COVID-19 应用程序工具包

立法者、

政策制定者、

应用程序开发者、运营商、公共机构委托方以及

公众

如何参与推动制衡，并确保疫情期间部署的工具切合目的？

目录

前言

Covid-19（新冠肺炎）促使全球各国政府采取各种应对措施，从传统的流行病学措施，如强制佩戴口罩和保持社交距离，到前所未有的技术应对方案，其中接触者追踪和免疫护照应用最为引人注目。

出于对 Covid 具体干预措施的研究兴趣，民间组织发起 Covid 应用程序项目(Covid App Project)。该项目包含两个阶段。

第一阶段为 2021 年 7 月之前接触者追踪应用程序的使用情况，涵盖巴西、哥伦比亚、印度、伊朗、黎巴嫩和南非。该阶段从公共卫生效能的角度评估应用带来的影响，并分析其功能潜变与意外后果，如获取社会权利受限。共同的研究兴趣吸引六个民间社会组织聚集到一起：ALT Advisory（南非）、Internet Democracy Project（印度）、InternetLAB（巴西）、Karisma（哥伦比亚）、SMEX（黎巴嫩）和 United for Iran。数据权利机构 AWO 提供协调支持。[1]

第二阶段包含自 2021 年 7 月以来开发的技术应用程序，其中“免疫护照”（可显示疫苗接种情况、检测结果或康复证明）最为引人注目。通过对全球代表性的应用样本进行技术评审，该研究考察了世界各地的政策、法律与技术手段的趋势。11 款受到评审的 Covid 应用程序主要由政府开发（或委托开发），但也有些其他参与者，其中包括澳大利亚、巴林、智利、印度尼西亚、以色列、荷兰、突尼斯和西澳大利亚州。作为全球不同大洲/地区的代表，这些国家可以反映研究过程中观测到的主要趋势。另外一些应用的开发设计可视为具有全球性：世界经济论坛 (WEF) 的 CommonPass 与国际航空运输协会 (IATA) 的 Travel Pass。

第二阶段的成果如下：

- 《Covid-19 应用：政策、法律与技术趋势报告》（下称《趋势报告》）：[2]阐述第二阶段的发现和建议。从公共卫生效能、功能潜变程度与个人意外后果的角度，该报告对应用的设计和使用方式进行探讨。对于利益相关者，该分析提出一系列建议与最佳实践，可用于制定有效且可持续的公共卫生措施。

[1] 第一阶段的研究结果可在此处获取：https://www.awo.agency/latest/covid-19-app-project/
[2] 此处获取：https://awo.agency/files/Covid-Apps-Policy-Legal-Tech-Trends.pdf

- 《COVID-19 软件隐私风险报告（第二部分）》（下称《技术报告》）：[3]通过对 11 款选中应用的全面技术评审，该报告探讨其是否符合最佳数据保护实践，包括但不限于，内置隐私设计与数据最小化。另外，对于如何最好地确保 Covid-19 应用安全有效，也提出建议。

- 《Covid-19 应用工具包》（下称《工具包》）：[4]根据《技术报告》和《趋势报告》两者都着重强调的发现和建议，编写该工具包。对于上述六个民间社会组织在 Covid 项目第一阶段确认的调查发现，也予以吸收和借鉴。总的来说，该文档提供了全面的最佳实践与方便易用的指南和工具，以便所有利益相关者进行部署，其中包括疫情响应参与者和关注者：立法者、政策制定者、应用开发人员、运营商、公共机构委托方与公众。

该工具包所提建议的重点是：增强疫情响应措施，确保公共卫生效能。同时，为疫情响应利益相关者提供实用指南，防止在部署技术工具时出现功能潜变与意外后果。利益相关者可将该工具包作为良好实践和建议的基准，并根据自身特定情况进行调整，以反映和处理各自遇到的各种其他问题。

这些建议按照直接利益相关者划分，如对政策制定者和立法者的建议，但可适用于所有利益相关者。

最后，对于公众而言，为了增强与其息息相关事务的意识，熟悉该工具包中的趋势与建议是有益的，例如：关于新冠肺炎应用的隐私政策，公众应该了解什么。为了进一步增强这种意识，该工具包两个章节都在开头为终端用户提供摘要。以此阐明，公众对于疫情响应利益相关者可有哪些预期，如：相称性原则、尊重公众权利以及确保公共卫生效能。

为了确保全球读者的理解，该工具包另提供七种语言：

- 阿拉伯语[5]
- 波斯语[6]
- 法语[7]
- 印地语[8]

[3] 此处获取：https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf
[4] 此处获取：https://awo.agency/files/covid-app-toolkit-en.pdf
[5] 此处获取：https://awo.agency/files/covid-app-toolkit-ar.pdf
[6] 此处获取：https://awo.agency/files/covid-app-toolkit-fa.pdf
[7] 此处获取：https://awo.agency/files/covid-app-toolkit-fr.pdf
[8] 此处获取：https://awo.agency/files/covid-app-toolkit-hi.pdf

- 葡萄牙语（巴西）[9]
- 俄语[10]
- 简体中文[11]
- 西班牙语[12]

[9] 此处获取：https://awo.agency/files/covid-app-toolkit-pr.pdf
[10] 此处获取：https://awo.agency/files/covid-app-toolkit-ru.pdf
[11] 此处获取：https://awo.agency/files/covid-app-toolkit-zh.pdf
[12] 此处获取：https://awo.agency/files/covid-app-toolkit-es.pdf

1. 对政策制定者和立法者的建议

对于疫情响应的利益相关者，公众可有哪些预期及其为什么

根据公共卫生界的相关咨询和建议，政策制定者和立法者可制定政策与法律框架。对于公众，重点在于这些框架与保护措施能够确保：政策制定者和立法者的行为具有相称性并保证公共卫生效能。在开发和使用 Covid-19 应用时，相称性原则可推动制定并提供有效的保障，确保符合全球最佳实践，尊重公众权利。为了防止意外后果，更为广泛的协调性 Covid-19 策略是至关重要的。实际上，当 Covid 应用被国家当作一种疫情响应措施时，其公共卫生效能将成为上述策略的要素之一。

Covid-19 应用终端用户（包括难民和外来工等弱势群体）必须能够维持关键服务的使用权。整体性的公共卫生策略应易懂可用并值得公众信任。为了确保这一点，Covid-19 应用必须是更为广泛的实证性策略的要素之一。这表示，应用程序的引入符合全球技术标准，并且是中央与地方不同职能部门共同协作的结果。同时，应用的使用应与检测和追踪计划、社会政策和公共卫生政策（如社交距离）相结合。应用程序的使用应透明且协调一致，并结合（社交）媒体的外联工作，来增强公众相关的理解和意识。

最终，公众必须能够相信政府的响应措施，包括上述内容以及防止功能潜变或其他意外后果。可通过以下方式实现：制定并实施适当的法律制度、数据使用透明政策以及数据共享协议。同时，这些方式应仅用于支持公共卫生策略，而非实现其他政治或政策目标。为了进一步推动这种信任，可采取如下方式：确保公共卫生措施在全国范围内公平实施并受到独立监管，同时，制定非数字化替代方案，防止因未使用应用程序而遭受不公待遇。

公共卫生效能		
趋势 1		
在使用接触者追踪应用和技术性措施的国家，互联网和移动技术使用率较低或存在不平等	**评估**	虽然在互联网接入和移动技术方面预先存在着差异，许多政府在应对 Covid-19 时仍采用技术措施。由于智能手机普及率存在不同，可导致已有不平等的加剧并引发伦理问题，因此这一问题的严重性不言而喻。此外，社会保障服务主要通过在线平台提供，由于互联网接入较差或没有移动设备，弱势群体更可能被剥夺获得关键援助的机会。
	建议	对于弱势群体（特别是难民和外来工），国家当局应维持他们获取关键服务的权利。
	如何实施建议？	
	□ 对于关键互联网基础设施的分布情况，国家当局可通过现状调查确定待开发的领域。 □ 在已确定的待开发领域，投资关键互联网基础设施建设。比如手机补贴计划、免费 Wi-Fi 热点，甚至数字技能课程。	

<table>
<tr><th colspan="3">公共卫生效能</th></tr>
<tr><td colspan="3">趋势 2</td></tr>
<tr><td rowspan="4">应用程序常常与更为广泛的公共卫生措施脱节，并因使用率较低而受影响</td><td>评估</td><td>接触者追踪应用的成败，与国家和地方不协调的疫情响应措施密切相关。很大程度上，某些应用与相当松散的公共卫生策略脱节，而且政府未将有效使用数据放在首位。这也表示，应用程序等技术未能满足公共卫生系统的需求；当中央与地方缺乏数据共享时，这种情况尤为明显。因此有人认为：接触者追踪应用在某些国家只是例行公事，以此表明政府对疫情采取了技术措施。</td></tr>
<tr><td>建议</td><td>为了应对 Covid-19（或其他全球性流行病），国家当局应制定统一的政府响应措施，同时兼顾国家与地方各级政府。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 在制定更为广泛的公共卫生策略以及检测和追踪机制时，国家当局可将接触者追踪应用集成其中。与传统的检测和追踪系统一起使用，应用程序可实现最大功效，而这反过来依赖于充足的检测能力以及地方、区域和国家公共卫生部门的工作人员。

□ 决策基于实证，确保公共卫生应对措施相称且有效。</td></tr>
</table>

<table>
<tr><th colspan="3">公共卫生效能</th></tr>
<tr><td colspan="3">趋势 3</td></tr>
<tr><td rowspan="3">部署多个包含多种功能的应用程序</td><td>评估</td><td>在许多国家，各种接触者追踪应用的数量迅速增加。尤其当各地政府参与开发时，出现功能各异的多种应用程序。特别是一些州政府推出的应用，除了追踪接触者，还有其他功能，如远程医疗。机构之间的协调不足以及公共卫生系统的分散，有时可导致这一现象。在一些国家，Covid-19 接触者追踪应用存在多个官方版本，这可能降低整体的使用率。</td></tr>
<tr><td>建议</td><td>对于全球性流行病，国家当局应制定统一的政府响应措施，同时兼顾国家与地方各级政府。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 应对疫情时，确保政府机构与公共卫生部门协调一致。

□ 遵守接触者追踪应用的全球最佳实践标准，如 GAEN (Google Apple Exposure Notification)API，为开发可靠的基础设施提供支持。</td></tr>
</table>

<table>
<tr><th colspan="3">公共卫生效能</th></tr>
<tr><td colspan="3">趋势 4</td></tr>
<tr><td rowspan="4">公众信任和意识的缺乏，影响接触者追踪应用</td><td>评估</td><td>在所有受到评审的国家中，缺乏公众信任或意识，阻碍了接触者追踪应用的采用。这种情况的部分原因是应用的宣传不足，包括政府没有专注而目标明确地进行沟通。此外，对监控和隐私的担忧也影响了一些应用。一些国家历史上曾出现执法和情报部门对监控的滥用，这对记者、反对派领袖、法官和人权活动家造成了影响。</td></tr>
<tr><td>建议</td><td>在与媒体进行沟通或通过媒体进行宣传方面，国家当局应进行改善。专业严谨地提供相关信息，加强公民意识和教育。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 为了发挥接触者追踪应用的真正价值，必须做到：公众知道并信任它，同时对于用户数据的使用，公众信任所有相关参与者或利益相关者。[13]应用的设计符合全球最佳实践，防止功能潜变或数据泄漏，提高公众意识并推广应用。

□ 通过各级政府、公共卫生部门、媒体和私营机构，推动公众对于该应用的了解与使用。</td></tr>
</table>

[13] 根据数据保护法，这些参与者被称为数据控制者。该定义如下：“……根据国家法律，有权决定个人数据内容和使用的一方，无论此类数据是否由该方或其代理人收集、存储、处理或传播”。经济合作与发展组织（经合组织）（2013 年 7 月 11 日）。《理事会关于隐私保护和个人数据跨境流通指导原则的建议》（下称《经合组织隐私保护和个人数据跨境流通指导原则》）
访问链接：https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

<table>
<tr><th colspan="3">公共卫生效能</th></tr>
<tr><td colspan="3">趋势 5</td></tr>
<tr><td rowspan="4">相对于接触者追踪应用，替代措施对公共卫生影响更大</td><td>评估</td><td>虽然接触者追踪应用成为公众关注和讨论的对象，但替代措施往往具有更大的影响力。一些国家主要依靠大规模筛查、定向测试和封锁，而这些措施需要动员医务人员对数百万人进行筛查。同时，在防止 Covid-19 传播方面，国家封锁与隔离措施似乎至关重要。</td></tr>
<tr><td>建议</td><td>应对新冠疫情时，在应用程序等技术性措施之外，国家当局应制定非技术性的替代方案。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 增强公私部门合作和协调，确保医疗资源充足，以及将接触者追踪应用集成至更广泛的公共卫生策略，其中包括检测、追踪和无障碍测试。

□ 确保社会政策准备就绪，方便（可能受感染的）人们遵守政策和准则，例如，在封锁或隔离期间，提供经济支持防止疫情贫困。

□ 确保向公众提供个人防护装备（如口罩）。</td></tr>
</table>

功能潜变与意外后果		
趋势 1		
紧急状态法规作用有限，特殊权力的扩大使用	**评估**	在研究期间，并非所有调查国家都宣布国家紧急状态。对于进入紧急状态的国家，部署各种措施的法律依据来自国家宪法或法律框架的具体规定。这通常表示，在符合某些条件和规则的情况下，虽然违背常规人权标准，国家仍可行使权力。 然而，对于某些弱势群体，特别是防疫措施巩固并加剧已有歧视时，紧急状态将带来负面影响。对于未宣布紧急状态的国家，依赖于普通的立法规定来提供特殊权力。与紧急状态不同，因为这种权力源自现有法律，通常为公共卫生法。它允许实施某些措施，而无需关联紧急状态类别。这未必始终符合宪法或法律框架的明确规定，因此更可能扩大这一权力的使用而没有相应的制衡制度。
	建议	制定公共卫生措施时，应通过适当的法律文书，为个人权利提供有效保障，包括合法宣布紧急状态的情况。 在应对未来的危机时，国家当局应进行人权影响评估，这将成为定义法律框架的原则，其中包括对紧急和灾难状态的意见，以及什么是必要的与合理的。 与严重侵犯人权的处理流程类似，可取的方式是建立过渡机制，对 Covid-19 疫情期间形成的实践和规范的影响进行评审，同时推动问责与和纠正，避免例外成为常规。

	如何实施建议？
	□ 制定法规与政策，应对下一波 Covid-19 或新的全球流行病，减少需宣布紧急状态的必要性。 □ 因快速响应需宣布紧急状态时，必须包含日落条款，规定公共卫生新措施的严格时限。 □ 在执行现有（和即将实施的）公共卫生法律之前，进行人权影响评估。人权影响的评估必须透明，确保充分的尽职调查和公众信任。[14] □ 决策基于实证，确保公共卫生应对措施相称且有效。采取民主筛选与监督方式，利用政策和影响评估的全球最佳实践，防止例外状态的扩大。

功能潜变与意外后果		
趋势 2		
数据保护制度刚刚起步，有时尚未执行	**评估**	第一阶段的调查发现，疫情期间全面的数据保护法尚未生效，或者仍在立法阶段，或者根本不存在。通常，更为强大的数据保护制度能够加强对有关国家的监督。

[14] 如何评估人权影响，可在此处获取相关指南：https://www.business-humanrights.org/fr/big-issues/un-guiding-principles-on-business-human-rights/human-rights-due-diligence-impact-assessment/

	建议	加快数据保护法的生效进程。同时，这些法律应包含必要的条款，可以涵盖所有 Covid 相关应用和 IT 工具。 政府及其私人合作伙伴应确保监管与政策框架是为了保护权利且透明，尤其注重隐私权。 应审核数据保护相关法规，同时与现有的数据保护法保持一致。
	如何实施建议？	
	□ 对于应急响应的数据使用，制定或扩展数据保护框架，并且不引入新的风险。 □ 建立独立的数据保护机构，并制定严格的监督机制。 □ 数据保护法与邻国保持协调，并符合全球最佳实践。[15] □ 对于数据保护法的制定和/或更好的执行，非政府组织(NGO)、人权团体和其他组织应继续为政府提供支持。	

[15] 包括《经合组织隐私保护和个人数据跨境流通指导原则》和欧盟的《一般数据保护条例》（GDPR），此处获取：https://eur-lex.europa.eu/eli/reg/2016/679/oj

功能潜变与意外后果		
趋势 3		
公共机构之间数据共享在增加，但不透明	**评估**	公共机构在应对疫情时收集并分享数据，这是世界各地政府的常见现象。其目的主要是在实施隔离政策时促进并批准国内旅行。这包括组合现有数据集以及 Covid-19 特定生成的数据集。然而，人们常常因无法访问在线平台申请许可而旅行受限。执法机构可获取敏感的个人数据，同时缺乏全面的数据保护法或其他监管制衡，从而导致功能潜变与对某些弱势群体的不利影响。
	建议	对于共同处理疫情个人数据的公共机构和私人实体，应编写并发布影响报告，并将其作为主动透明与问责制度的良好实践。 所有应用程序都应提供关键的法律文档，如服务条款和隐私政策，并且这些文档应可供公众查阅。 提供明确的相关信息，包括：收集数据的类型和目的、数据储存的地点和时长、数据分享的对象和目的、以及所有这些功能的安全协议。 隐私政策应列出所有访问个人数据的第三方应用程序。
	如何实施建议？	

	□ 数据共享协议包含明确的日落条款。 □ 无论是购买或自愿共享，从私营部门获取数据时，应受到数据保护法和尽职调查的制约。 □ 制定并公布数据共享服务条款和隐私政策，公开有关何人如何使用何种数据的信息。 □ 隐私政策必须全面且易懂，并提供所有第三方应用的详细信息。
相关实施工具	
● 接触者追踪应用的隐私通知模板	

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 4</td></tr>
<tr><td rowspan="4">公众信任和意识的缺乏，影响接触者追踪应用</td><td>评估</td><td>在所有受到评审的国家中，缺乏公众信任或意识，阻碍了接触者追踪应用的采用。部分原因在于应用的宣传不足。政府未进行定向而专注的沟通，造成公众对某些应用的困惑。此外，一些应用所受影响源于对监控和隐私的担忧。</td></tr>
<tr><td>建议</td><td>公共机构应进行定向而专注的沟通，提供及时且准确的 Covid-19 信息。专业严谨地提供相关信息，加强公民意识和教育，从而改善公众对于措施和限制法规的反应。

公共机构应定期与民间社会进行透明、民主和科学的协商。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 为了真正地提升公共卫生效能，接触者追踪应用必须获得较大范围的公众接受，而这需要信任。建立并维持公众信任的关键在于，采用全球最佳实践标准（如数据最小化和用途规范）以及普遍防止功能潜变。请查阅该工具包下方的软件需求规范模板。</td></tr>
</table>

功能潜变与意外后果		
趋势 5		
歧视边缘群体	**评估**	在一些受到评审的国家，通过应用提供的功能，用户可举报本地大规模聚会和跨国旅行者，使得人们可向公共当局检举封锁违规者。然而，社会成员代表国家执行监视，并且国家未提供必须遵循的平等承诺，这可对边缘群体带来严重的后果。用户因此被赋予了一种机会，可用来不公地惩罚某些人乃至整个群体。 Covid-19 措施，尤其是国家封锁和边境严控，将影响所有人，但移民和难民面临着被排斥或被歧视的高度风险。正如在一些国家所见，政府常常无法很好地提供保障，以避免弱势群体遭受这些风险。出行限制，尤其是只能通过数字平台获取许可，让很多人无法正常活动。一些国家的案例表明，一些人在封锁期间甚至很难找到住处。同时，农村与非正规经济部门所面临的挑战因 Covid-19 而更加艰难，例如，供水不足和过度拥挤。此外，隔离营的使用引发争议，在其中隔离数周的移民没有接受 Covid-19 检测，也没有机会自我隔离。
	建议	公共当局应在全国平等地执行公共卫生措施。 主管当局应确保维持对弱势人群（如移民和难民）提供的服务，确保他们能够战胜因疫情造成的持续困难。这些服务包括获取医疗、经济援助和教育权利。

		公共当局应确保：即使没有使用 Covid 应用，任何人不会因此受罚，或者拒绝为其提供任何公共或私人服务。 公共卫生措施应得到影响分析的支持，这一分析评估了措施对于弱势群体可能造成的后果。
	如何实施建议？	
	□ 不可鼓励或要求公众举报 Covid 措施的“违规者”，因为这是公共当局的职责。 □ 在全国平等地执行公共卫生措施，确保执行和纠正机制具有独立监督。 □ 确保将移民和难民纳入公共卫生政策、社会保障以及其他支持体系。 □ 如果没有手机或不愿使用接触者追踪应用，确保为其提供纸质（非数字）替代品。 □ 确保持续地提供庇护申请以及清洁安全的住所，同时考虑新的选择，如入住酒店（因疫情而空置）。 □ 公共当局应进行人权影响评估，同时顾及对不同弱势群体的潜在影响。	

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 6</td></tr>
<tr><td rowspan="4">镇压抗议</td><td>评估</td><td>在一些受到评审的国家，对于因封锁和其他 Covid 相关措施造成的困难，国家和地方政府未提供足够的援助，因此爆发了抗议活动。在一些案例中，执法部门使用过度的武力镇压抗议，伤及儿童、病患和老人。

另一项国家评审清晰地显示，政府被指对疫情期期间的经济危机处理不当，导致了抗议升级。在全国封锁期间，因缺乏政府援助，波及许多人的经济衰退进一步恶化，这也导致抗议活动增加。当局试图镇压抗议，包括在全国封锁期间，导致示威活动与安全部队发生冲突，出现了人员伤亡。</td></tr>
<tr><td>建议</td><td>政府不应通过防疫政策来恐吓和镇压政治异见者，也不应利用这些政策来惩罚被关押的异见者。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 公共卫生政策和立法行为必须源于实证，并设定明确的防疫目标；在这些法规约束之下，保证社会与经济活动尽可能正常进行，基本权利充分行使。

□ 如果纠正机制尚不存在，应建立并维持这种机制，防止疫情期间基本权利受到侵犯。如果纠正机制已存在，应得到有效实施。</td></tr>
</table>

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 7</td></tr>
<tr><td rowspan="3">基于技术的 Covid-19 响应扩大数字鸿沟与不平等</td><td>评估</td><td>互联网和移动技术在使用方面存在差异，这对疫情期间个人获取社会权利造成影响。无法平等获取这些资源将扩大已有不平等，甚至引发伦理问题。这将造成严重的后果。此外，社会保障服务主要通过在线平台提供，因互联网接入较差或缺少移动设备，许多弱势人员可能被剥夺基本生活设施。然而，即使能够实际访问平台，其设计也存在负面影响，并且不限于弱势群体。例如，用户可使用多种地方语言，但接触者追踪应用仅提供英文。</td></tr>
<tr><td>建议</td><td>必须制作数字材料，并易于获取。这些材料必须易懂和实用，同时为使用相关的应用提供培训和工具，并强调关键的数据隐私问题。为政府职员、社区医务人员以及应用程序的用户提供数字技术培训。

对于出行请求和疫苗登记，公共当局应开发非数字化的替代方式。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 确保所有 Covid-19 响应政策和措施具有纸质的（和非数字化）的替代方案，包括但不限于：接触者追踪、接触者追踪应用程序和社会保障获取。

□ 处理远程教育问题。远程教育将对于经济困难的儿童造成不利。</td></tr>
</table>

	□ 确保政策和资助能够防止数字鸿沟，避免儿童之间出现（更大）差距。

公共卫生效能		
趋势 1		
缺少与实证性决策的互动	**评估**	应急政策或措施应具有坚实的底层逻辑，确保有效。对于 Covid-19 疫情，任何公共卫生干预应根据国家或地区的特定情况作出调整，并且依赖于相关科学研究。在制定 Covid-19 疫情响应的决策过程中，公共卫生机构和其他相关专家应参与进来。这在一些国家取得了不同程度的成功。
	建议	政府应确保相关关键基础设施已经到位，保证技术疫情响应措施尽可能有效。尤其是，对于移动应用或其他基于网络的服务，政府应建立互联网基础设施，以使互联网接入充分普及，能够支持相关干预所需的网络覆盖率。 公共卫生应急响应所用的技术措施，其底层逻辑应基于相关科学研究，确保能够有效应对突发事件。 公共卫生部门或相关专业机构应充分参与决策过程，以便决策者能够确保并展示这些措施是基于相关研究，并适合于特定的应急情况。
	如何实施建议？	
	□ 对于关键互联网基础设施的分布情况，国家机构可通过现状调查确定待开发的领域。	

	□ 在已确定的待开发领域，应投资建设关键互联网基础设施。比如手机补贴计划、免费 Wi-Fi 热点，甚至数字技能培训。 □ 在进行部署之前，政策制定者和立法者应向专家核实：该技术是否能为 Covid-19 防疫工作带来实际价值，还是会造成过多附带损害而无效。对于这种辩论的结果，应以建议的方式提交至下述的决策委员会。在任何情况下，这些建议都应公开发布。 □ 建立具有决策权的委员会，成员包括：独立的公共卫生机构（流行病学家）、技术专家、政策制定者和数据保护机构。确保该委员会所做的决策受到制衡。

公共卫生效能		
趋势 2		
公众对 Covid 措施所依赖的科学研究缺乏认识。	**评估**	在多数人看来，在世界各地快速传播的 Covid-19 是一种新的风险。政府和公民一样面对着陡峭的学习曲线。尤其是疫情早期，需要采取行动而认知有限。在许多地方，有关该疾病的阴谋论出现激增。越来越多的证据表明，社交距离、隔离和接种激励相关策略，都受到精心设计的公共宣传活动的强烈影响。在一些地方，这些宣传促使公众配合公共卫生措施，推动口罩缺乏时在本地生产，并提升接种意愿。
	建议	与民间社会的广泛民意代表建立“意愿联盟”。线上和线下的认知宣传活动，都能够推动公共卫生措施的遵守并防止失去信任。顾及不同的人口状况，特别是边缘群体；建立与群体中可信任代表的合作。
	如何实施建议？	

	□ 基于社区建立干预措施相关合作，有效提升边缘群体的认知。[16]

公共卫生效能		
趋势 3		
Covid-19 疫情期间，公共采购缺少能效	评估	一些法律框架规定快速采购流程，以便政府获得所需资源，快速高效地应对即将发生的紧急情况。然而，如果没有制定全面的快速公共采购流程，或者没有遵守，将出现一系列问题，包括必需设备的短缺。
	建议	对于紧急情况下的公共采购，制定永久而非临时的规则，确保更有效地获得货物或服务。 同时，可结合预先采购安排，快速获得相关紧急情况所需货物和服务。
	如何实施建议？	
	□ 参考《联合国国际贸易法委员会公共采购示范法》（下称《示范法》）或其他类似国际标准的相关部分，引入公共采购立法草案，特别关注极端紧急情况公共采购相关规定。这些规定可包括，例如： ● 应对灾难性事件时，因时间紧急无法使用其他采购方法，为了满足需求，允许从单一来源采购（参考《示范法》第 30.5(b) 条）。 ● 应与供应商谈判确定建议书和价格，情况不允许的情况除外（参考《示范法》第 52 条）。	

[16] 请参阅：https://apps.who.int/iris/rest/bitstreams/1277158/retrieve，https://www.ajtmh.org/view/journals/tpmd/105/4/article-p879.xml，https://www.cdc.gov/pcd/issues/2020/20_0408.htm

	● 在紧急情况下，可从某些供应商采购商品或服务，前提是在突发事件引发紧急状态之前国家与供应商达成了协议，并按照协议采购。

功能潜变与意外后果		
趋势 1		
部署和使用 Covid 应用时缺少法律框架	**评估**	在一些重点国家，部署 Covid-19 防疫应用和措施时，往往没有现成的法律框架来规范其使用，或批准国家机构创建和部署这些应用。在某些情况下，对于如何使用 Covid 应用所需的个人数据，相关法律并不存在。因为这些立法上的疏忽，功能渐变的可能性越来越大。这表示，国家机构可将这些措施和个人数据用于 Covid-19 之外的倡议。
	建议	实施全面的法律框架，为紧急响应措施的制定提供基础。应在国家宪法或法律体系中制定相关条款，来实施一种紧急状态：在有限时间内，紧急状态下的不同国家机关可调整职能，以此获得足够的监督和保障措施，来保护个人权利。
	如何实施建议？	
	□ 提出立法草案，制定以下条款： ● 行政当局/政府可在特定条件下宣布紧急状态，但规定只有通过州立法机构的批准方可宣布。 ● 立法和司法机关在紧急状态下保持监督。 ● 只有明确规定措施的性质和范围时，政府方可采取这些措施来应对紧急状态。 ● 紧急状态应对措施需符合现行法律，包括但不限于数据保护法。 ● 对于法律体系或宪法对个人权利的任何减损，政府应保证其符合相称性原则。 ● 为了应对紧急状态而部署的措施，应接受立法机构的事后审查并获得批准。	

	• 紧急状态以及部署的应急措施必须遵守严格的时间限制，任何延期都必须事先获得立法机关的批准。

功能潜变与意外后果		
趋势 2		
进入社会权利的减少和不平等	评估	在公共卫生紧急状态下，有时政府制定的措施可导致某些群体遭受歧视。对于 Covid-19 疫情，某些措施成为强制性规定，但未提供足够的资源或支持以便人们遵守。例如，在一些国家，获得疫苗的途径有限或者大部分人仍未接种。尽管如此，仍然规定接种 Covid-19 疫苗之后方可进入公共场所或外出。
	建议	政府应确保：在紧急状态下，部署强制性公共卫生措施时，应提供必要的资源和设施，以便人们遵守这些措施，不会遭受不公而无法进入社会。
	如何实施建议？	
	□ 确保为民众广泛提供进入社会的资源，包括疫苗接种、检测和应用纸质替代品。 □ 必须在城市和农村地区都提供疫苗接种点和检测场所，并且能够轻易获取纸质/非数字的应用程序替代品。	

1. 对应用开发人员、运营商和公共机构委托方的建议

对于疫情响应的利益相关者，公众可有哪些预期以及为什么

重要的是，公众应知道，应用开发人员、运营商以及委托开发 Covid-19 应用的公共实体，可通过一些步骤来确保应用程序有效且可持续。这些步骤包括开发和设计选择、保障措施和过程化行为。作为更为广泛的公共卫生策略的一部分，它们共同推动信任的建立以及 Covid-19 应用的成功使用。

实际上，Covid 应用的功能和设计将影响个人数据的收集和使用，以及用户的基本权利，包括隐私权。

例如，应用程序代码的公开可促进公民社会和公众的信任。隐私保护设计原则可防止功能渐变和其他意外后果，避免因引入应用程序而失去信任或造成伤害。这包括限制不必要的数据使用，如位置数据，而且通常存在其他方式而不必使用这些数据。明确定义（个人）数据处理，特别是目的、数据敏感性、存储、安全和共享限制。任何类型的数据共享，尤其是涉及私营部门，必须在公共卫生策略中扮演明确的角色。研究数据除外，特别是有助于未来制定公共卫生政策的数据。

在尊重权利这一框架之内，应用程序应预防潜在欺诈而保持不会过时。出现欺诈时可有效且透明地进行处理，如此才能保证应用程序正常运作。

公共卫生效能		
趋势 1		
并非所有应用程序都公开代码	**评估**	在透明度方面，所有受到分析的应用程序都存在缺陷，不过在不同应用之间存在显著差异。只有三个应用程序为检查提供源代码。大多数使用代码混淆、反射和其他防分析技术，从而难以可靠地认定或确认某些行为是否存在。这些措施对信任造成负面影响，违背国际透明度和隐私设计建议。
	建议	所有现有 Covid 相关的应用程序，应在所有平台上开放源代码。通过使得服务器端代码可公开访问和审核，人们可以展开合作，检查代码漏洞以及创建同行评审系统。
	如何实施建议？	
	□ 在 GitHub 或其他类似开源网站/平台上发布源代码 □ 不要使用任何混淆技术来隐藏或扭曲源代码，妨碍独立代码检查。	

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 1</td></tr>
<tr><td rowspan="4">与私营部门合作，部署技术解决方案</td><td>评估</td><td>一些合作通过数据共享协议的方式来实现。另一些合作关系涉及私营公司帮助政府进行监视。这些合作关系的主要缺点是缺少适当的监管检查。此外，所有接受评审的国家都缺少全面的数据保护法规，进一步削弱公私合作的合法性，为功能潜变和权力不平衡创造了机会。</td></tr>
<tr><td>建议</td><td>对不同的政府机构和私营部门之间的数据共享，制定明确的规定。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 查询相关软件需求规范，确认应用或系统的功能是否需要数据共享。

□ 创建数据流程图和处理操作记录，记录与政府机构共享的数据及其目的。关于这类文档包含哪些内容，请参阅下方“实施工具”中的模板。

□ 咨询法律专家制定相关条款：与政府部门共享哪些数据、共享的目的以及其他相关的责任。在开发人员与政府之间的任何服务合同中，应包含这些条款。</td></tr>
<tr><td colspan="3">相关实施工具</td></tr>
<tr><td colspan="3">● 软件需求规范模板
● 免疫护照数据流程图模板</td></tr>
</table>

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 2</td></tr>
<tr><td rowspan="4">在大多数国家，接触者追踪应用采用中心化系统</td><td>评估</td><td>相对于去中心化系统，中心化系统可能更偏离隐私保护设计这一概念。在中心化系统中，公共机构的中央服务器处理大部分运算，使得这些机构更容易获取个人敏感数据。相比之下，在去中心化系统中，运算大部分在用户设备上进行，最敏感的个人数据也保留在本地，只与其他设备和中央服务器共享假名化的数据。在使用 GAEN API 的国家，就是这种情况。</td></tr>
<tr><td>建议</td><td>应用程序的开发使用隐私保护设计框架。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 为软件开发制定软件需求规范，列出 Covid 应用程序所需的功能以及相关隐私原则或法规。请参阅下方“实施工具”部分的模板。

□ 征求独立第三方专家意见，在开发周期的每个阶段，评估 Covid 应用程序的数据保护或隐私风险，确保在部署之前正确理解并实施数据保护和隐私原则。</td></tr>
<tr><td colspan="3">相关实施工具</td></tr>
<tr><td colspan="3">● 软件需求规范模板</td></tr>
</table>

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 3</td></tr>
<tr><td rowspan="3">位置数据常规用途</td><td>评估</td><td>通过位置数据，国家机构可追踪用户，也可以进行超出公共卫生需求的更具入侵性的监视。更令人担忧的是，位置数据可以暴漏“用户的习惯、家庭住址、工作场所数据甚至宗教信仰（即礼拜场所）”。</td></tr>
<tr><td>建议</td><td>如非必要，尽可能减少数据的收集，特别是个人或可识别数据，其中包括 GPS 定位。

为了保护隐私，所有接触者追踪应用程序取消对位置数据的请求。

提供易懂可用的选项，以便从应用程序和服务器上删除帐户和信息。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="3">□ 在将高级设计转化为代码行的过程中，定期进行代码审核。

□ 邀请数据保护和隐私专家参与，确保应用程序功能符合软件需求规范，其中包括相关法规或原则。</td></tr>
</table>

<table>
<tr><th colspan="3">功能潜变与意外后果</th></tr>
<tr><td colspan="3">趋势 4</td></tr>
<tr><td rowspan="4">跟踪和分析工具的常见用途</td><td>评估</td><td>在重点关注的国家，已部署的 SDK 并未完全遵循隐私保护设计的原则。特别是，Google Firebase 库或其他 SDK 并未在各自隐私政策中明确声明。因此，无法完全确定 Google Firebase 是如何使用的，尤其它是否仅限于安装分析，还是用于更大更侵犯隐私的追踪目的。</td></tr>
<tr><td>建议</td><td>提供明确的相关信息，包括：收集数据的类型和目的、数据储存的地点和时长、数据分享的对象和目的、以及所有这些功能的安全协议。

公布更详细的隐私政策（用所有当地语言编写），并明确地列出所有能够获取数据的第三方。</td></tr>
<tr><td colspan="2">如何实施建议？</td></tr>
<tr><td colspan="2">□ 对于 Covid 应用中第三方提供的 SDK 和其他软件库，实施供应商评估。这些评估应包括：检查隐私政策和其他相关数据保护文档，检查应用开发工作区导入的第三方代码。</td></tr>
</table>

公共卫生效能		
趋势 1		
Covid 证明造假	**评估**	一些案例显示，人们试图获得虚假二维码，以便能够出行或进入场地。其原因一部分源自有关 Covid-19 的错误信息和阴谋论。在一些国家，欺诈案例高达数万。
	建议	提前应对欺诈，确保对所有参与方进行适当的审核，其中包括私营合作方。 根据隐私保护设计原则，允许移除虚假证书，确保透明地将该流程集成至隐私声明。
	如何实施建议？	
	□ 实施验证测试，以确保系统的性能符合要求。测试应包括：单元测试（处理单个功能和系统组件）、集成测试（处理组件之间的相互作用）、系统测试（处理整个系统的完成部分）和验收测试（提供系统给选定用户，即 alpha 和 beta 测试）。	

功能潜变与意外后果		
趋势 1		
Covid 应用程序缺少隐私保护设计	评估	在隐私保护设计方面，Covid 应用存在着不同程度的成功。如果未遵守这一概念，用户可能受到不相称的伤害。这种伤害往往可以转移至应用开发人员以及使用其服务的政府，而政府未能适当地维护个人的隐私和数据保护权利。一些应用程序将处理数据的 SDK 用于与应用主要用途（公共卫生）无关的其他目的，或与第三方分享数据。同时，有关应用程序所用的第三方 SDK 或软件库，大多数应用开发人员采取非透明态度，或者不公开或混淆其源代码。此外，在部署之前，大多数 Covid 应用未**进行**数据保护或隐私影响评估，以便确定和降低潜在的数据保护或隐私风险。不过，对于需收集某些个人数据以便追踪接触者的公共场所，一些国家确实提供了数据保护指南。
	建议	所用的 SDK 仅处理应用程序必需的个人数据（即追踪接触者和/ 或显示健康信息）。 提供隐私通知，以人性化且简明扼要的方式，告知用户其数据如何收集和处理。 开源应用程序，以便独立验证应用程序的功能和数据处理。 如果公共场所组织者需处理个人数据（例如，用于数字和人工接触者追踪），应提供相关指南：如何负责地处理此类数据，以便良好地保护数据。 在部署之前，进行数据保护或隐私影响评估，确定数据保护或隐私的潜在风险，并制定适当的措施来降低这种风险。
	如何实施建议？	

	□ 征求独立第三方专家的意见，在开发期间评估 Covid 应用的数据保护或隐私风险，同时，在部署之前的开发周期的每个阶段，确保正确地实施数据保护和隐私原则。 □ 为软件开发流程制定软件需求规范，列出 Covid 应用程序的建议功能，并且这些功能符合相关隐私原则或法律规定。关于此类文档的内容，请参阅下方“实施工具”中的模板。 □ 关于 Covid 应用中第三方 SDK 和其他软件库，对供应商进行评估。评估应包括：检查隐私政策和其他相关数据保护文档，检查开发工作区导入的第三方代码。 □ 提供完整的隐私声明，同时为首次使用提供简要声明，并且在此之后可查看该声明。请参阅下方“实施工具”中的模板。 □ 在 GitHub 或其他类似开源网站/平台上发布源代码。 □ 不要使用任何混淆技术来隐藏或扭曲源代码，妨碍独立代码检查。 □ 为场所经营者提供数据保护指南，包括：(i) 收集哪些数据以及为什么，(ii) 如何收集并存储数据，(iii) 数据保密要求，以及 (iv) 仅与某些数据收集相关的第三方共享数据。 □ 使用下方“实施工具”中的模板，将其作为数据保护或隐私影响评估的起点，并在应用程序开发期间完成评估。
相关实施工具	
● 软件需求规范模板 ● 接触者追踪应用的隐私声明模板 ● 数据保护/隐私影响评估模板	

功能潜变与意外后果		
趋势 2		
公私合作增加但缺少透明度	评估	政府往往利用与私营部门合作来达到各种政策目的。Covid-19 也是如此；许多政府利用 Google/Apple Exposure Notification 系统来开发接触者追踪应用程序；一些国家从电信公司获取数据，创建热度地图并追踪病毒传播；同时，政府安装摄像系统来监视隔离规定的遵守情况，进一步扩大了国家监控能力。但这些合作关系常常不是公开的，或者，利用 Covid-19 的紧急情况来躲避政策监管，而这种监管用来确保权利得到保护。
	建议	对于任何公私合作开发的应用程序，应公开发布合作条款。
	如何实施建议？	
	□ 政府应确保公私合作关系的透明度（如批准信息开放请求）。	

实施工具

以下提供了一些模板以及良好实践示例，可用于实施 Covid-19 应用程序工具包提出的一些建议。

接触者追踪应用程序的隐私保护设计

该示例为接触者追踪应用程序的模型，可用于增加隐私保护。经用户同意，该应用程序可生成二维码，用于已注册的场所（下称“注册场所”）的出入登记。

这些应用程序的设计，是为了方便记录注册场所的出入，同时保护隐私和个人数据。这表示：

a. 应用程序处理的个人数据尽可能最小化；
b. 对个人数据尽可能最大化加密。在出现阳性 Covid 病例时，只能通过公共卫生机构解密。
c. 当存在 Covid-19 传播风险时，公共卫生机构只能接收必需的数据，以便追踪特定时间和场所内出现的特定个人。
d. 当出入信息与接触者追踪不再相关时，即 14 天后，应立即删除。

数据访问和转移

- 应用开发人员/运营商不可访问任何个人信息，包括：从个人收集的数据，注册场所处理的数据，以及转移至公共卫生机构的数据。
- 这些场所可通过应用程序记录出入信息，但应严格限制对个人数据的访问。仅在场所入口处显示相关信息，以便进行身份验证。只有场所已授权人员可访问这些数据。
- 当个人与 Covid-19 患者曾同时在注册场所出现时，经过授权的公共卫生机构可接收个人数据，以便联系。

用途明确

个人数据可用于：

a. 为个人提供二维码。
b. 为场所提供安全的方式来收集访客数据。
c. 为公共卫生机构提供所需数据，用于确认并联系 Covid-19 确诊患者的密接者。

处理的数据

1. 使用应用程序的个人数据：
   a. 姓名和出生年，用于识别和接触者追踪。
   b. 手机号码，用于接收应用程序二维码，以及在必要时方便公共卫生机构联系。
   c. 场所出入二维码标记；在个人设备和应用的服务器上存储；由公共卫生机构进行公开请求，由场所进行解密并用于追踪。

2. 注册场所处理的数据
   a. 电子邮箱、用户名、帐户密码，用于帐户的创建和管理。
   b. 三个场所联系人的姓名、电子邮箱和手机号码；在需要追踪接触者时，由公共卫生机构进行公开请求。

3. 公共卫生机构处理的数据
    a. 特定时间特定场所访客的姓名、出生年和电话号码，用于识别并联系相关人员，防止 Covid-19 扩散。

数据保留和删除

1. 已注册的用户和二维码：
    a. 为了注册和接收二维码所提供的个人数据，在收到二维码链接之后立即删除。
    b. 二维码包含已加密的个人数据，它保存在以下两处：
        i. 个人设备，以便场所扫码。
        ii. 应用开发人员/运营商的服务器，以便个人通过短信链接下载二维码图片。
    c. 用户可随时删除二维码或者两者之间的关联，但相关二维码的出入记录将保留 14 天，以便追踪接触者。
    d. 根据相关法律规定，场所对出入数据进行收集。在公共卫生机构撤销该规定之后，删除所有二维码及其解密方式。

2. 场所及其访客的数据：
    a. 场所相关的个人数据将一直保留，直到：
        i. 场所停用他们的帐户。在这种情况下，场所数据及其相关的出入数据将保留 14 天，以便追踪接触者。
        ii. 公共卫生机构撤销相关法律规定，不再要求场所收集出入数据。所有帐户将被删除。
    b. 注册场所的出入数据自动在 14 天后删除。
    c. 为了追踪接触者向公共卫生机构披露的数据，将根据相关的国家法规、政策和流程进行处理。

3. 短信发送之后，应用程序将立即删除短信数据，并且负责发送短信的数据处理方将从其服务器删除相关数据。

向公共卫生机构披露的数据

1. 在二维码中保存的个人数据是加密的。扫描二维码时，这些数据将关联至到访场所。只有在需要追踪接触者时，公共卫生机构才能访问并解密这些数据。

2. 如果经过追踪发现 Covid-19 患者曾访问某场所，公共卫生局可请求该场所公开当时所有访客的信息。该场所可授权相关个人数据的转移，或者在需要验证请求时，要求公共卫生机构提供更多信息。

3. 数据披露授权仅允许公共卫生机构访问相关的个人数据：指定时间内的场所访客。

信息安全

1. 通过数据隔离、可靠的访问控制和加密来实现信息安全。信息安全功能、架构和代码库经过独立的计算机科学家的审核和验证。

Cookie

1. 为了方便创建帐户以及确保数据安全，应用程序网站仅使用以下必需的 Cookie：
    a. Csrftoken 用于防止服务器受到跨站请求伪造攻击。
    b. Sessionid 用于服务器为可访问操作面板的用户指定正确的会话。

软件需求规范模板

软件需求规范对需求作出了详细的说明，并且应用程序或系统应满足其中所有的需求。该文档可同时包含技术和法律的需求。以下示例展示了软件需求规范的一部分，其中对接触者追踪应用程序的法律需求进行了说明。

需求 ID	REQ-31
需求说明	对于接触者追踪模型，应用程序应使用 Google/Apple Exposure Notification 框架。
作者	[姓名]
修订版	1.1
发布日期	[日期]
关键字	去中心化接触者追踪、数据最小化
法律需求	*FIPPs 收集限制原则：*个人数据的收集应受到限制。在需要时，此类数据应通过合法和公平的方式获取，并且数据主体应知情并同意。

场景说明

应用程序通过 GAEN 生成随机 ID （加密令牌，称为“滚动接近标识符”）。为了反映设备的位置，每 10-20 分钟更改一次。当用户与其他使用 GAEN 系统的设备密切接触时，两台设备通过蓝牙交换并记录对方的随机 ID。在用户将 Covid-19 阳性测试结果输入应用程序之后，设备将过去 14 天内记录的随机 ID 列表发送至公共机构运营的中央服务器。随后，移动设备定期将记录的随机 ID 与 Covid-19 检测阳性相关联的随机 ID 数据库进行对比。如果发现匹配，应用程序将通知用户：他们可能与 Covid-19 患者密接，建议遵守相关公共机构的指南，例如，进行 Covid-19 检测和/或自我隔离一段时间。

设计假设

设备上的加密令牌定期更改，并与设备的位置保持一致。

公共机构运营的中央服务器仅保存用户的假名个人数据（加密的随机 ID）。

免疫护照数据流程图模板

通过数据流程图，可将法律要求与数据生命周期的特定阶段进行关联，以确保数据的收集和处理完全满足这些要求。以下为数据流程图示例，列出了数据生命周期每个阶段的具体法律要求，以及应用程序相应的功能。此处的需求 ID 与上述软件需求规范中的 ID 相对应。

用户健康信息的数据生命周期		
数据生命周期的阶段	**需求 ID**	**需求说明**
收集	REQ-51	应用程序处理的数据包括：用户 Covid-19 疫苗接种状态、Covid-19 测试结果和 Covid-19 自然免疫信息。 在注册以及之后用户输入时，应用程序对健康信息进行收集。
使用	REQ-78	应用程序将用户健康信息转换至二维码。用户进入场所时向组织者展示。
披露	REQ-09	生成用户二维码，以便进入场所时扫描。
保留	REQ-12	用户健康信息将在设备上一直保留，直到用户删除应用程序。 应用程序不保留扫码时用户的位置。
销毁	REQ-34	删除应用程序时，将销毁用户健康信息。

接触者追踪应用的隐私声明模板

以下为简短版的隐私声明示例。在用户注册时，接触者追踪应用程序可显示该声明。该声明目的在于：显示有关应用程序数据处理的最关键信息，提供查看完整声明的选项，以及向开发人员提交问题。

English Text	译文
Your Privacy	您的隐私
This app was developed by [Company A] on behalf of [Government 1].	本应用程序由[公司 A]代表[政府 1]开发。
When you use our app, we collect your name, address, phone number and health information. This health data includes for example your Covid-19 test results.	当您使用该应用程序时，我们将收集您的姓名、住址、手机号码以及健康信息。健康信息包括您的 Covid-19 检测结果。
We use your data because it is necessary for the performance of a task carried out for public health purposes.	出于公共卫生的目的，执行某些任务需使用您的数据。
We collect your data when you first register on the app and as you continue to use the app.	在首次注册以及之后使用该应用程序时，我们将收集您的数据。
We use your data to notify you if you have been in close contact with a person potentially infected with Covid-19.	如果您与 Covid-19 潜在感染者发生密接，我们将使用您的数据向您发送通知。
We store your data in [Country X] and we use servers that are certified for health data hosting.	我们将您的数据保存在[国家 X]，并且所用服务器已经过认证，可用于健康数据托管。
We use SDKs from the following third party providers: • [Provider 1] • [Provider 2]	我们使用以下第三方提供的 SDK： • [提供商 1] • [提供商 2]
This privacy notice was last updated on 1/1/22.	该隐私声明的上次更新时间为 22年1月1日。
See Full Privacy Notice	查看完整的隐私声明
Have a Question?	是否有问题？

数据保护/隐私影响评估模板

以下示例为数据保护/隐私影响评估模板。应用程序在部署之前应进行相关评估。

系统/应用程序	[...]
系统/应用程序版本	[...]
数据保护/隐私影响评估日期	[...]

项目开发背景	
正在开发的系统/应用程序是什么？	[...]
为什么开发该系统/应用程序？	[...]
什么人参与系统/应用程序的开发？	[...]
对系统/应用程序进行了哪些测试？	[...]
完全部署的计划日期是哪天？	[...]

处理操作说明	
系统/应用程序使用哪些个人数据？	[...]
个人数据被用于什么目的？	[...]
个人数据披露给什么人？	[...]
系统/应用程序的开发使用哪些 SDK 或第三方软件库？	[...]

风险识别			
威胁	**漏洞**	**事件**	**风险**
[...]	[...]	[...]	[低、中或高]

风险管理			
风险	**响应**	**响应类型**	**理由**
[...]	［接受、转移、减缓或避免］	［技术、机构或合同］	[...]