Lookout, Inc.

Lookout for Work 应用程序

隐私权声明

生效日期：2023 年 4 月 1 日

原发日期：2016 年 10 月 24 日

Lookout for Work 应用程序隐私权声明

Lookout, Inc.（“Lookout”、“我方”或“我方的”）坚信您的隐私与安全同等重要，因此，对于为保护您的设备及您雇主的安全而收集到的数据，我方希望您完全知情。Lookout 会向您提供本“企业隐私权声明”（“声明”），以说明我方对 Lookout for Work 应用程序（“服务”）的信息处理方式。本声明适用于您在移动设备上安装和激活我方服务时，我方从您那里收集到的或与您相关的数据。下载并激活此服务，即表示您承认本声明中所述的数据收集、使用、披露和存储方式。Lookout 从您那收集到的任何信息（Lookout 在您使用此服务的过程中收集的信息除外）均受另一份隐私权声明约束。

如您的任职机构 (1) 要求全部或部分员工安装该等服务或 (2) 要求全部或部分员工安装含该等服务的移动设备管理套件，您可能已按指示下载并安装过该等服务。请理解，除非本声明另有明确规定，否则本声明仅适用于有关此服务的信息处理方式。如您对您的雇主（“雇主”）或移动设备管理提供商（“MDM 提供商”）的数据收集、使用、披露和安全处理方式有疑问或要求，或对我方代表您雇主收集的数据有疑问或要求，您应向当事方提出这些疑问或要求。

Lookout 有权随时更改本声明，以反映法律、数据收集方式及使用方式、服务功能或技术进步方面发生的变更。如我方对本声明作重大变更，我方将尽力通知您。如您对本声明中的信息有所异议，则请停止使用此服务。

我方已在本声明中加入相应的详细说明，以解答有关此服务的常见问题。本声明包含以下问题的答案：

1. **何为 Lookout for Work 应用程序？**
2. **Lookout 会从用户的移动设备中收集哪些数据？**
3. **Lookout 是否会阅读或查看本人的电子邮件或查看本人照片？**
4. **Lookout 是否会在移动设备之外收集有关本人的其他任何数据？**
5. **Lookout 何时收集本人移动设备上的数据？**
6. **Lookout 如何使用从本人移动设备上收集的数据？**
7. **Lookout 是否与其他人共享本人的数据？**
8. **Lookout 是否将我的个人信息出售给其他人?**
9. **哪些信息是本人雇主看不到的？**
10. **您是否会将本人的数据用于营销目的？**
11. **Lookout 如何保护本人数据以及会将其保留多长时间？**
12. **Lookout 在哪里存储本人数据？**
13. **本人有哪些数据权利和选择？**
14. **本人如有其他问题，该如何联系贵方？**

1. 何为 Lookout for Work 应用程序？

Lookout for Work 应用程序是一种移动安全解决方案，可保护移动设备和企业，使其免受威胁并避免违反公司政策。Lookout 会利用由逾 1 亿个传感器组成的全球传感器网络，通过使用机器智能识别无法通过人工分析得出的复杂风险模式，以做出安全预测。当检测到威胁时，Lookout 会为员工和管理员提供补救措施（例如，卸载应用程序、调用条件式访问权限）。

2. Lookout 会从用户的移动设备中收集哪些数据？

为保护您的移动设备和雇主，使其免受威胁，Lookout 会从您的设备中收集特定类别的数据。此类数据可能包括：

- **分析数据**，用于在您的设备上分析产品性能，
- **应用程序数据**，包括您移动设备上安装的所有应用程序的元数据（包括但不限于应用程序的名称和版本），在某些情况下，我方还会收集该应用程序的副本；
- **配置数据**，例如您的设备是否配置为具有 root 访问权限或是否已删除设备的硬件限制；
- **设备数据**，包括设备以及您移动设备上的 MDM 标识符；
- **固件/操作系统数据**，包括您移动设备的制造商和设备型号、您移动设备的某些技术设置（包括您移动设备的显示器尺寸和固件版本）以及您移动设备上的操作系统类型和版本；
- **识别数据**，例如，除非您的雇主使用我方服务中的隐私控制功能，否则我方会随机收集您的电子邮件地址；
- **网络数据**，包括您移动设备所连接网络的元数据（包括但不限于网络 SSID 或网络设备的唯一 MAC/BSSID 地址）以及 IP 地址（可指示您所在国家/地区以及地理位置）；
- **Web 内容数据**，包括恶意内容的 URL 和域，以及需进一步分析的内容。

请注意，我方提供服务前需获取特定类型的信息。如您没有向我方提供此类信息，或要求我方删除此类信息，请勿再访问该等服务。

3. Lookout 是否会阅读或查看本人的电子邮件或查看本人照片？

不会。Lookout 仅收集您设备上应用程序的相关元数据或应用程序本身的元数据。Lookout 不会收集您输入到应用程序中的用户数据。鉴于 Lookout 不会收集您输入到移动设备应用程序中的任何用户数据，Lookout 不会收集、阅读、查看或扫描您的电子邮件或短信。Lookout 不会收集您的照片或视频，但可能在本地设备上扫描此类文件，保护您不受照片或视频文件中隐藏的某些威胁侵害。

4. Lookout 是否会在移动设备之外收集有关本人的其他任何数据？

您的雇主为启用该等服务，会向 Lookout 提供您的电子邮箱地址。如在该等服务中组合提供 MDM 解决方

案，启动隐私权控制功能，即使 Lookout 可通过 MDM 访问您的电子邮箱地址，Lookout 亦不会收集您的电子邮箱地址。

如您将该等服务安装到 MDM 提供商产品中，我方亦可从 MDM 提供商处收集或访问包含您电子邮箱地址的信息。请与适当的 MDM 提供商联系，了解该提供商的隐私处理方式。

如您直接联系我方，向我方提供您的其他信息，并自愿披露此类信息，Lookout 亦可收集此类信息。

5. Lookout 何时收集本人移动设备上的数据？

在您下载、安装并激活该等服务后，Lookout 将立即开始收集您设备上的数据，确保其不受威胁且符合公司政策要求。鉴于您在移动设备上安装或访问应用程序，我方将扫描该等应用程序，查找潜在的安全威胁。

6. Lookout 如何使用从本人移动设备上收集的数据？

我方会将收集到的数据用于各种商业用途。举例来说，我方可使用从您移动设备上收集的数据检测您和/或您雇主是否受到任何威胁，以改进我方服务以及我方的其他产品。我方还可将从您移动设备上收集的数据与从第三方处收集的数据结合起来，改进我方服务。该数据属于假名数据。如我方的分析结果可公开分享，我方将汇总该等分析结果并对其作假名化处理，保护您以及您雇主的隐私。我方使用您信息的方式将取决于下述数据类型：

- **应用程序数据。**我方在使用该数据提供服务之前，会扫描应用程序文件来确定是否有恶意应用程序。在分析您移动设备上的应用程序时，如遇到以前尚未分析过的应用程序，我方会下载该应用程序的部分或全部副本，以便分析和确定其是否有风险，这具体取决于您雇主配置该等服务的方式。如第 3 节所述，我方在下载应用程序副本时，没有收集您输入到应用程序中的任何用户数据。
- **配置数据。**我方会分析您设备的配置数据，确定您的设备是否已被修改、破坏或配置是否安全，例如受感染、被刷机或破解或未设置密码。
- **设备数据。**我方使用设备或 MDM 标识符，协助您匹配您的设备与第三方系统中的设备（例如移动设备管理解决方案），我方将借助该系统报告您的设备是否遇到了任何威胁。
- **固件/OS 数据。**Lookout 使用该信息识别被攻破的固件和操作系统，并在设备有安全更新时通知您。
- **识别数据。**当我方通知您的雇主，您遇到威胁时，我方可能会选择收集您的工作邮箱地址，协助提供背景信息。未经许可，我方绝不会向您发送电子邮件。
- **网络数据。**攻击者可能会使用 Wi-Fi 等互联网连接来窃取数据，即中间人攻击 (MitM)。我方可使用 SSID 协助识别此类 MitM 攻击。Lookout 可能还会使用您的 IP 地址来粗略估计您所在国家和地区，但 Lookout 不会读取、存储或传输用户的实际设备位置 (GPS) 数据。我方会对数据作假名化处理并汇总该信息，按区域显示应用程序的普及程度，并执行移动威胁分析。为保护数据隐私，该信息将保留为假名信息。

- Web 内容数据。Lookout 会使用 VPN 接口分析设备上的流量是否受到威胁，阻止访问恶意网站或网络钓鱼网站，VPN 接口是我方安全浏览功能的一部分。我方不会将您的流量内容和历史记录共享给您的雇主，只有当您受到威胁时我方才会通知您的雇主。

根据《通用数据保护条例》，本声明中，使用您信息的法律依据将取决于您与雇主之间的关系以及雇主的用例，包括：(a) 为履行我们双方在任何合同项下的义务而有必要使用您的个人信息（例如，为确保您的雇主履行其雇佣合同，或确保 Lookout 遵守您在下载和使用我方应用程序后接受的服务条款）；或 (b) 履行合同并非一定要使用您的信息，但出于我方的合法权益或雇主或其他方的合法权益考虑，有必要使用您的信息（例如，为确保服务的安全、运营该等服务、确保我方和您雇主的工作人员及其他人员的工作环境安全、支付和收取相关款项、防止欺诈以及了解我方服务的客户）；以及遵守法律要求，例如提出适当数据安全要求的法律。

7. Lookout 是否与其他人共享本人的数据？

作为一种企业产品，Lookout for Work 会与您的雇主或经其授权，有权查看此类数据的任何人共享特定数据。雇主或其授权人员有权通过服务仪表板，访问有关您移动设备的安全信息。您的雇主会看到您的设备属性，例如设备型号和运营商。您的雇主会看到我方确定为恶意的应用程序，以及违反您雇主的适用公司政策的应用程序。请联系您的雇主，了解违反适用公司政策会给您造成的影响。

如您通过 MDM 提供商安装并激活我方服务中的一项产品，我方可能会与该 MDM 提供商共享您移动设备的安全状态和激活状态。

我方可能会与我方公司群中的其他成员以及经我方聘用，代表我方执行业务相关职能的服务提供商或合作伙伴等第三方共享您的任何数据。上述服务提供商可包括提供以下服务者：(a) 提供客户、技术或运营支持；(b) 履行订单以及满足用户或雇主的要求；(c) 托管我方服务；(d) 维护数据库；(e) 分析数据，改进和增强产品；以及 (f) 以其他方式支持或营销我方服务或任何其他 Lookout 产品。我方可能会披露您的有关数据，回应收到的任何传票、法院命令或其他法律程序，或确立或行使我方的合法权利，或抗辩法定求偿权。如我方收到地方、州、联邦或外国执法机构的信息申请，我方将尽力将该等申请传输给您的雇主，由其作相应处理，但我方保留在认为有关申请合法适当的情况下，直接回复并提供申请信息的权利。如我方以诚信的态度认为，为调查、防范可能的非法活动、涉嫌欺诈行为、可能威胁人身安全的情况、违反本声明、许可协议或最终用户服务协议的情况，就此采取应对措施，和/或保护 Lookout、我方员工、用户和公众的权利和财产，可适当披露您相关的任何信息，则我方可作此披露。这可能涉及与执法机构、政府机构、法院和/或其他组织共享您的信息。

我方可能会在任何合并、重组、出售我方部分或全部资产或另一家公司融资或收购我方全部或部分业务时，共享您的任何相关数据。

8. Lookout 是否将我的个人信息出售给其他人?

否。Lookout 不会出售其用户的个人信息（据我们所知，该术语将由加州消费者隐私法案定义）。如上文第

6 节所述，我方还可能将从您移动设备上收集的数据与从第三方处收集的数据结合起来，改进我方服务，但这些数据是假名的，不包含任何个人信息

9. 哪些信息是本人雇主看不到的？

Lookout 仅会将可确保您的设备不受威胁并符合公司安全策略的必要信息共享给您的雇主。举例来说，Lookout 不会让您的雇主查看您的电子邮件内容、浏览历史记录、联系人、日历、短信、已安装的非恶意应用程序（除非使用此类应用程序违反了您雇主的任何适用的公司政策），亦不会允许其跟踪您的位置。

10. 您是否会将本人的数据用于营销目的？

我方不会使用从您的移动设备上自动收集的数据来向您销售产品，亦不会出于营销目的与第三方共享该数据。我方可能会汇总从您的设备上收集的信息供研究用，并就移动设备的安全性及其面临的威胁发表见解。在该等情况下，应对研究中的汇总信息作假名化处理。

11. Lookout 如何保护本人数据以及会将其保留多长时间？

我方已采取合理的管理、技术和实体安全措施，可防范未经授权访问、破坏或更改您的信息。该等保护措施旨在应对我方收集、处理和存储的信息的敏感度，满足当前技术水平的要求。

尽管我方采取了适当措施，防止未经授权披露信息，但由于互联网传输方法或电子存储方法并非 100% 安全，我方无法向您保证，我方一定会以符合本声明要求的方式披露我方收集到的信息。

我方的政策是，仅在向您和他人提供服务所需的合理范围内或根据其他法律合规要求保留个人数据。如您的帐户属于不活动帐户或我方服务条款另有规定，我方可能会在 60 日后删除您的数据。但为备份和业务连续性目的而制作的副本中还会保留相关信息。在这种情况下，可使用 256 位静态加密来保护数据。

12. Lookout 在哪里存储本人数据？

Lookout 总部位于旧金山，其服务器位于美国。美国境外用户的个人数据会被传输到美国。如您在美国境外使用该等服务，您的信息将被传输并存储到我方服务器所在地及数据库运营地美国，亦将在美国进行处理。我方还可能会将您的信息传输到 Lookout 或我方关联方、子公司和服务提供商运营所在的其他国家/地区。

这些国家/地区的数据保护法可能与您所在国家/地区的法律不同，在某些情况下，保护力度可能不同。但是，无论我们在何处传输和处理您的信息，我们都会采取措施确保您的个人数据按照本通知和适用的数据保护法得到保护。如果您是欧洲经济区 ("EEA")、英国或瑞士的居民，我们会使用各种法律机制来帮助确保您的个人数据和权利得到保护，包括欧盟委员会批准的向第三国传输个人数据的标准合同条款。

Lookout 还通过美国商务部制定的关于收集、使用和保留来自欧盟、英国和瑞士的个人数据的 欧盟-美国隐私护盾和瑞士-美国隐私护盾 框架，进行了自我认证。制定这些框架是为了使公司在将个人数据从欧盟、英

国和瑞士传输到美国时遵守数据保护要求。要了解更多关于隐私护盾，并查看我们的隐私护盾认证，请访问：http://www.privacyshield.gov。

作为隐私护盾认证组织，Lookout 在从欧盟、英国和瑞士向美国传输个人数据时遵守隐私护盾原则。根据隐私护盾原则的要求，当 Lookout 在隐私护盾下接收信息，然后将其传输给作为 Lookout 代理的第三方服务提供商时，如果 (i) 代理以不符合隐私护盾的方式处理信息，并且 (ii) Lookout 对造成损害的事件负责，则 Lookout 在隐私护盾下负有一定责任。

如您对 Lookout 的隐私处理方式有任何疑问或投诉，包括隐私护盾相关问题，您可通过"如有任何疑问或疑虑，请联系我方"中载明的电子邮件地址或邮寄地址，联系我方。我方将与您一起解决问题。

13. 本人有哪些数据权利和选择？

如果您是欧洲经济区、英国或瑞士的居民，那么根据一般数据保护条例 ("GDPR")，您可能拥有以下权利：

- **访问。**您有权要求获得我们正在处理的有关您的个人数据的副本。如果您需要额外的副本，我们可能需要收取合理的费用;。
- **矫正。**您有权要求更正我们掌握的关于您的个人数据中的任何错误，无论是不完整的，还是不准确的；
- **删除。**在某些情况下，您有权要求删除与您有关的个人数据，例如我们不再需要这些数据，或者您撤回了同意（如适用）；
- **可移植性。**您有权以结构化、常用且机器可读的格式接收您提供给我们的有关您的个人数据，并有权在特定情况下将该数据传输给第三方；
- **反对。**您有权 (i) 随时反对出于直接营销目的处理您的个人数据; (ii) 反对我们处理您的个人数据，如果此类处理的法律依据是我们或第三方追求合法利益所必需的。
- **限制。**您有权要求我们在某些情况下限制对您的个人数据的处理，例如当您质疑该个人数据的准确性时；
- **撤销同意。**如果我们以您的同意（或明确同意）作为处理您个人数据的法律依据，您有权随时撤销该同意。

如果您希望行使这些权利，请联系您的雇主。 如果 Lookout 是数据控制者，您也可以使用下面的联系信息与我们联系，以行使这些权利。在适当的情况下，我们可能会将请求发送给雇主，并按照他们的指示处理。我们将在不迟于 30 天内及时回复您的请求但是，在某些情况下，Lookout 可能无法访问或删除其保存的所有个人数据。

此外，如果您是欧洲经济区、英国或瑞士的居民，并且就您对我们的隐私做法表示担忧，我们解决此担忧的方式不满意，您可以免费从我们指定的隐私保护独立申诉机制寻求进一步的帮助，您可以访问 https://www.jamsadr.com/eu-us-privacy-shield了解更多信息。您还有权向相关监管机构提出投诉。但是，我们鼓励您先与我们联系，然后我们将尽最大努力解决您的问题。欧盟居民也可以选择对未解决的投诉进行

有约束力的仲裁，但在启动此类仲裁之前，您必须：(1) 联系 Lookout，让我们有机会解决这个问题；(2) 向上述 Lookout 指定的独立追索机制寻求帮助；以及 (3) 联系美国商务部（直接联系或通过欧洲数据保护机构），给商务部时间尝试解决问题。欲了解更多有关私隐护盾有约束力的仲裁方案，请参阅 https://www.privacyshield.gov/article?id=ANNEX-I-introduction.各方应自行承担律师费。请注意，根据隐私护盾条例，仲裁员只能针对个人实施必要的非金钱的衡平法救济，以补救个人违反隐私保护条例的行为。Lookout 受制于美国美国联邦贸易委员会 (FTC) 的调查和执法权力。

根据适用法律，您可能拥有某些权利，包括《通用数据保护条例》和《加州消费者隐私法》。如果您希望行使这些权利，请联系您的雇主。 您也可以使用下面的联系方式与我们联系。

14. 本人如有其他问题，该如何联系贵方？

如您有其他问题，我方建议您联系您的雇主。您亦可直接将问题发送给我方的数据保护官，邮箱：privacy@lookout.com或寄信给 Lookout, Inc.，收件人：Michael Musi, Data Protection Officer, 3 Center Plaza, Suite 330, Boston, MA 02108.欧洲经济区的居民通过邮件联系我们 Lookout, Inc.，收件人：Wim Van Campen, VP, Sales EMEA, Florapark 3, 2012 HK Haarlem, Netherlands.