tested, what remains unknown, and what the institution decided to do about the uncertainty.

作为问责工具的采购档案

4. 作为问责工具的采购档案

Procurement files are often understood primarily as administrative records. For AI, they should increasingly be understood as governance instruments. A mature AI procurement record should allow an independent reviewer to reconstruct the institution′s reasoning without relying on the institutional memory of the people who participated in the purchase. That means the record should answer several questions:

1. 该系统被购买的确切目的是什么？
2. 它被明确禁止做什么？
3. 预期哪些人群会接触到它？

4. 在批准过程中所依赖的各项声明，有什么证据支持？这些证据由谁产生？
5. 已知哪些局限性？还有哪些局限性仍属未知？
6. 当系统出现不确定或错误时会发生什么？
7. 谁保留着推翻其结果的权力？
8. 受影响的人如何能够对其输出结果提出质疑？
9. 什么情况会促使机构重新考虑该部署？
10. 谁拥有叫停它的权力？

这些不是故障发生后事故调查时才需要提出的问题，而是采购环节就应回答的问题。

1. 预期用途与禁止用途

5. 1. 预期用途与禁止用途

第一项要求看似简单：明确机构究竟购买了什么。人工智能系统常常是通过宽泛的功能描述来采购的。系统可能被描述为助手、翻译工具、无障碍工具、决策支持系统、聊天机器人、代理、筛查工具或生产力平台。这些标签作为治理规范是不充分的。采购记录应当明确该系统的实际机构职能。

用于帮助某人浏览网站的通讯工具，其风险与用于医疗接诊环节的同一技术不同。用于生成会议记录的自动转录系统，其风险与用于形成纪律处分程序正式记录的同一系统不同。个人出于试验性目的使用的手语识别系统，与机构将其作为另一种沟通可及方式之替代品来呈现的同一系统，二者并不等同。因此，同一项技术在底层模型未发生任何变化的情况下，也可能在不同风险类别之间转移，原因在于部署场景发生了变化。

> **在便利抹去边界之前先划定边界**
>
> 采购档案应当同时说明预期用途和禁止用途。若缺少后者，机构就会产生可预见的范围扩张：一款为有限用途而获批的工具变得可用，员工发现了额外的应用方式，机构的使用范围便逐渐超出了最初获批所依据的证据。

2. 受影响人群分析

6. 2. 受影响人群分析

传统技术采购问的是谁将使用该系统。人工智能治理还必须追问谁将受其影响，而这两类人群未必相同。员工可能操作某一人工智能系统，而承受其后果的却是患者、学生、申请人、居民、客户或福利领取者。残障人士往往特别难以通过常规的用户分析被识别出来，因为残障状况改变的往往是通过系统的路径，而非名义上的用户类别。

The procurement record should therefore identify foreseeable accessibility interactions. Does the system process speech? Does it generate or interpret language? Does it depend on vision, hearing, dexterity, cognition, timing, biometric characteristics, or a particular mode of communication? Does it infer intent or competence from behavior that disability may affect? Does an inaccessible output alter a person′s ability to participate in a subsequent decision? These questions convert accessibility from a compliance artifact into a system-risk inquiry.

3. 供应商声明记录

7. 3. 供应商声明记录

Every consequential vendor claim relied upon during procurement should have an evidentiary status. Not every claim requires independent testing, but institutions should distinguish among at least three categories. A capability is claimed when the vendor states that it exists. It is demonstrated when evidence shows that it has been observed under specified conditions. It is established for deployment when evidence reasonably supports reliance on it in the institution′s intended context. Those categories are not interchangeable.

一次演示可以证明系统能够产生某种输出结果，但未必能够证明该系统在不同人群、不同环境或不同重大用例下产生该结果的可靠程度。同样，文档可以证明供应商就其系统做出了何种陈述，却不能独立证明该陈述的正确性。采购档案应当保留这一区分，否则，断言仅仅因为在足够多的文件中被反复重申，就会逐渐被当作既定事实。

> **已确立可供部署**
>
> A vendor claim status meaning evidence reasonably supports reliance on the capability in the institution′s actual, intended context, not merely that the capability has been observed under demonstration conditions.

4. 独立保障

8. 4. 独立保障

供应商提供的证据在采购中具有正当作用。供应商比采购方更了解自身的系统,理应披露测试情况、架构、局限性、已知故障条件以及相关性能证据。但商业关系是一个不可忽视的因素。寻求合同的一方不应是唯一决定该证据是否足以促成合同授予的一方。

Independent assurance does not mean recreating the vendor's engineering program. It means testing the claims that matter to the purchasing decision under conditions capable of disproving them. For accessibility-related AI, this may require evaluation involving people with the relevant disability and, where linguistic access is involved, qualified members of the language community. The objective is not ceremonial participation. It is evidentiary authority. The people capable of identifying a consequential failure must have a mechanism for causing that failure to affect the procurement decision. Otherwise, participation exists without governance.

5. 故障与后备机制架构

9. 5. 故障与后备机制架构

Every AI procurement should contain a written answer to a single question: what happens when the system does not work? "Human in the loop" is not an adequate answer. The record should identify the human, the trigger, the authority, the response time, and the alternative pathway available to the affected person.

对残障用户而言,后备机制本身也必须是无障碍的。一个失灵后要求聋人拨打电话的人工智能沟通系统,并未真正提供后备方案。一个变得不可及、却仍要求盲人用户使用同样不可及界面来完成操作的自动化数字流程,也并未在任何实质意义上将该用户转交给人工监督。

6. 性能边界与已知的未知

备用机制只有在需要的人真正能够使用它时，

才称得上是一种保障。

Heather Grizzle

10. 6. 性能边界与已知的未知

采购文件通常会记录产品能够做到什么。治理记录同样需要说明信心止于何处。人工智能的表现是有条件的,可能因语言、方言、口音、手语风格、光线、摄像头位置、残障类型、设备、环境、专业术语、交互时长、人口特征以及无数其他变量而有所不同。机构应要求供应商披露已知的性能边界,并另行记录尚未经过评估的领域。

这一区分至关重要。“未经评估”与“已经失败”并非同一种结论,但它同样也不等同于“安全”。如果不确定性被识别并加以治理,它就不构成采购上的缺陷。未被记录的不确定性才是缺陷。

7. 日志记录、可追溯性与事件重建

11. 7. 日志记录、可追溯性与事件重建

当人工智能介导的交互造成损害时,机构应当能够重建事件经过,而这需要在部署之前就对日志记录做出决定。当时运行的是哪个系统版本?接收到了哪些输入?生成了哪些输出?该输出是否被修改过?是否有人工审核过?审核人看到了哪些信息?随后采取了什么行动?机构能否在不保留本不应保留的数据的前提下,重现该事件?

可追溯性与隐私保护之间可能存在正当的相互竞争的要求。这种冲突应通过系统设计和治理加以解决,而不应在诉讼、无障碍投诉或内部调查过程中才被发现。采购文件应记录该冲突的解决方式。

8. 投诉、可争议性与救济

12. 8. 投诉、可争议性与救济

受人工智能影响的人所需要的,不仅仅是一个报告技术问题的机制。他们可能需要对机构因该系统而做出的行为提出异议,而这是一项不同的功能。如果人工智能系统错误翻译了沟通内容、错误刻画了行为、生成了不可及的信息、得出了错误的推断,或促成了不利的机构行动,受影响的人需要有途径对由此产生的决定提出质疑。

机构应在部署之前就明确:由谁接收异议、由谁进行调查、保留哪些证据、在审查期间受质疑的人工智能输出是否仍然有效、可采取哪些补救措施,以及机构必须在多长时间内作出回应。

反馈表单不是救济机制

救济需要有明确的接收方、调查流程、被保留的证据、关于受质疑输出在审查期间是否继续生效的决定、明确规定的补救措施,以及回应期限。

9. 模型变更与重新验证

13. 9. 模型变更与重新验证

人工智能采购带来了一个传统软件合同并未特别针对性设计来应对的问题:当初经过评估的产品,未必仍是最终部署的产品。模型会更新,防护机制会改变,训练数据会改变,界面会改变,第三方依赖关系会改变,供应商会更换底层模型。即使采购机构自身未发起任何变更,系统性能也可能在某一领域有所提升,而在另一领域有所下降。

因此,采购文件需要制定变更控制规则。关键问题不在于供应商是否有权更新其产品,而在于哪些变更会使机构此前所依赖的证据失效。合同应明确哪些属于重大变更,须发出通知、重新评估、重新进行验收测试,或在特定场景下继续使用前须获得批准。否则,机构即便在采购阶段进行了严格的保障审查,六个月后仍可能发现自己正在用为前一版本系统所准备的证据,来治理一个实质上已然不同的系统。

10. 暂停与退出权限

14. 10. 暂停与退出权限

没有叫停权的治理只是一种建议。机构内部必须有人拥有相应权限,能够在证据不再支持继续使用时限制、暂停或终止某项人工智能部署,而触发条件不应等到危机发生时才临时制定。

- ☐ 反复出现的无障碍故障
- ☐ 未披露的重大模型变更
- ☐ 丧失所需的人工监督
- ☐ 与已验证性能出现重大偏差
- ☐ 未解决的投诉

☐ 出现针对特定群体造成伤害的新证据

☐ 未能提供合同要求的信息

☐ 超出已批准的使用场景

采购记录应同时明确触发条件与决策权限归属。

它还应涉及退出安排。合作关系结束时,机构数据归谁所有或由谁接收?哪些记录必须保留?哪些必须删除?机构如何恢复此前的服务途径?对于已经依赖该人工智能介导流程的人员将会怎样?退出规划不仅仅是供应商管理问题,它更是可及性延续的规划。

从人工智能政策到机构层面的证据

15. 从人工智能政策到机构层面的证据

人工智能治理当前面临的挑战,并非原则数量不足,而在于如何转化落地。公平必须转化为评估标准。透明必须转化为披露要求。人工监督必须转化为明确授权的职责。无障碍必须转化为部署条件。问责必须转化为具名的负责部门和有据可查的补救措施。监测必须转化为触发行动的机制。而“负责任的人工智能”最终必须转化为采购官员能够归入档案的实际材料。

This is particularly important in public institutions because procurement is where abstract institutional commitments encounter money, contracts, vendors, statutory duties, and people who cannot simply choose another government, school, hospital, court, or public service when the technology does not work for them. The procurement file therefore performs a function much larger than recordkeeping. It establishes the institution's theory of acceptable risk.

NCG政策立场

16. NCG政策立场

Novara Consulting Group holds that AI systems affecting disabled people should not be approved solely because they have satisfied an organization's general AI governance process. The procurement record should contain sufficient evidence to reconstruct and defend the specific deployment decision.

该记录至少应当明确以下内容

- 该系统的预期用途与禁止用途
- 可预见受影响的人群
- 关键供应商主张的证据状态
- 在必要情况下进行独立保障审查的依据
- 未知的失效条件与未经测试的条件
- 无障碍备用方案与人工复核途径
- 日志记录与可追溯性要求
- 投诉、可争议性与救济程序
- 重大变更与重新验证触发条件
- 机构限制、暂停或终止部署的权力

该标准并非完美的认知。任何采购流程都无法消除不确定性。该标准所治理的是受控的不确定性:即明确哪些已经确立、哪些尚未确立、哪些证据支持在此情况下仍然推进,以及谁对这一决定承担责任。

结语立场

17. 结语立场

在人工智能发生失误之后,机构往往会追问供应商是否本应发出警示。有时答案确实是肯定的。但公共问责还要求另一个问题:机构在同意推进之前要求了哪些证据?这个问题不能外包。供应商可以提供证据,评估者可以对其进行评估,委员会可以提出建议,残障利益相关者可以识别他人看不到的失效之处,律师可以就合同风险的分配进行协商。但决定权始终在机构手中,其采购记录应当证明它清楚自己所做的是怎样的决定。

一个人工智能系统之所以受到治理,并不是因为采购档案正是问责得以开始的地方。

> 某个组织制定了人工智能政策,而是当该机构能够说明,为什么在这些条件下,针对这些受影响的人群,出于这一目的,这一系统被准许运行。
>
> Heather Grizzle

TIPS

Know something about a sign language AI system that the public should know? Send it to tips@novaracg.com. Every tip is read by me and kept confidential. If you work in the UK, writing to us is not by itself a protected disclosure under the Public Interest Disclosure Act 1998, so before you share employer information, check your options with Protect (protect-advice.org.uk), the free whistleblowing advice line.

---

18. 引用方式

Grizzle, H. M. (2026, August 30). 采购档案就是治理体系. Novara Consulting Group. https://doi.org/10.5281/zenodo.23003317