Chinese Simplified

information and privacy commission new south wales

信息介绍

2023年11月

MNDB计划常见问题解答

本文为谁提供信息?	本文供新南威尔士州的公众了解有关数据泄露强制通报计划(Mandatory Notification of Data Breach Scheme 简称：MNDB计划)的详情。
为什么这些信息很重要	本资料帮助你详细了解数据泄露强制通报计划，以及你在受到数据泄露事件影响后可行使的权利。

什么是数据泄露强制通报计划?

新州公共机构在发生数据泄露事件并且该泄露属"须通报事件"时，必须依据《1998年隐私和个人信息保护法》(Privacy and Personal Information Protection Act 1998, 简称：PPIP法）规定通报。

MNDB计划何时生效?

MNDB计划于2023年11月28日正式生效施行。

MNDB计划适用于哪些机构?

MNDB计划适用于新州公共部门的机构、部长办公室、大学、地方议会政府，以及不受联邦隐私法管辖的州政府所有企业。

什么是数据泄露应对政策?

数据泄露应对政策 (Data Breach Policy，简称：DBP) 由一系列书面政策或计划组成，规定了公共机构在发生数据泄露事件后应该采取的应对措施。法律规定所有公共机构必须制定各自的DBP。DBP必须确定公共机构内部人员在管理数据泄露方面的角色和职责，以及在数据泄露事件发生时应该遵循的处理步骤。

公共机构必须确保公众能够自由获取其DBP。换言之，公共机构需要在网站上发布DBP。

什么是须通报数据泄露事件?

MNDB计划规定，任何公共机构在发生属于须通报数据泄露事件后，必须向隐私专员(Privacy Commissioner)报告。

有以下情况的数据泄露即属于"须通报事件"：

- 未经授权访问或披露公共机构持有的个人资料，并可能对此等资料涉及的个人造成**严重伤害**。
- 疑似在未经授权访问或披露的情况下导致公共机构持有的个人资料承受损失，并可能对此等资料涉及的个人造成**严重伤害**。

什么是严重伤害?

严重伤害可以包括身体、经济或物质伤害，情感或心理伤害，或名誉伤害。伤害导致的影响因人而异，但是可能包括：

- 因诈骗造成经济损失；
- 可能带来有害身心健康的风险，例如受到来自曾经施虐的前伴侣的伤害；
- 因个人身份资料遭到盗窃而影响你的财务以及/或者信用记录；
- 严重损害个人名誉。

为何会发生数据泄露?

笼统而言，人为错误、系统故障，或恶意及违法网络入侵等，都可能导致数据泄露。

哪些情况可能导致数据泄露?

部分导致数据泄露发生的情况包括：

人为错误：

- 信件或电子邮件发送给错误的收件人；
- 错误地向未经授权或密码保护不足的人员授予系统访问权；
- 文件档案、手提电脑、USB或电话等储存有个人资料的实物资产丢失或放错地方。

系统故障：

- 编程错误，导致无需身份验证即可访问系统或自动生成通知；
- 没有弥补系统的已知漏洞或使用支持补丁予以维护。

恶意或违法入侵：

- 勒索软件、恶意软件、黑客攻击、网络钓鱼、暴力破解攻击等网络事件；
- 利用社会工程或冒充手法，导致个人资料不恰当地受到披露；
- 来自机构内部的威胁，包括雇员使用有效登录凭证，在其职权或授权范围之外调用或披露其他人的资料。

公共机构是否必须通知隐私专员？

如果经评估数据泄露属须通报事件，相关机构必须立即使用IPC网站提供的专用表格，通知隐私专员。

须通报数据泄露事件发生后，我是否会收到通知？

如果公共机构确定其发生的数据泄露属须通报事件，并涉及你的个人资料，则必须尽快通知你。这意味着，公共机构必须以书面形式向你告知数据泄露事件，同时提供相关信息，包括：

- 该机构已经采取或计划采取的行动，从而控制或减少对你造成伤害；
- 你在数据泄露事件发生后应该考虑采取的应对措施；
- 如何要求对公共机构的行为进行内部审查或如何向隐私专员提出投诉的信息。

我将在数据泄露事件发生多长时间后才会收到通知？

当公共机构有合理的理由怀疑资料可能遭到泄露，并且该泄露属于须通报事件，他们必须采取以下措施：

- 尽一切合理努力，遏制违法行为；
- 评估该机构在过去30天内是否存在未经授权的系统访问、信息披露或个人资料遭受损失的情况；
- 评估过去30天内是否有可能对任何受影响的个人造成了严重伤害；
- 尽一切合理努力，减少疑似违法行为造成的损害。

如果完成上述步骤后，公共机构确定其发生的数据泄露属于须通报事件，同时你的个人资料受到影响，则必须尽快通知你。

公共机构没有我的联系详情而无法通知数据泄露事件，我应该怎么办？

MNDB计划赋予各公共机构共享信息的权力，从而使他们能够向另一个公共机构索取相关的个人资料。公共机构仅可要求获取用于确认受数据泄露事件影响的个人的姓名及其联系方式等合理必要的信息。

但是，如果发生数据泄露的机构无法直接通知你，他们必须在其网站上发布通知，同时采取合理措施广而告之。通知必须在机构的公共通知登记档案页上保留至少12个月。

公共机构是否可有任何理由不通知我？

是的。在部分例外情况下，公共机构可以不通知受数据泄露事件影响的个人。例如，涉事机构迅速采取补救措施，并由于这些措施致使数据泄露可能没有造成严重伤害。在这种情况下，他们无需通知任何受影响的个人。

涉事机构通知我之后是否还会提供其他帮助？

取决于数据泄露事件的具体情况，涉事机构在通知你之后，还有可能提供其他类型的协助和支持。例如：

- 协助更换驾驶执照等受数据泄露事件影响的政府官方身份证件或文件；
- 提供保护个人信息的建议；
- 提供其他支持以及辅导服务。

我收到通知后应该做些什么？

你可以采取一些具体实用的措施，保护你的个人资料，并降低数据泄露事件可能为你带来的伤害风险。这些措施将取决于数据泄露发生的情况以及事件所涉及的资料类型。你收到的通知应该建议可以针对已获识别的泄露资料类型采取哪些行动。

如果你需要获得有关数据泄露事件的详情，或希望了解如何更好地保护自己的个人信息，可以联系向你发出通知的机构。

如何获得更多信息?

你可以在信息和隐私委员会 (IPC) 的官方网站上找到更多信息以及其他资源。你也可以通过以下方式联系IPC。

获取更多信息

联系新州信息和隐私委员会 (Information and Privacy Commission NSW - IPC):

免费电话: 1800 472 679

电邮: ipcinfo@ipc.nsw.gov.au

网址: www.ipc.nsw.gov.au

注意: 本文信息仅供参考。个人应该就具体情况获取法律建议。