

## 对《2023 年隐私影响评估报告》的回应

### 国家残障数据资产和澳大利亚国家数据集成基础设施

社会服务部 (Department of Social Services) 正在与澳大利亚统计局 (Australian Bureau of Statistics, 以下简称为 ABS) 和澳大利亚健康与福利研究所 (Australian Institute of Health and Welfare, 以下简称为 AIHW) 合作, 创建国家残障数据资产 (National Disability Data Asset)。我们将这三个澳大利亚政府机构并称为联邦机构合作伙伴。

各州、领地和残障社区也参与了残障数据资产的开发。[National Disability Data Asset Council](#) (国家残障数据资产理事会, 以下简称为理事会) 负责监督残障数据资产的使用。这包括了政府和残障社区的共同决策。残障数据资产汇集了来自不同政府机构的有关所有澳大利亚人的信息, 以便更好地了解残障人群的各方面情况。此类信息皆经过处理, 不包含个人身份信息。

残障数据资产的底层支持系统是澳大利亚国家数据集成基础设施 (Australian National Data Integration Infrastructure)。在该系统的支持下, 我们能够在残障数据资产中实现数据联动, 并对数据进行分析。澳大利亚国家数据集成基础设施委员会 (Australian National Data Integration Infrastructure Board, 以下简称为委员会) 负责监督该系统的交付和使用。

更多信息请参阅[国家残障数据资产网站](#), 其中包括有关[国家残障数据资产中的隐私保护](#)的信息。

### 什么是隐私影响评估?

本文件是联邦机构合作伙伴对 2023 年隐私影响评估 (Privacy Impact Assessment, 以下简称为 PIA) 中提出的建议做出的回应。

PIA 是对某个项目及其可能对隐私产生的影响进行的审查。PIA 对管理、降低或消除隐私风险和影响的方法提出了建议。

Maddocks 的隐私专家对残障数据资产及其底层系统进行了 PIA 评估。

为了进行 PIA 评估, 联邦机构合作伙伴和 Maddocks 在 2023 年 3 月至 7 月期间征询了利益相关者的意见。Maddocks 根据反馈意见撰写了一份详细的《意见征询报告》。

有关 PIA 评估报告的摘要和有关《意见征询报告》的摘要可在国家残障数据资产网站的 [Privacy for the National Disability Data Asset](#) (国家残障数据资产中的隐私保护) 页面查阅。

联邦机构合作伙伴计划于 2025 年对 PIA 进行更新。

## 评估流程

2023 年进行的 PIA 评估包括以下流程：

- 审核了残障数据资产和底层系统是否符合澳大利亚的 [Privacy Act 1988](#)（《1988 年隐私法》），包括 [Australian Privacy Principles](#)（《澳大利亚隐私原则》）——这些法律是关于如何管理个人信息法律
- 指出了所有隐私风险以及降低风险的方法
- 帮助我们管理项目的所有隐私风险和影响
- 审核了残障数据资产保护个人信息的方法。这包括防止滥用和遗失信息以及防止未经授权的人员访问、更改或共享信息。

## 我们将如何回应所提出的建议

### 建议 1：有关今后向残障数据资产添加数据集的原则

Maddocks 建议我们制定一套原则，以便在政府将新数据添加到残障数据资产中时提供指导。我们应该在国家残障数据资产网站上发布这些原则，并附上对所添加数据的描述。

### 我们的回应

联邦机构合作伙伴对此表示同意。

我们将制定一套原则。这些原则将指导今后有关向残障数据资产添加数据集的决策。数据集是信息、记录和事实情况的集合。

添加新数据集时，这些原则将考虑以下因素：

- 公共利益：特别是是否符合残障人群的利益
- 新数据在残障数据资产中有多大用处
- 使用数据时存在的任何限制。

我们将与各州和领地政府、残障社区和研究人员一起制定这些原则。我们会将这套原则提交给理事会以待批准。我们将在网站上发布这些原则并附上对所添加数据的描述。

我们将在 2024 年 12 月之前完成此项工作。

## 建议 2：数据提供方的收集通知

收集通知是组织机构在向个人索取信息时提供的一种声明。该声明解释了组织机构为什么需要这些信息以及将如何使用这些信息。Maddocks 建议数据提供方在撰写收集通知（例如，表格和网站上的通知）时使用标准措辞。数据提供方是指提供数据以纳入残障数据资产的政府机构。

这些标准措辞应该得到理事会的支持以及委员会的批准。

我们可以要求数据提供方在接下来的一段时间内，开始采用新的标准措辞来更新他们的收集通知。例如，我们可以将该要求包含在数据共享协议中。我们也可以鼓励数据提供方自行采用标准措辞来更新收集通知。这将是告诉人们其个人信息会如何被使用的最佳方式。

## 我们的回应

联邦机构合作伙伴对此表示同意。

我们将要求澳大利亚联邦、州和领地政府的数据提供方采用标准措辞来更新他们的收集通知。

我们将编写一份标准版本的收集通知，以供数据提供方使用。我们将根据以下来源中的措辞来编写该收集通知：

- 国家残障数据资产网站上的隐私声明
- 来自其他资产的收集通知或隐私声明：例如，[Person Level Integrated Data Asset](#)（人员级别集成数据资产）。

我们将征询相关监管团体和数据提供方的意见。

我们将请求委员会在理事会的支持下批准标准措辞。

我们将在 2024 年 7 月之前完成此项工作。

## 建议 3：管理重新识别数据的风险：对流程进行审查

Maddocks 建议理事会定期审查用于管理数据重新识别风险的方法。例如，可以每年进行一次审查。

理事会还可以就审查的触发机制做出决定。例如，可以决定在发生数据泄露时或政府就网络安全威胁提出建议时进行审查。这是为了确保我们在去除数据识别信息和管理重新识别的风险时能够继续采用最佳方式。以上决定应考虑到未来技术和风险的变化。

## 我们的回应

联邦机构合作伙伴对此表示同意。

我们将要求委员会承诺制定重新识别审查流程。该审查将检验我们是否仍在最佳方法来管理重新识别风险。审查可能包括以下方面：

- 监管团体的工作计划
- 对监管工作的记录情况
- 所落实的安全保障措施。

我们将支持至少每年完成一次审查流程。发现任何重大的新风险或风险变化时也会进行审查。

我们将做好以下记录：

- 触发审查流程的所有情况
- 我们采取的所有行动
- 我们实施的所有变革。

我们将向相关监管团体报告审查情况，其中包括委员会和理事会。

我们将在 2025 年 7 月之前完成第一次审查。

### 建议 4：管理重新识别数据的风险：有关共享内容的规则

Maddocks 建议，任何去识别化政策（现称为去识别化策略）都应明确指出：

- 因通过使用残障数据资产中的数据识别出某人而造成严重伤害的风险
- 在使用数据时将该风险纳入考虑范围并进行控制的必要性。

该策略还应包括适用于使用数据的项目的规则。我们应该考虑是否需要任何额外的流程，例如在其他数据资产中使用的流程。例如，用于检查数据分析结果在离开底层系统之前是否已经获得正确的去识别化处理的流程。

## 我们的回应

联邦机构合作伙伴对此表示同意。

我们将在以下方面应用该建议：

- 去识别化策略
- 数据访问、使用和发布协议。

我们将在 2024 年 6 月之前完成此项工作。

## 建议 5：管理数据泄露

Maddocks 建议数据泄露应对计划（现称为数据泄露与事件应对框架（Data Breach and Incident Response Framework））制定好一致的方法来处理所有经手残障数据资产的政府机构的数据泄露问题。该框架应明确说明每个相关监管团体和组织的职责，包括 ABS 在存储数据时的职责。

该框架还应明确规定由谁负责撰写有关泄漏事件的通报，以便告知以下机构和个人：

- 澳大利亚信息专员办公室（Office of the Australian Information Commissioner）
- 国家数据专员办公室（Office of the National Data Commissioner）
- 任何受到泄漏事件影响的人。

## 我们的回应

联邦机构合作伙伴对此表示同意。

我们正在为残障数据资产及其底层系统制定强有力的安全保障流程。所有系统都需要经过审核，在其安全保障性获得核准后才能存储和使用数据。

我们在制定框架时会考虑这一建议。该框架将采用一致的方法来处理数据泄露问题。框架将清楚地解释涉及数据泄露的每个相关监管团体和组织应尽的事宜，并规定负责监督、报告泄露问题并发出通报的人员和机构。

所有职责均应与以下文件中的内容相一致：

- 数据共享安排
- 适用的法律，例如 [Data Availability and Transparency Act 2022](#)（《2022 年数据可用性和透明度法》）中的数据泄露责任和《隐私法》中的数据泄露强制通报计划（Notifiable Data Breaches scheme）
- 任何其他适用的法律或政策。

根据《数据可用性和透明度法》，所有组织都必须获得认证才能提供数据服务。获得认证的组织必须制定自己的政策和流程来管理数据泄露风险。

国家数据专员办公室可以对获认证的组织进行独立审查。例如，他们可能会审查某个组织的活动是否符合《数据可用性和透明度法》体系。

我们将在 2024 年 6 月之前完成该框架。

### 建议 6：制定合规框架

Maddocks 建议委员会制定一个合规框架，以确保每个人都遵守我们的数据共享协议。该框架应涵盖残障数据资产和底层系统。例如，使用残障数据资产和被批准的系统的人员可以每年向以下官员报告：

- 澳大利亚国家数据集成基础设施监管员（Australian National Data Integration Infrastructure Guardian）
- 国家残障数据资产监管员（National Disability Data Asset Guardian）

这两名监管员都是 ABS 官员。他们负责以安全且符合法律和道德的方式管理残障数据资产及其底层系统。他们还将核准访问和使用这些系统的人员。

这些报告可能包括对以下方面的审查：

- 收集通知
- 安全性
- 其他事项，例如对系统和流程进行的独立审查。

### 我们的回应

联邦机构合作伙伴对此表示同意。

我们将制定残障数据资产及其底层系统的合规框架。该框架将有助于评估和报告个人和组织是否遵守各项协议和安全义务，其中包括总协议（Head Agreement）、双边附表（Bilateral Schedules）和多边数据共享协议（Multilateral Data Sharing Agreement）。

该框架还将建立在以下基础之上：

- 其他保证文件：例如法律授权框架（Legal Authorisation Framework）和数据监管框架（Data Governance Framework）
- 现有要求：例如，《数据可用性和透明度法》体系下的规定。

我们将在 2024 年 10 月之前完成此项工作。