Chinese (Simplified) | 简体中文

有关《2023 年隐私影响评估报告》的摘要

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）负责监督对该系统的使用。

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?

隐私影响评估（Privacy Impact Assessment，以下简称为 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。

Maddocks 撰写了一份详细的 PIA 评估报告。本文件是该报告的摘要，其中包括评估的流程以及有关评估结果和建议的摘要。

更多信息请参阅国家残障数据资产网站上的 Privacy for the National Disability Data Asset（国家残障数据资产中的隐私保护）页面。

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《澳大利亚隐私原则》（Australian Privacy Principles）——这些法律是关于如何管理个人信息的法律
- 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。

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。超过 150 人参加了意见征询会议。澳大利亚视听障碍协会（Deafblind Australia）帮助我们举办了两场面向残障人群的会议。在澳大利亚唐氏综合征协会（Down Syndrome Australia）的帮助下，澳大利亚包容组织（Inclusion Australia）为智力障碍人群举办了一场会议。

Maddocks 根据反馈意见撰写了一份详细的《意见征询报告》。该报告的摘要可在 Privacy for the National Disability Data Asset（国家残障数据资产中的隐私保护）网页上查看。

评估结果摘要

在意见征询会议上，人们告诉我们，他们大力支持开发残障数据资产。有些人指出，在未经授权的情况下，有关个人健康状况或残障情况的信息一旦被共享，将会给受影响的人带来严重后果。

澳大利亚的广大群众认为，相比其他个人信息，敏感信息应该得到更多保护。敏感信息可能包括有关个人的健康、种族或民族出身和宗教信仰的信息。您可以在 Privacy Act（《隐私法》）第 6 节和 Office of the Australian Information Commissioner（澳大利亚信息专员办公室）网站上找到更多信息和示例。

Maddocks 指出，联邦机构合作伙伴在设计残障数据资产时非常注重保护隐私。在监管工作方案方面尤其如此，做到了强效有力、缜密周到。监管工作方案指的是有关项目决策人员以及决策方式的规则。规则和流程经过精心设计，可以管理项目的数据和隐私风险。这包括发现未来的风险。

联邦机构合作伙伴将制定措施来保护个人信息。在进行各类数据的联动时，保护措施包括：

- 使用详细的数据共享协议
- 遵守有关数据共享方式的法律，包括 Data Availability and Transparency Act 2022（《2022 年数据可用性和透明度法》）
- 对联动数据中共享的内容制定规则。例如，发布研究结果之前要先进行审查。

我们将对残障数据资产中的所有数据进行去识别化处理，以确保没有人能够从中识别个人的身份。但利益相关者在意见征询会议上指出，数据联动可能会引发风险，导致个人身份重新变得可以识别。随着更多数据被添加到残障数据资产中，这种重新识别的风险可能会增加。

Maddocks 建议采取一些方法来应对这种风险并改善对个人隐私的保护方式。

建议

PIA 报告中的建议涉及以下主题：

1. 有关今后向残障数据资产添加数据集的原则
2. 数据提供方的收集通知
3. 管理重新识别数据的风险：对流程进行审查
4. 管理重新识别数据的风险：有关共享内容的规则
5. 管理数据泄露
6. 制定合规框架

欲知更多信息，请参见《附录：详细建议》。

附录：详细建议

澳大利亚隐私原则（Australian Privacy Principles，以下简称为 APP）共有 13 条，是 Privacy Act（《隐私法》）中有关管理个人信息的规则。每条建议内容后面都会列出与之相关的 APP。您可以在澳大利亚信息专员办公室的 Australian Privacy Principles（澳大利亚隐私原则）网页上找到有关 APP 的更多信息。

建议 1：有关今后向残障数据资产添加数据集的原则

背景

《国家残障数据资产章程》（National Disability Data Asset Charter，以下简称为《章程》）制定了强有力的原则和规则，用于管理残障数据资产的使用方式。该章程由残障社区起草，并将获得理事会和残障事务部长的批准。

同样重要的是，为了在向残障数据资产中添加数据集时有章可循，要制定相关的明确规则。数据集是信息、记录和事实情况的集合。

建议的方法

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。

Maddocks 建议这些原则至少应该包含以下考虑因素：

- 添加新数据集的公共利益：可以制定对公共利益进行评估的指导方针，例如检验添加数据集是否有利于残障群体
- 新数据在残障数据资产中有多大用处：只有在经批准的研究项目可能会使用新数据时，才可将相关数据添加到残障数据资产中
- 新数据集内信息的类型及其使用限制：例如，是否包含敏感信息，即使《隐私法》并未将其定义为敏感信息
- 该数据是否包含有关原住民或其他弱势群体的信息。

相关 APP

- APP 1：对个人信息进行公开透明管理
- APP 3：个人信息的收集
- APP 6：使用或披露个人信息
- APP 11：个人信息的安全性

建议 2：数据提供方的收集通知

背景

我们会通过各种合法手段，将数据添加到残障数据资产中。这将取决于数据提供方的数据收集方式。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。有些数据可以在未经个人同意的情况下合法地共享到残障数据资产中。

隐私原则中比较重要的一条是确保人们知道自己的个人信息将如何被使用和共享。

建议的方法

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。

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。

相关 APP

- APP 1：对个人信息进行公开透明管理
- APP 3：个人信息的收集
- APP 5：信息收集通知

建议 3：管理重新识别数据的风险：对流程进行审查

背景

《章程》草案中拟定了各项原则，其中一条是确保数据的私密性和安全性。残障数据资产将仅包含去识别化的信息。但有些人指出，这些数据存在被重新识别的风险，而且风险会随着时间的推移而增加。

建议的方法

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。

相关 APP

- APP 6：使用或披露个人信息
- APP 11：个人信息的安全性

建议 4：管理重新识别数据的风险：有关共享内容的规则

背景

如果残障数据资产中的信息被重新识别，则可能对受影响的人造成更大的伤害。原因之一在于构成残障数据资产的信息类型，原因之二是残障数据资产包含了有关弱势群体的信息。

根据数据监管框架（Data Governance Framework），我们将制定有关数据去识别化的政策。该框架是一套规则，旨在确保以安全、有保障、符合道德与法律的方式共享、管理和使用数据。

建议的方法

Maddocks 建议，任何去识别化政策都应明确指出：

- 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。

该政策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。

相关 APP

- APP 6：使用或披露个人信息
- APP 11：个人信息的安全性

建议 5：管理数据泄露

背景

各政府机构共同合作管理残障数据资产及其底层系统。这意味着数据泄露的风险可能会增加。同时，无法迅速应对数据泄露事件的风险也可能会增加。

根据数据监管框架，我们将制定数据泄露应对计划（Data Breach Response Plan）。计划中的措施包括做好有关数据与隐私泄露和事件的记录，以及每年进行一次审查。

建议的方法

Maddocks 建议数据泄露应对计划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。该计划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。

该计划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。

相关 APP

- APP 11：个人信息的安全性

建议 6：制定合规框架

背景

我们将制定一系列规则和流程（包括数据共享协议）来管理残障数据资产。我们将根据数据监管框架制定计划，对底层系统进行审计和审查。

建议的方法

Maddocks 建议董事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。

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。

相关 APP

- APP 1：对个人信息进行公开透明管理
- APP 6：使用或披露个人信息
- APP 11：个人信息的安全性

了解更多

联邦机构合作伙伴对《2023 年隐私影响评估报告》中提出的 6 项建议均做出了回应。您可以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）页面阅读对该报告的回应。