

## جعبه ابزار برنامه‌های کووید-۱۹

چگونه قانون‌گذاران، سیاست‌گذاران، توسعه‌دهندگان، متصدیان، نهادهای عمومی کمیسیون‌دهنده، و عموم مردم می‌توانند

در بهبود نظارت و ایجاد توازن سهمی داشته باشند و اطمینان حاصل کنند که ابزارهای اعزام شده در طول یک همه‌گیری با هدف متناسب هستند؟

1	مقدمه
3	۱. توصیه‌ها برای سیاست‌گذاران و قانون‌گذاران
4	برای برنامه‌های ردیابی تماس
21	برای همهٔ انواع برنامه‌های کووید
28	۲. توصیه‌ها برای توسعه‌دهندگان برنامه، متصدیان و نهادهای عمومی کمیسیون‌دهنده
29	برای برنامه‌های ردیابی تماس
35	برای همهٔ انواع برنامه‌های کووید
40	۳. ابزارهای پیاده‌سازی
41	حریم خصوصی مبتنی بر طراحی برای برنامه‌های ردیابی تماس
45	قالب مشخصات الزامات نرم‌افزار
46	نقشهٔ جریان داده برای قالب برنامهٔ گذرنامهٔ واکسن
47	قالب اطلاع‌رسانی حریم خصوصی برای برنامهٔ ردیابی تماس
49	قالب ارزیابی اثرگذاری بر حریم خصوصی /محافظةت از داده‌ها

## مقدمه

کووید-۱۹ دولت‌ها را در سراسر جهان بر آن داشت تا اقدامات گسترده‌ای، از اقدامات همه‌گیرشناختی سنتی، مانند ماسک اجباری و فاصله‌گیری اجتماعی گرفته، تا شماری از واکنش‌های فناورانه و بی‌سابقه، از جمله برنامه‌های ردیابی تماس و گذرنامه‌های واکسن را به کار بگیرند.

پروژه برنامه کووید یک طرح پیشگامانه دو-بخشی جامعه مدنی است که از یک علاقه پژوهشی در مداخلات مختص به کووید سرچشمه می‌گیرد.

فاز ۱ پروژه که استفاده از برنامه‌های ردیابی تماس در برزیل، کلمبیا، هند، ایران، لبنان، و آفریقای جنوبی را تا ۲۱م جولای ۲۰۲۱ پوشش می‌داد، اثرگذاری استفاده از این برنامه‌ها را از منظر تأثیرگذاری بر سلامت عمومی ارزیابی کرد و تخطی از عملکرد و پیامدهای ناخواسته، همانند دسترسی محدود به جامعه را بررسی نمود. این علاقه مشترک پژوهشی شش سازمان جامعه مدنی را گرد هم آورد: ALT Advisory (آفریقای جنوبی)، Internet Democracy Project (هند)، InternetLab (برزیل)، Karisma (کلمبیا)، SMEX (لبنان)، و United for Iran. همچنین AWO، یک آژانس حقوق داده، حمایت خود را در زمینه هماهنگ‌سازی ارائه دادند.<sup>۱</sup>

فاز ۲ پروژه، برنامه‌های کاربردی فناورانه‌ای را در بر می‌گیرد که از جولای ۲۰۲۱ توسعه داده شده‌اند، از جمله «گذرنامه‌های واکسن» (نمایش‌دهنده وضعیت واکسیناسیون، نتایج آزمایش یا گواهی بهبودی). این مطالعه با پشتوانه نقدوبررسی فنی نمونه‌ای از برنامه‌ها در سطح جهانی، به روند سیاست‌ها، رویکردهای قانونی و فنی در سراسر جهان از طریق ارزیابی ۱۱ برنامه کووید می‌نگرد، که دولت‌ها و همچنین بازیگران دیگر در استرالیا، بحرین، شیلی، اندونزی، اسرائیل، هلند، تونس، و استرالیا غربی آن‌ها را توسعه داده‌اند (یا برون‌سپاری کرده‌اند).

این کشورها انتخاب شدند تا نماینده قاره‌ها/مناطق مختلف جهان باشند و روندهای اصلی مشاهده شده در طول تحقیق را نمایش دهند. سایر برنامه‌های بررسی شده، برنامه‌هایی هستند که در توسعه آن‌ها دسترسی جهانی مد نظر بوده است: (از انجمن بین‌المللی حمل‌ونقل هوایی، Travel Pass) و WEF (از سوی مجمع جهانی اقتصاد، CommonPass IATA).

خروجی این فاز دوم مشتمل است بر:

- «برنامه‌های کووید-۱۹: گزارش روندهای سیاست‌گذاری، قانونی و فنی» (از اینجا به بعد «گزارش روند»):<sup>۲</sup> یافته‌ها و توصیه‌ها از فاز ۲ در این گزارش ارائه شدند. این گزارش رویکردها به طراحی و استفاده برنامه را به لحاظ نتیجه‌بخشی سلامت عمومی، درجه خزش عملکرد و پیامدهای ناخواسته برای افراد مطرح می‌کند. این تحلیل به مجموعه‌ای از توصیه‌ها و بهترین شیوه‌ها برای ذی‌نفعان مرتبط جهت می‌دهد تا شیوه‌ها و اصول سلامت عمومی مؤثر و پایدار توسعه داده شود.
- گزارش درباره خطرات حریم خصوصی نرم‌افزار کووید-۱۹ (بخش ۲) «(از اینجا به بعد «گزارش فنی»):<sup>۳</sup> این گزارش یک نقدوبررسی فنی از ۱۱ برنامه منتخب ارائه می‌کند، با در نظر گرفتن اینکه آیا آن‌ها به بهترین شیوه‌ها در حفاظت از داده‌ها، شامل ولی نه محدود به، حریم خصوصی مبتنی بر طراحی و کمینه‌سازی داده‌ها پایبند بوده‌اند. این گزارش همچنین حاوی توصیه‌هایی در مورد بهترین شیوه حصول اطمینان از برنامه‌های مؤثر و ایمن کووید-۱۹ است.

<sup>۱</sup> نتایج فاز ۱ از اینجا قابل دسترس هستند: <https://www.awo.agency/latest/covid-19-app-project/>

<sup>۲</sup> قابل دسترس از اینجا: <https://awo.agency/files/Covid-Apps-Policy-Legal-Tech-Trends.pdf>

<sup>۳</sup> قابل دسترس از اینجا: <https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf>

- «جعبه‌ابزار برنامه‌های کووید-۱۹» (از اینجا به بعد «جعبه‌ابزار»):<sup>4</sup> جعبه‌ابزار بر مبنای یافته‌ها و توصیه‌های برجسته‌شده در گزارش فنی و گزارش روند نگاشته شده است. جعبه‌ابزار همچنین بر مبنای یافته‌های شناسایی شده در طول فاز ۱ پروژه کووید، توسط شش سازمان جامعه مدنی معرفی شده در بالا شکل می‌گیرد. به طور کلی، این سند مجموعه جامعی از بهترین شیوه‌ها و راهنمایی‌های قابل دسترس و همچنین ابزارهای پیاده‌سازی را برای تمامی ذی‌نفعان دخیل در پاسخ هم‌گیری یا مرتبط با چنین پاسخی فراهم می‌کند: قانون‌گذاران، سیاست‌گذاران، توسعه‌دهندگان برنامه، نهادهای عمومی کمیسیون‌دهنده، و عموم مردم.

توصیه‌های ارائه شده در این جعبه‌ابزار بر راه‌هایی برای بهبود اقدامات صورت گرفته به عنوان بخشی از پاسخ هم‌گیری تمرکز می‌کند تا ضامن اثربخشی از منظر سلامت عمومی باشد. این توصیه‌ها همچنین قصد دارند برای ذی‌نفعان دخیل در پاسخ هم‌گیری راهنمایی عملی فراهم کنند تا از خزش عملکرد و پیامدهای ناخواسته در زمان اعزام ابزارهای فناوری-محور جلوگیری شود. اگر این جعبه‌ابزار سطح پایه‌ای از اقدامات و توصیه‌های خوب را ارائه می‌دهد، ذی‌نفعان می‌توانند تصمیم بگیرند که آن را به گونه‌ای انطباق دهند تا تمامی اشکالات مختص به شرایطشان را انعکاس و پوشش دهد.

هرچند این توصیه‌ها بر مبنای ذی‌نفعان مستقیماً دخیل، تقسیم می‌شوند (به عنوان مثال توصیه‌ها برای سیاست‌گذاران و قانون‌گذاران)، تمامی این توصیه‌ها به تمامی ذی‌نفعان مرتبطند.

در نهایت، عموم مردم می‌توانند از آشنا شدن با روندها و توصیه‌های ارائه شده بهره‌مند شوند تا آگاهی خود را از مسائل مربوط به خود ارتقا دهند (به عنوان مثال: در خط مشی حریم خصوصی یک برنامه کووید باید به دنبال چه چیزی باشیم؟). برای تسهیل بیشتر چنین آگاهی‌هایی، هر یک از دو بخش این جعبه‌ابزار با خلاصه‌ای مختصر برای کاربران نهایی آغاز می‌شود: هدف آن شفاف‌سازی انتظاراتی است که عموم مردم می‌توانند از ذی‌نفعان دخیل در واکنش به هم‌گیری داشته باشند، از جمله در رابطه با رویکردی تناسب‌محور که به حقوق آنان احترام می‌گذارد و ضمانت‌کننده کارآمدی سلامت عمومی است.

- برای اطمینان از دسترس‌پذیری جهانی، جعبه‌ابزار به هفت زبان دیگر در دسترس است:
- عربی<sup>5</sup>
- فارسی<sup>6</sup>
- فرانسوی<sup>7</sup>
- هندی<sup>8</sup>
- پرتغالی (برزیل)<sup>9</sup>
- روسی<sup>10</sup>
- چینی ساده‌شده<sup>11</sup>
- اسپانیایی<sup>12</sup>

---

<sup>4</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-en.pdf>

<sup>5</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-ar.pdf>

<sup>6</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-fa.pdf>

<sup>7</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-fr.pdf>

<sup>8</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-hi.pdf>

<sup>9</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-pr.pdf>

<sup>10</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-ru.pdf>

<sup>11</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-zh.pdf>

<sup>12</sup> قابل دسترس از اینجا: <https://awo.agency/files/covid-app-toolkit-es.pdf>

## 1. توصیه‌ها برای سیاست‌گذاران و قانون‌گذاران

عموم مردم چه انتظاری می‌توانند از ذی‌نفعان دخیل در پاسخ همه‌گیری داشته باشند و چرا؟

سیاست‌گذاران و قانون‌گذاران می‌توانند بر اساس مشاوره‌ها و توصیه‌های جامعه سلامت عمومی، سیاست‌ها و چارچوب‌هایی قانونی معرفی کنند. برای عموم، مهم است بدانند که هدف از معرفی چنین چارچوب‌ها و پادمان‌هایی حصول اطمینان از این است، که اقدامات سیاست‌گذاران و قانون‌گذاران، در حین اتخاذ یک رویکرد تناسب-محور، معطوف به تضمین اثربخشی سلامت عمومی هستند. چنین رویکردی منجر به توسعه و تدارک پادمان‌های مؤثر در توسعه و استفاده برنامه‌های کووید-۱۹ می‌شود تا از پایبندی به بهترین شیوه‌های جهانی که به حقوق افراد احترام می‌گذارند، اطمینان حاصل شود. در عمل، اگر کشوری از یک برنامه کووید به عنوان یک مؤلفه در پاسخ همه‌گیری استفاده کند، اثربخشی سلامت عمومی چنین برنامه‌ای به مؤلفه‌ای از یک راهبرد وسیع‌تر و هماهنگ‌شده کووید-۱۹ تبدیل می‌شود، که وجود چنین راهبردی در جلوگیری از پیامدهای ناخواسته کلیدی است.

کاربران نهایی برنامه‌های کووید-۱۹ — شامل جوامع آسیب‌پذیر همانند پناهمجویان و کارگران مهاجر — باید قادر باشند تا دسترسی خود را به خدمات حیاتی حفظ کنند. برای حصول اطمینان از یک استراتژی سلامت عمومی جامع که تسهیل‌کننده اعتماد و دسترس‌پذیر برای عموم و به سادگی قابل فهم است، برنامه‌ها باید بخشی از یک راهبرد شواهد-محور وسیع‌تر باشند. این بدین معنی است، در صورتی که برنامه‌ها معرفی شوند، در میان شاخه‌های مختلف دولت، در سطوح کشوری و محلی بر مبنای استانداردهای فنی جهانی هماهنگ‌شده هستند و استفاده از آن‌ها با طرح‌های پیشگامانه آزمایش و ردیابی، سیاست‌های اجتماعی و سلامت عمومی، مانند فاصله‌گیری اجتماعی ترکیب شود. استفاده شفاف و هماهنگ‌شده از برنامه باید با خبررسانی رسانه‌ها (ی اجتماعی) به منظور افزایش آگاهی و آموزش درباره برنامه همراه شود.

در پایان، عموم باید بتوانند به پاسخ دولت اعتماد کنند، که مستلزم موارد بالا و نیز جلوگیری از خزش عملکرد و دیگر پیامدهای ناخواسته است. این امر می‌تواند با توسعه و پیاده‌سازی نظام‌های قانونی مناسب، شفافیت درباره توافق‌نامه‌های استفاده از داده‌ها و اشتراک‌گذاری داده‌ها تنها در راستای حمایت از راهبرد سلامت عمومی — و نه در راستای اهداف سیاسی و سیاست‌های دیگر — محقق شود. این اعتماد می‌تواند با اجرای برابر اقدامات سلامت عمومی در سراسر کشور، با نظارت مستقل، و با ایجاد بدیل‌های غیر-دیجیتالی، یا به عبارت دیگر جلوگیری از تنبیه کسانی که از برنامه استفاده نمی‌کنند، گسترش بیشتری پیدا کند.

نتیجه‌بخشی سلامت عمومی

روند ۱

<p>بسیاری از دولت‌ها، علی‌رغم نابرابری‌های از پیش موجود در زمینه دسترسی به اینترنت و پذیرش فناوری تلفن همراه، اقدامات فناورانه‌ای در پاسخ به کووید-۱۹ معرفی کردند. در بیان اهمیت این مشکل نمی‌توان اغراق کرد، چرا که دسترسی نابرابر به فناوری تلفن هوشمند می‌تواند به بی‌عدالتی‌های موجود دامن بزند و به افزایش نگرانی‌های اخلاقی بیانجامد. بعلاوه، با در دسترس قرار دادن خدمات تأمین اجتماعی به صورت عمده از طریق پلتفرم‌های آنلاین، جامعه‌های آسیب‌پذیری که با احتمال بیشتری دارای دسترسی اینترنت ضعیف و بدون تلفن همراه هستند، ممکن است از دریافت کمک‌های حیاتی محروم شوند.</p>	<p>ارزیابی</p>	<p>برنامه‌های ردیابی تماس و اقدامات فناوری-محور در کشورهایی با دسترسی ضعیف و نابرابر به اینترنت و فناوری تلفن همراه بکار گرفته شدند.</p>
<p>مسئولین کشور باید دسترسی به خدمات حیاتی را برای جمعیت‌های آسیب‌پذیر حفظ کنند (به طور خاص برای پناهمجویان و کاگران مهاجر).</p>	<p>توصیه</p>	
<p>توصیه چگونه پیاده‌سازی شود؟</p>		
<p><input type="checkbox"/> مسئولین کشور می‌توانند وضعیت امور را در رابطه با توزیع زیرساخت حیاتی اینترنت در کشورهای خود شناسایی کنند تا مناطق نیازمند به توسعه شناخته شوند.</p> <p><input type="checkbox"/> سرمایه‌گذاری‌ها می‌توانند روی زیرساخت حیاتی اینترنت در مناطق شناسایی شده که نیازمند توسعه هستند، انجام شود. این کار می‌تواند شامل یارانه برای طرح‌های تلفن همراه، فراهم کردن نقاط اتصال Wi-Fi رایگان و حتی برنامه‌های سواد دیجیتال باشد.</p>		

سر نوشت برنامه های رديابی تماس به طور نزديکی به پاسخ همه گیری ناهماهنگ در سطوح ملی و محلی گره خورده است. برخی برنامه ها تا حد زیادی از استراتژی پراکنده سلامت عمومی منقطع شده بودند. همچنین به این معنا بود که برنامه ها و اقدامات فناورانه دیگر با نیازهای سیستم بهداشت عمومی همجهت نشده بودند، این امر به خصوص در نبود اشتراک گذاری داده ها میان مراجع دولتی مرکزی و محلی مشهود شده بود. این مسئله منجر شد تا برخی استدلال کنند که استفاده از برنامه های رديابی تماس در برخی کشورها صرفاً تمرینی در جهت نشان دادن مشارکت دولت در پاسخ های فناوری-محور به همه گیری است.

ارزیابی

مسئولان کشور باید با در نظر گرفتن ارگان های دولتی در سطح ملی و محلی، پاسخی یکپارچه برای کووید-۱۹ (یا هر بیماری همه گیر دیگری) توسعه دهند.

توصیه

برنامه ها اغلب، تحت تأثیر استقبال پایین، از پاسخ سلامت عمومی وسیع تر منقطع بودند

توصیه چگونه پیاده سازی شود؟

- مسئولان کشور می توانند برنامه های رديابی تماس را در بستر زیرساخت وسیع تر سلامت عمومی و آزمایش و رديابی تعبیه کنند. برنامه ها زمانی دارای بهترین عملکرد هستند که در کنار سامانه های آزمایش و رديابی سنتی استفاده شوند، که متعاقباً به ظرفیت آزمایش کافی و کارکنان سازمان بهداشت عمومی در سطح محلی، منطقه ای و ملی وابسته است.
- سیاست گذاری شواهد-محور را برای تضمین یک پاسخ سلامت عمومی متناسب و اثربخش به کار بگیرید.

<p>در بسیاری کشورها، برنامه‌های ردیابی تماس متفاوت گسترش یافتند. بویژه زمانی که دولت‌های محلی منفرد تعدادی برنامه متفاوت انتشار دادند که دارای عملکردهای مختلفی بودند. برخی دولت‌های محلی برنامه‌هایی را با عملکردهایی فراتر از ردیابی تماس اعزام کردند، مانند ارائه مراقبت سلامت از راه دور. این مسئله گاهی پیامد هماهنگی بین‌انهادی محدود و سیستم‌های سلامت عمومی تمرکززدایی شده بودند. آرایه برنامه‌های کووید-۱۹ ردیابی تماس رسمی در برخی کشورها احتمالاً از استقبال کلی از آنها کاسته است.</p>	ارزیابی	چندین برنامه و برنامه‌هایی چند منظوره اعزام شده‌اند
<p>مسئولان کشور، با در نظر گرفتن ارگان‌های دولتی هم در سطح ملی و هم در سطح محلی، باید یک پاسخ یکپارچه به همه‌گیری توسعه دهند.</p>	توصیه	
<p>توصیه چگونه پیاده‌سازی شود؟</p>		
<p> <input type="checkbox"/> حصول اطمینان از پاسخ هماهنگ دستگاه‌های دولتی و مراجع بهداشت عمومی.  <input type="checkbox"/> پایبندی به استانداردهای بهترین شیوه کاربرد برای برنامه‌های ردیابی تماس، از توسعه یک زیرساخت قدرتمند پشتیبانی می‌کند، مانند: API (Google Apple Exposure Notification) .GAEN.         </p>		



<p>استقبال از برنامه‌های ردیابی تماس به علت فقدان اعتماد یا آگاهی عمومی در تمام کشورهای مورد نقد و بررسی، مختل شده بود. بخشی از این مسئله از کارزارهای ضعیف صورت گرفته حول برنامه نشئت می‌گرفت، که غیاب ارتباطات متمرکز و هدفمند از سوی دولت را نیز شامل می‌شد. بعلاوه، برخی از برنامه‌ها از نگرانی‌هایی در مورد نظارت و دیدبانی، و حریم خصوصی رنج می‌بردند، از جمله در کشورهایهایی که دارای سابقه سوءاستفاده نهادهای اجرایی و سازمان‌های اطلاعاتی از قدرت‌های دیدبانی هستند، که خبرنگاران، رهبران اپوزیسیون، قضات، و فعالان حقوق بشر را تحت فشار قرار می‌دهد.</p>	ارزیابی	
<p>مسئولان کشور باید ارتباط با و از طریق رسانه‌ها را بهبود دهند. محتوا باید علمی باشد و به نحو حرفه‌ای به مخاطبان انتقال داده شود تا به افزایش آگاهی و آموزش عمومی بیانجامد.</p>	توصیه	فقدان اعتماد و آگاهی عمومی بر برنامه‌های ردیابی تماس تأثیر می‌گذارد
<p>توصیه چگونه پیاده‌سازی شود؟</p>		
<p>برنامه‌های ردیابی تماس تنها در صورتی می‌توانند نقشی معنادار ایفا کنند که مردم از وجود آن‌ها آگاه بوده و به برنامه و استفاده همه بازیگران/ذینفعان مرتبط از داده‌های افراد توسط اعتماد داشته باشند. ۱۲ استفاده از بهترین اصول جهانی در طراحی برنامه از خزش عملکرد یا نشئت داده‌ها جلوگیری می‌کند تا تمایل عموم به استفاده از برنامه افزایش پیدا کند.</p> <p>مردم را از وجود برنامه مطلع ساخته و استفاده از آن را در سطوح مختلف دولت، مراجع سلامت عمومی، رسانه‌ها، و بخش خصوصی ترغیب کنید.</p>		

<p>در حالی که برنامه‌های ردیابی تماس توجه و بحث عمومی را به خود جلب می‌کنند، اقدامات جایگزین اغلب دارای نفوذ بیشتری هستند. برخی کشورها عمدتاً بر غربال‌گری جمعی، آزمایش‌گری هدفمند و دستورهای خانه‌نشینی متکی بودند، که مستلزم بسیج کارکنان بهداشت و سلامت برای غربال‌گری بیش از میلیون‌ها نفر بود. دستورهای خانه‌نشینی کشوری و اقدامات قرنطینه نیز نقش چشمگیری در متوقف کردن انتشار کووید-۱۹ داشتند.</p>	ارزیابی	<p>اقدامات جایگزین اغلب دارای اثربخشی بیشتری بر سلامت عمومی نسبت به برنامه‌های ردیابی تماس هستند</p>
<p>مسئولین کشوری باید پاسخ‌های غیر-فناوری-محور را به همه‌گیری، به عنوان جایگزین‌هایی در کنار پاسخ فناوری-محور با استفاده از برنامه‌ها، توسعه دهند.</p>	توصیه	
<p>توصیه چگونه پیاده‌سازی شود؟</p>		
<ul style="list-style-type: none"> <li><input type="checkbox"/> تقویت همکاری و هماهنگی میان بخش‌های دولتی و خصوصی برای حصول اطمینان از آمادگی بیمارستانی و تعیبه کردن برنامه‌های ردیابی تماس در یک راهبرد سلامت عمومی وسیع‌تر، شامل آزمایش و ردیابی و آزمایش دسترس‌پذیر.</li> <li><input type="checkbox"/> حصول اطمینان از اینکه شکلی از سیاست‌های اجتماعی برقرار هستند که افراد (بالقوه مبتلا) را قادر می‌سازند که از سیاست‌ها و دستورالعمل‌ها پیروی کنند، به عنوان مثال، جلوگیری از فقر ناشی از همه‌گیری با فراهم ساختن حمایت اقتصادی در طول قرنطینه یا جداسازی بیماران.</li> <li><input type="checkbox"/> اطمینان حاصل کنید تجهیزات محافظتی برای عموم مردم در دسترس است (به عنوان مثال ماسک).</li> </ul>		

<p>در طول این دوره از مطالعه، همه کشورهای مورد نظر وضعیت اضطراری ملی اعلام نکردند. برای آن کشورهایی که وضعیت اضطرار ملی اعلام کردند، مبنای قانونی برای پیادهسازی اقدامات مختلف از تمهیدات ویژه درون قانون اساسی یا چارچوب قانونی آن کشور مشتق می‌شد. این موضوع معمولاً به این معناست که تحت قواعد و شروطی خاص، دولت می‌تواند قدرت‌هایی را در حین فاصله گرفتن از معیارهای مرسوم حقوق بشر بکار ببندد.</p> <p>هرچند، یک وضعیت اضطراری می‌تواند بر برخی جوامع آسیب‌پذیر به طور منفی اثر بگذارد، بویژه در جایی که اقدامات پیادهسازی شده گرایش‌های تبعیض‌آمیز موجود را نهادینه و تشدید می‌کند. آن دسته از کشورهایی که وضعیت اضطراری اعلام نکردند، بر تمهیدات قانون‌گذارانه عادی همراه با قدرت‌های فوق‌العاده متکی بودند. این شرایط با اعلام وضعیتی اضطراری متفاوت است چرا که مبنای چنین قدرت‌هایی متشکل از قانون‌گذاری‌های پیشین و به طور معمول قوانین سلامت عمومی است، که به اقدامات مشخصی اجازه پیادهسازی شدن می‌دهد بدون اینکه این اقدامات به شرایط اضطراری خاصی گره خورده باشند. این امر شاید همیشه مطابق با تمهیدات صریح در قانون اساسی یا چارچوب قانونی نباشد، به همین خاطر، بدون وجود نظارت‌ها و توازن‌های مستقر، این امکان را بوجود می‌آورد تا قدرت‌های وسیعی، بدون اینکه نظارت‌ها و توازن‌های مناسبی برقرار باشند اعمال شوند.</p>	<p>ارزیابی</p>	<p>مراجعه محدود به قوانین اضطراری، استفاده مضاعف از قدرت‌های فوق‌العاده</p>
<p>مقامات ملی باید اقدامات سلامت عمومی را از طریق ابزارهای قانونی مناسب معرفی کنند که فراهم‌کننده پادمان‌های مؤثر برای حقوق فرد هستند، از جمله هنگامی که این اقدام‌ها مبتنی بر اعلام مشروع وضعیت اضطراری هستند.</p> <p>در بحران‌های آتی، مراجع ملی باید ارزیابی‌هایی از اثرگذاری بر حقوق بشر بعمل آورند که چارچوب‌های حقوقی را مطلع می‌کنند، این ارزیابی‌ها شامل ملاحظاتی درباره وضعیت‌های اضطراری و وضعیت‌های بحرانی است، و آنچه ضروری و توجیه‌پذیر خواهد بود را در بر می‌گیرد.</p>	<p>توصیه‌ها</p>	

در فرآیندی مشابه به آنچه برای رسیدگی به نقض جدی حقوق بشر طراحی شده بود، می‌توان توصیه کرد تا سازوکارهای موقتی در نظر گرفته شود که اثرات بلند مدت رویه‌ها و هنجارهای ایجاد شده در طول همه‌گیری کووید-۱۹ را ارزیابی کنند، و همچنین پاسخ‌گویی و بازپیکربندی را ترویج دهید تا شرایط استثنائی تداوم پیدا نکند

#### چگونه توصیه‌ها را پیاده‌سازی کنیم؟

- قانون‌گذاری و سیاست‌هایی را برای مواجهه با موج دیگری از کووید-۱۹ یا یک همه‌گیری جدید معرفی کنید تا نیاز به وضعیت اضطراری را محدود سازید.
- اگر برای یک واکنش سریع به وضعیت اضطراری نیاز است، یک بند انقضا باید وجود داشته باشد، که تصریح کند اقدامات سلامت عمومی جدید باید مؤکداً از لحاظ زمانی محدود شده باشند.
- ارزیابی‌هایی از اثرگذاری قوانین سلامت عمومی فعلی (و آتی) بر حقوق بشر بعمل آورید، پیش از آنکه اعمال آن قوانین ضروری باشد. ارزیابی‌های اثرگذاری بر حقوق بشر باید به صورت شفاف صورت بپذیرند تا از ارزیابی بایسته و اعتماد عمومی کافی اطمینان حاصل شود.<sup>۱۳</sup>
- از سیاست‌گذاری مبتنی بر شواهد برای تضمین پاسخ سلامت عمومی متناسب و مؤثر بهره بگیرید. با استفاده از بهترین شیوه‌های جهانی که متکی بر پذیرش و نظارت دموکراتیک هستند، از وضعیت‌های استثنایی تداوم یافته جلوگیری کنید.

<p>در یافته‌های فاز ۱، قوانین جامع حفاظت از داده‌ها در طول همه‌گیری، یا اعمال نشده بودند، کماکان در فرایند قانون‌گذاری قرار داشتند، یا به سادگی وجود نداشتند. به طور کلی، نظام‌های قوی‌تر حفاظت از داده‌ها ممکن است نظارت را در سطح کشورهای مورد نظر تقویت کنند.</p>	<p>ارزیابی</p>	<p>کشورها نظام‌های حفاظت از داده نوپا و گاهاً اجرا نشده‌ای دارند</p>
<p>مراجع کشور باید فرایند اجرایی کردن قوانین حفاظتی را به همراه تمهیدات ضروری تسریع کنند، تا همه برنامه‌های مرتبط با کووید و ابزارهای فناوری اطلاعات را پوشش دهند.</p> <p>دولت‌ها و شرکای خصوصی آن‌ها باید از وجود چارچوب‌های مقرراتی و سیاستی شفاف و مبتنی بر حقوق، با تأکیدی ویژه بر حقوق حریم خصوصی اطمینان حاصل کنند.</p> <p>قانون‌گذاری و لایحه‌ای که به حفاظت از داده‌ها مرتبط است باید بازبینی شده و با هر قانون حفاظت از داده‌های جداگانه موجود دیگری هماهنگ شود.</p>	<p>توصیه‌ها</p>	
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p><input type="checkbox"/> چارچوب‌های حفاظت از داده‌ها را برای استفاده از آن‌ها در پاسخ به بحران بدون معرفی مخاطرات جدید، معرفی کرده یا گسترش دهید.</p> <p><input type="checkbox"/> یک زیرساخت نظارتی قدرتمند با یک مرجع حفاظت از داده مستقل توسعه دهید.</p>		

<input type="checkbox"/> قانون‌گذاری حفاظت از داده‌ها را با کشورهای همسایه هماهنگ کرده و آن را همجهت با بهترین شیوه‌ها و اصول جهانی قرار دهید. ۱۴	
<input type="checkbox"/> سازمان‌های مردم‌نهاد (NGOها)، گروه‌های حقوق بشر و سازمان‌های دیگر باید به ارائه پشتیبانی به دولت‌ها در زمینه تصویب و/یا اعمال بهتر قانون‌گذاری حفاظت از داده‌ها ادامه دهند.	

خزش عملکرد و پیامدهای ناخواسته		
روند ۳		
<p>جمع‌آوری و اشتراک‌گذاری داده‌ها از سوی مراجع عمومی و در پاسخ به همه‌گیری در بین دولت‌های سراسر جهان رایج است. دلیل اصلی برای این امر تسهیل و تأیید برنامه‌ها برای سفرهای داخلی است در حالی که اقدامات قرنطینه‌ای برقرار هستند. این فرایند مستلزم ترکیب مجموعه داده‌های از پیش موجود و نیز آن مجموعه داده‌هایی است که اختصاصاً برای کووید-۱۹ تولید شده‌اند. با این وجود، غیاب قوانین جامع حفاظت از داده‌ها یا دیگر نظارت‌های مقرارتی به رشد خزش عملکرد و تأثیرات مخرب بر برخی جوامع خاص و آسیب‌پذیر می‌انجامد. این اتفاق از طریق اشتراک‌گذاری اطلاعات شخصی حساس با نیروی انتظامی و محدودسازی تردد کسانی رخ می‌دهد که به طور معمول به پلتفرم‌های آنلاین دسترسی ندارند تا برای مجوزهای سفر درخواست خود را ثبت کنند.</p>	ارزیابی	اشتراک‌گذاری افزایش‌یافته و غیر شفاف داده‌ها میان مراجع عمومی
<p>مراجع عمومی و نهادهای خصوصی که برای پردازش داده‌های شخصی در یک همه‌گیری همکاری می‌کنند باید گزارش‌های اثرگذاری را به عنوان یک شیوه عملکرد صحیح در شفافیت و پاسخ‌گویی فعال تهیه و منتشر کنند.</p>	توصیه‌ها	

همه برنامه‌ها باید با مدارک حقوقی حیاتی همانند شرایط خدمات و خط مشی حریم خصوصی همراه شوند و این مستندات باید در عرصه عمومی قرار بگیرند.

اطلاعات روشنی را در رابطه با نوع داده‌های جمع‌آوری شده و هدف از آن، محل ذخیره داده‌ها و طول مدت ذخیره‌سازی آن‌ها، افرادی که داده‌ها با آن‌ها به اشتراک گذاشته می‌شود و اهداف آن و پروتکل‌های امنیتی برای تمامی این عملکردها ارائه کنید.

خط مشی‌های حریم خصوصی باید هر برنامه شخص ثالثی را که به داده‌های شخصی دسترسی دارد فهرست کنند.

#### چگونه توصیه‌ها را پیاده‌سازی کنیم؟

- در توافق‌نامه‌های اشتراک‌گذاری داده‌ها بندهای انقضای شفاف قرار دهید.
- اطمینان حاصل کنید که داده‌های بدست آمده از بخش خصوصی مشمول قوانین حفاظت از داده‌ها و ارزیابی بایسته قرار می‌گیرد، از جمله زمانی که این داده‌ها خریداری و یا به صورت داوطلبانه به اشتراک گذاشته می‌شوند.
- شرایط خدمات، خط مشی‌های حریم خصوصی و اطلاعات در مورد اینکه چه داده‌هایی، از سوی چه کسانی و چگونه استفاده خواهند شد را توسعه و انتشار دهید.
- سیاست‌های حریم خصوصی باید قابل فهم و کل‌گرا باشند و هر گونه برنامه کاربردی شخص ثالثی را توضیح دهند.

ابزارهای پیاده‌سازی مرتبط

● قالب اطلاع‌رسانی حریم خصوصی برای برنامه ردیابی تماس

<p>استقبال از برنامه‌های ردیابی تماس به علت فقدان اعتماد یا آگاهی پایین عمومی در تمام کشورهای مورد بازبینی و مطالعه، با مشکل مواجه شد. بخشی از این امر ناشی از کارزارهای ضعیف صورت گرفته حول برنامه بود، که در کنار غیاب ارتباطات متمرکز و هدفمند از سوی دولت به سردرگمی عمومی حول برخی برنامه‌ها می‌انجامید. بعلاوه، برخی از برنامه‌ها از نگرانی‌هایی در مورد دیدبانی و حریم خصوصی رنج می‌بردند.</p>	<p>ارزیابی</p>	<p>نبود اعتماد و آگاهی عمومی بر برنامه‌های ردیابی تماس اثر می‌گذارد.</p>
<p>مراجع عمومی باید از ارتباطات متمرکز و هدفمندی استفاده کنند که دسترسی به اطلاعات دقیق و به‌موقع در مورد کووید-۱۹ را ارائه می‌دهد. محتوای تهیه شده باید علمی و حرفه‌ای باشد تا آگاهی‌رسانی و آموزش را میان عموم افزایش دهد و در نتیجه پاسخ به اقدامات و محدودیت‌ها را بهبود ببخشند.</p> <p>مراجع عمومی باید فرایندهای رایزنی منظم، شفاف، دموکراتیک و علمی را با اعضای جامعه مدنی حفظ کنند.</p>	<p>توصیه‌ها</p>	
<p>چگونه توصیه‌ها پیاده‌سازی شوند؟</p>		
<p>□ برنامه‌های ردیابی تماس تنها در صورتی می‌توانند نقشی معنادار در اثربخشی سلامت عمومی داشته باشند که به صورت وسیع مورد استقبال عموم قرار گیرند، که لازمه آن اعتماد است. استفاده از بهترین شیوه‌ها و استانداردهای جهانی (به عنوان مثال، کمپنه‌سازی داده‌ها، مشخصات هدف) و به صورت کلی جلوگیری از خزش عملکرد مؤلفه‌هایی کلیدی در ساخت و حفظ اعتماد عمومی هستند. قالب مشخصات الزامات نرم‌افزاری را که در بخش انتهایی این جعبه‌ابزار قرار گرفته است مشاهده کنید.</p>		



برخی از کشورهای تحت بررسی برنامه‌هایی را اعزام کردند که به مردم اجازه می‌داد تا متخلفان دستور خانه‌نشینی را با استفاده از ویژگی‌هایی که به کاربران اجازه می‌داد تجمعات انبوه و مسافران بین‌ایالتی را در منطقه خود به مقامات عمومی گزارش کنند. هرچند، هنگامی که از اعضای جامعه خواسته می‌شود که عمل دیدبانی را به نیابت از دولت انجام دهند، بدون تعهد به برابری که دولت‌ها باید به طور معمول رعایت کنند، این امر می‌تواند تبعات سنگینی برای گروه‌های به حاشیه رانده شده داشته باشد.

در حالی که اقدامات کووید-۱۹ به طور خاص، دستورهای در خانه ماندن کشوری و کنترل‌های مرزی سخت‌گیرانه روی کل جمعیت‌ها اثر می‌گذارند، مهاجران و پناهنجویان در معرض خطر محرومیت و یا تبعیض بالاتری هستند. اطمینان از اینکه جوامع آسیب‌پذیر از این خطرات محفوظ هستند، همانگونه که در تعدادی از کشورها دیده می‌شود، همیشه به خوبی مدیریت نمی‌شود. بسیاری از مردم با محدودیت‌های سفر به مشکل برمی‌خورند، بویژه هنگامی که دریافت مجوز سفر فقط از پلتفرم‌های دیجیتال امکان‌پذیر است. برخی حتی در یافتن مسکن در میانه دستورهای خانه‌نشینی کشوری با دشواری‌هایی مواجهند، همانگونه که در برخی کشورها اتفاق افتاد. کووید-۱۹ همچنین چالش‌هایی که مردم روستایی و افراد شاغل در بخش‌های غیررسمی اقتصاد با آن مواجه هستند، مثل عرضه آب ناکافی و فزونی جمعیت را تشدید کرد. این امر افزون بر استفاده مشاجره‌آمیز از اردوگاه‌های قرنطینه بود، که مهاجران برای هفته‌ها در آن‌ها بدون آزمایش شدن برای کووید-۱۹ در انزوا نگهداری می‌شدند و از فرصت قرنطینه کردن خود به صورت شخصی محروم شدند.

ارزیابی

تبعیض علیه گروه‌های به حاشیه رانده شده

<p>مراجع عمومی باید اقدامات سلامت عمومی را به صورت مساوی در سراسر کشور پیاده کنند.</p> <p>مراجع عمومی باید تضمین کنند که خدمات برای جمعیت‌های آسیب‌پذیر (مثل مهاجران و پناجویان) حفظ می‌شوند تا آن‌ها بتوانند از دشواری‌های مداوم مرتبط با همه‌گیری در امان باشند. چنین خدماتی شامل دسترسی به مراقبت سلامت، کمک‌های اقتصادی، و آموزش است.</p> <p>مقامات عمومی باید اطمینان حاصل کنند که هیچ فردی به علت عدم استفاده از برنامه‌های کووید جریمه، و یا دسترسی او از هیچ‌گونه خدماتی، عمومی یا خصوصی، سلب نمی‌شود.</p> <p>اقدامات سلامت عمومی باید متکی بر تحلیل اثرگذاری باشند که پیامدهای احتمالی را که اقدامات می‌توانند روی گروه‌های آسیب‌پذیر داشته باشند در نظر بگیرد.</p>	<p>توصیه‌ها</p>	
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<ul style="list-style-type: none"> <li><input type="checkbox"/> افراد را به گزارش «متخلفان» اقدامات کووید ترغیب و یا ملزم نکنید، چرا که این کار بر عهده مراجع عمومی است.</li> <li><input type="checkbox"/> اقدامات سلامت عمومی را به صورت یکسان در سراسر کشور اعمال کنید و از نظارت مستقل بر اعمال این اقدامات و همچنین سازوکارهای جبران آن‌ها اطمینان کسب کنید.</li> <li><input type="checkbox"/> اطمینان حاصل کنید مهاجران و پناجویان مشمول سیاست‌های سلامت عمومی، تأمین اجتماعی و دیگر نظام‌های پشتیبانی می‌شوند.</li> </ul>		

<p>□ برای افراد بدون تلفن هوشمند یا کسانی که مایل به استفاده از برنامه‌ها نیستند، از وجود بدیل‌های کاغذی (غیر دیجیتال) در کنار برنامه‌های ردیابی تماس اطمینان حاصل کنید.</p> <p>□ از تداوم درخواست‌های پناهندگی، و مسکن پاکیزه و ایمن اطمینان حاصل کنید، با در نظر گرفتن گزینه‌های بدیعی چون اقامت در هتل‌ها (که در غیر این صورت بدلیل بحران خالی خواهند بود).</p> <p>□ مراجع عمومی باید ارزیابی‌هایی از اثرگذاری بر حقوق بشر بعمل بیاورند که تأثیرات بالقوه بر گروه‌های آسیب‌پذیر متفاوت را مورد توجه قرار می‌دهند.</p>	
--	--

<p>در برخی از کشورهای مورد نقدوبررسی، اعتراضات در پاسخ به کمک‌های ارائه شده محدود از سوی دولت‌های ملی و محلی در رسیدگی به مسائل ناشی از دستوره‌های خانه‌نشینی و دیگر اقدامات مربوط به کووید رخ دادند. در بعضی موارد، اعتراضات منجر به این شد تا نیروی انتظامی از قدرت نامتناسبی برای سرکوب اعتراضات استفاده کند، که کودکان، بیماران و افراد سالمند را تحت تأثیر قرار می‌داد.</p> <p>در نقدوبررسی کشوری دیگر، روشن شد که اعتراضات در پاسخ به سوءمدیریت بحران اقتصادی در طول همه‌گیری شدت گرفتند. اعتراضات همچنین به خاطر نبود حمایت دولت در طول مدت خانه‌نشینی ملی، که وضعیت رکود اقتصادی را که افراد زیادی را تحت تأثیر خود قرار داده بود وخیم‌تر می‌کرد. تظاهرات به تلفاتی در حین درگیری با نیروهای امنیتی منجر شدند، چرا که مسئولین سعی داشتند تا اعتراضات را، از جمله در طول دستورات خانه‌نشینی ملی، سرکوب کنند.</p>	<p>ارزیابی</p>	<p>سرکوب اعتراضات</p>
<p>دولت‌ها نباید از سیاست‌های ضد-کووید برای ارعاب و سرکوب مخالفان سیاسی استفاده کنند، و همینطور نباید از آن‌ها برای مجازات مخالفان در زندان استفاده شود.</p>	<p>توصیه‌ها</p>	
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p>□ سیاست‌های سلامت عمومی و عملیات قانون‌گذاری باید شواهد-محور و دارای اهداف تعیین شده و روشنی برای مبارزه با شیوع کووید-۱۹ باشند و تا جای ممکن به فعالیت‌های اقتصادی اجازه ادامه دهند و برخورداری کامل از حقوق بنیادی در حیطه این محدودیت‌ها را امکان‌پذیر سازند.</p>		

□ اگر این قوانین و سیاست‌ها هنوز وجود ندارند، در صورت نقض حقوق بنیادی در طول یک همه‌گیری، سازوکارهای جبران خسارت یا باید مستقر و یا حفظ شوند. در غیر این صورت، اگر وجود دارند باید به نحوی اثربخش پیاده‌سازی شوند.	
--	--

خزش عملکرد و پیامدهای ناخواسته		
روند ۷		
<p>نابرابری‌ها در زمینه دسترسی به اینترنت و استفاده از فناوری موبایل اثر مستقیمی روی دسترسی افراد به جامعه در طول همه‌گیری دارند. این امر در نهایت به مسئله‌ای حیاتی بدل می‌شود چرا که دسترسی نابرابر به چنین منابعی می‌تواند به نابرابری‌های موجود دامن بزند و نگرانی‌های اخلاقی را افزایش دهد. بعلاوه، با دسترس‌پذیر ساختن خدمات تأمین اجتماعی به صورت عمده از طریق پلتفرم‌های آنلاین، ممکن است جوامع آسیب‌پذیر، که بسیاری از آنان فاقد دسترسی کافی به اینترنت بوده و دارای تعداد محدودی دستگاه موبایل هستند، از خدمات حیاتی محروم شوند. با این حال، حتی در جایی که پلتفرم‌ها به صورت فیزیکی قابل دسترس هستند، طراحی آن‌ها می‌تواند تبعاتی منفی داشته باشد که از جوامع آسیب‌پذیر فراتر می‌رود. به عنوان نمونه، برخی برنامه‌های ردیابی تماس، علی‌رغم اینکه کاربرانشان به زبان‌های محلی بسیاری صحبت می‌کنند فقط به زبان انگلیسی در دسترس قرار گرفتند.</p>	ارزیابی	پاسخ فناوری-محور کووید-۱۹، شکاف دیجیتال و نابرابری‌ها را تشدید کرده است
<p>مطالب دیجیتال باید توسعه یافته و در دسترس قرار داده شوند. این مطالب باید روشن و متناسب باشند، همراه با آموزش و ابزارهایی که نحوه استفاده از برنامه را نشان می‌دهند و نیز مسائل کلیدی را در رابطه حریم خصوصی داده‌ها برجسته می‌سازند. آموزش سواد دیجیتال نیز باید برای کارکنان دولت، کارکنان سلامت اجتماعی و کاربران برنامه فراهم شود.</p> <p>مراجعه عمومی باید ابزارهای جایگزین و غیر-دیجیتال را برای درخواست‌های تردد و ثبت‌نام واکسیناسیون توسعه دهند.</p>	توصیه‌ها	

## چگونه توصیه‌ها را پیاده‌سازی کنیم؟

- از وجود جایگزین‌های مبتنی بر کاغذ (و غیر-دیجیتال) برای تمامی پاسخ‌ها و طرح‌های پیشگامانه کووید-۱۹ مطمئن شوید، شامل، و اما نه محدود به، ردیابی تماس، برنامه‌های ردیابی تماس و دسترسی به تأمین اجتماعی.
- به مسأله آموزش از راه دور که کودکانی که در وضعیت اقتصادی متزلزل قرار دارند را در وضعیت نامساعدتری قرار می‌دهد رسیدگی کنید.
- از وجود سیاست‌ها و منابع مالی اطمینان حاصل کنید تا از ایجاد تبعات (بزرگتر) شکاف دیجیتال میان کودکان جلوگیری کنید.

<p>سیاست‌ها و اقداماتی که تلاش دارند به یک وضعیت اضطراری رسیدگی کنند باید دارای یک مبنای عقلانی زیربنایی باشند تا از اثربخش بودن آن‌ها اطمینان حاصل شود. بنابراین در زمینه همه‌گیری کووید-۱۹، هر نوعی از مداخله سلامت عمومی باید با شرایط خاص کشور یا منطقه تطبیق داده شود، و با تحقیقات علمی مربوطه حمایت شود. دولت‌ها درجات موفقیت متفاوتی در دخیل کردن مسئولین سلامت عمومی و دیگر کارشناسان مربوطه در فرایند تصمیم‌گیری برای توسعه پاسخ به همه‌گیری کووید-۱۹ داشتند.</p>	<p>ارزیابی</p>	
<p>دولت‌ها باید از استقرار زیرساخت حیاتی اطمینان حاصل کنند، تا در صورتی که فناوری بخشی از پاسخ همه‌گیری است، اقدامات فناورانه معرفی شده در حد امکان اثربخش باشند. بویژه در رابطه با برنامه‌های موبایل و دیگر سرویس‌های مبتنی بر وب، زیرساخت اینترنت باید توسعه پیدا کند تا دسترسی اینترنت به طور کافی میان جمعیت توزیع شود تا از استفاده از شبکه پشتیبانی کند که لازمه چنین مداخلاتی است.</p>		<p>عدم پرداختن به سیاست‌گذاری مبتنی بر شواهد</p>
<p>اقدامات فناورانه‌ای که در پاسخ به وضعیت اضطراری سلامت عمومی مورد استفاده واقع شدند دارای یک مبنای عقلانی مبتنی بر تحقیقات علمی مرتبط هستند تا از رسیدگی اثربخش به وضعیت اضطراری اطمینان حاصل کنند.</p> <p>مسئولین سلامت عمومی یا ارگان‌های دیگر که متشکل از کارشناسان مرتبط هستند باید به نحوی کافی در فرایند تصمیم‌گیری دخیل شده باشند تا سیاست‌گذاران بتوانند تضمین کرده و نشان دهند که مداخلات آن‌ها مبتنی بر تحقیقات مرتبط بوده و برای شرایط خاص وضعیت اضطراری که در دست رسیدگی شدن است، مناسب است.</p>	<p>توصیه‌ها</p>	

## چگونه توصیه‌ها را پیاده‌سازی کنیم؟

- مسئولین کشور باید وضعیت امور مربوط به توزیع زیرساخت‌های حیاتی اینترنت در کشورهای خود را شناسایی کنند تا حوزه‌های نیازمند به توسعه را تشخیص دهند.
- سرمایه‌گذاری‌ها می‌توانند روی زیرساخت حیاتی اینترنت در مناطق شناسایی‌شده که نیازمند توسعه هستند، انجام شود. این کار می‌تواند شامل یارانه برای طرح‌های تلفن همراه، فراهم کردن نقاط اتصال Wi-Fi رایگان و حتی برنامه‌های سواد دیجیتال باشد.
- پیش از اعزام برنامه، سیاست‌گذاران و قانون‌گذاران باید با حضور کارشناسان این موضوع را بررسی کنند که آیا این فناوری برای توجیه وجود خود، ارزش قابل توجهی را به مبارزه علیه کووید می‌افزاید یا صدمات جانبی زیادی ایجاد می‌کند. نتایج چنین بحث‌هایی می‌توانند در قالب توصیه‌هایی ارائه شده و به کمیته تصمیم‌گیری مذکور در پایین ارائه گردد. در هر صورت، این توصیه‌ها باید در منابع باز در دسترس عموم قرار گیرد.
- کمیته‌ای با اختیارات تصمیم‌گیری متشکل از: بخش مستقل سلامت عمومی (همه‌گیرشناسان یا اپیدمیولوژیست‌ها)، متخصصان فناوری، سیاست‌گذاران و مقامات حفاظت از داده‌ها برپا کنید. مطمئن شوید که تصمیماتی که از سوی کمیته اتخاذ شده‌اند تحت نظارت و توازن هستند.



<p>کووید-۱۹ به سرعت در سرتاسر جهان شیوع پیدا کرد و نوع تازه‌ای از مخاطره را برای بیشتر مردم ایجاد کرد. بدین ترتیب شیب منحنی یادگیری برای دولت‌ها و شهروندان به طور مشابهی تند بود، و - بویژه در ابتدا - مستلزم انجام اقدامات با دانشی محدود بود. مکان‌های بسیاری شاهد شکل‌گیری موجی از تئوری‌های توطئه حول بیماری بودند. شواهد در حال رشدی وجود دارد، که نشان می‌دهد پایبندی به فاصله‌گیری اجتماعی و قرنطینه‌سازی، و نیز مشوق‌های واکسیناسیون، به شدت تحت تأثیر کارزارهای آگاهی عمومی است که به درستی طراحی شده‌اند. در تعدادی از محل‌ها، این کارزارها سهمی در پایبندی فعالانه‌تر در اقدامات سلامت عمومی ایفا کردند، مانند تولید محلی ماسک‌ها، در جایی که در دسترس نبودند، و تمایل به واکسیناسیون وجود نداشت.</p>	ارزیابی	عدم آگاهی عمومی در مورد تحقیقات علمی که زیربنای اقدامات کووید را تشکیل می‌دهند.
<p>«انتلاف‌هایی از مشتاقان» با نمایندگی وسیع از جامعه مدنی ایجاد کنید. کارزارهای آگاهی‌رسانی، هم آنلاین و هم آفلاین، می‌توانند پایبندی به اقدامات سلامت عمومی را تسهیل کنند و از دست رفتن اعتماد جلوگیری کنند. جمعیت‌شناسی‌های مختلف را، بویژه در مورد اجتماعات به حاشیه رانده شده، در نظر بگیرید، و با گروه‌های مورد اعتماد درون آن اجتماعات کار کنید.</p>	توصیه	
<p>چگونه توصیه را پیاده‌سازی کنیم؟</p>		
<p><input type="checkbox"/> همکاری‌های اجتماع-محور در مداخلات می‌تواند به نحوی اثربخش آگاهی میان گروه‌های به حاشیه رانده شده را افزایش دهد. ۱۵</p>		

<p>برخی از چارچوب‌های حقوقی تمهیدی برای نسخه‌های تسریع شده فرایند تدارکات قرار می‌دهند که به دولت‌ها اجازه می‌دهند که منابع مورد نیاز را برای پاسخ سریع و اثربخش به وضعیت اضطراری پیش رو بدست آورند. هرچند، در جایی که فرایندهای تسریع شده و جامع برای تدارکات عمومی موجود نباشند و دنبال نشوند، ممکن است طیفی از مسائل، از جمله کمبود تجهیزات حیاتی بوجود بیاید.</p>	ارزیابی	
<p>قوانینی دائمی، در برابر قوانین موردی برای تدارکات عمومی در طول وضعیت‌های اضطراری برقرار کنید تا از دستیابی کارآمدتر به کالاها و خدمات اطمینان حاصل شود.</p> <p>این کار می‌تواند با سامان‌دهی‌های خریداری پیشرفته‌ای همراه گردد تا تأمین سریع کالاها و خدماتی ممکن است در رسیدگی به وضعیت اضطراری لازم باشند، صورت بگیرد.</p>	توصیه	
<p>چگونه توصیه را پیاده‌سازی کنیم؟</p>		<p>عدم کارایی تدارکات عمومی در دوران کووید-۱۹</p>
<p>□ پیش‌نویس قانون‌گذاری برای تدارکات عمومی را معرفی کنید که منعکس‌کننده بخش‌های مربوط به مدل قانونی آنسیترال (UNCITRAL) درباره تدارکات عمومی یا سایر استانداردهای بین‌المللی مشابه باشند، با توجه ویژه به تمهیداتی که به تدارکات عمومی در موارد با فوریت حاد مربوطند.</p> <p>این تمهیدات ممکن است بعنوان مثال، شامل موارد زیر باشند:</p> <ul style="list-style-type: none"> <li>● تدارکات تک-منبعی تنها در جایی مجاز است که نیازی فوری به انجام آن به خاطر یک رویداد فاجعه‌بار وجود داشته باشد، که در آن روش‌های دیگر تدارکات، به علت زمان دخیل در استفاده از آن‌ها یا روش‌های دیگر عملی نباشند (انعکاس‌دهنده اصل ۳۰.۵ (ب) از آنسیترال).</li> </ul>		

<ul style="list-style-type: none"> <li>● برای تعیین پیشنهاد و قیمت باید مذاکرات با تأمین‌کننده برگزار شوند، مگر اینکه شرایط تدارکات به نحوی باشند که مذاکرات امکان‌پذیر نباشند (انعکاس‌دهنده اصل ۵۲ آنسیترال).</li> <li>● پیش از اینکه وضعیت اضطراری موجب فوریت شود، مطابق با توافق‌نامه‌هایی که میان دولت و آن تأمین‌کنندگان نهایی شده است، کالاها یا خدمات باید از تأمین‌کنندگان مشخص در موارد فوری تهیه شوند.</li> </ul>	
---	--

خزش عملکرد و پیامدهای ناخواسته		
روند ۱		
<p>در برخی از کشورهای مورد نظر، برنامه‌ها و اقدامات برای مبارزه با کووید-۱۹، اغلب بدون چارچوب‌های قانونی مقرر برای تنظیم استفاده از آن‌ها یا دادن اجازه به مسئولین کشور برای ایجاد و اعزام برنامه‌های کووید، در دستور کار قرار گرفتند. در برخی موارد، هیچ قانون‌گذاری مقرری در رابطه با پردازش داده‌های شخصی مورد نیاز برای کارکرد برنامه‌های کووید وجود نداشته است. بخاطر چنین فروگذاری‌هایی در قانون‌گذاری، خزش عملکرد به یک احتمال جدی‌تر بدل شد، یعنی مسئولین کشور می‌توانستند از این اقدامات و داده‌های شخصی برای اهدافی فراتر از کووید-۱۹ استفاده کنند.</p>	ارزیابی	<p>نبود چارچوب قانونی برای اعزام و استفاده از برنامه‌های کووید</p>
<p>پیاده‌سازی یک چارچوب حقوقی جامع که مبنایی را برای توسعه اقداماتی فراهم می‌آورد که بخشی از پاسخ اضطراری را تشکیل می‌دهند. تمهیدی باید در قانون اساسی یا نظام حقوقی کشور صورت گیرد، که برای بازهای محدود، نقش‌های تغییر یافته‌ای را برای ارگان‌های دولت در طول وضعیت اضطراری دایر می‌کند، تا نظارت‌ها و پادمان‌های کافی جهت محافظت از حقوق فردی حفظ شوند.</p>	توصیه	
<p>چگونه توصیه را پیاده‌سازی کنیم؟</p>		
<p>□ معرفی پیش‌نویس قانون‌گذاری جهت ایجاد تمهیدات ذیل:</p>		

- نهاد اجرایی/دولت باید تحت شرایطی معین وضعیت اضطراری اعلام کند، مشروط به اینکه اعلام وضعیت اضطراری از سوی قوه مقننه ضمانت اجرایی داشته باشد.
- قوه مقننه و قضائیه در طول وضعیت اضطراری نظارت خود را حفظ می‌کنند.
- دولت تنها هنگامی می‌تواند اقداماتی در پاسخ به وضعیت اضطراری اعلام شده انجام دهد، که ماهیت و دامنه این اقدامات به روشنی مشخص شده باشد.
- اقدامات پیاده‌سازی شده در پاسخ به وضعیت اضطراری با قوانین موجود سازگاری دارند، این قوانین شامل و نه محدود به قانون حفاظت از داده‌ها هستند.
- دولت اطمینان حاصل می‌کند هر گونه تخطی از حقوق فردی که در نظام حقوقی یا قانون اساسی‌اش وجود دارد، آزمون تناسب را با موفقیت پشت سر می‌گذارد.
- اقدامات تصویب شده در پاسخ به وضعیت اضطراری اعلام شده مشمول بازبینی و تأیید پس‌از اجرا از سوی قوه مقننه هستند.
- وضعیت اضطراری و اقدامات پیاده‌سازی شده در پاسخ به آن باید دارای محدودیت زمانی دقیق باشند و هر گونه تمدید آن منوط به موافقت قبلی قوه قانون‌گذاری است.

<p>گاهی اوقات در یک وضعیت اضطراری سلامت عمومی، دولت‌ها اقداماتی را اعمال می‌کنند که ممکن است به تبعیض علیه گروه‌های معینی منجر شود. در متن همه‌گیری کووید-۱۹، با وجود اینکه منابع یا حمایت کافی برای مردم وجود نداشت تا از آن‌ها تبعیت کنند، اقدامات معینی اجباری شدند. به عنوان مثال، برخی کشورها، با وجود دسترسی محدود به واکسن‌ها و/یا واکسینه نبودن بخش‌های اعظمی از جمعیت مردم را ملزم می‌کردند تا پیش از اینکه دسترسی به مکان‌های عمومی یا سفر به آن‌ها داده شود، خود را در برابر کووید-۱۹ واکسینه کنند.</p>	<p>ارزیابی</p>	<p>دسترسی تقلیل‌یافته و نابرابر به جامعه</p>
<p>دولت‌ها باید تضمین کنند که اقدامات سلامت عمومی الزامی در طول یک وضعیت اضطراری سلامت عمومی با منابع و تسهیلات لازم و موجود پشتیبانی می‌شوند، تا مردم بتوانند از چنین اقداماتی پیروی کنند و به نحو غیر منصفانه از دسترسی به جامعه منع نشوند.</p>	<p>توصیه</p>	
<p>چگونه توصیه را پیاده‌سازی کنیم؟</p>		
<p><input type="checkbox"/> اطمینان حاصل کنید که ملزومات دسترسی به جامعه شامل واکسیناسیون، آزمایش و بدیل‌های کاغذ-محور برای برنامه‌ها به صورت گسترده برای تمامی جمعیت در دسترس هستند.</p> <p><input type="checkbox"/> مراکز واکسیناسیون و مکان‌های آزمایش هم باید در مناطق شهری و هم روستایی قابل دسترس باشند، و بدیل‌های کاغذ-محور/غیر-دیجیتال برای برنامه‌ها باید به آسانی قابل دسترس باشند.</p>		

## ۲. توصیه‌ها برای توسعه‌دهندگان برنامه، متصدیان و نهادهای عمومی کمیسیون‌دهنده

عموم مردم چه انتظاری می‌توانند از ذی‌نفعان دخیل در پاسخ همه‌گیری داشته باشند و چرا؟

برای عموم مهم است بدانند که توسعه‌دهندگان و متصدیان برنامه و نیز نهادهای عمومی کمیسیون‌دهنده برنامه‌های کووید-۱۹ می‌توانند شماری از گام‌ها را برای ضمانت استفاده مؤثر و پایدار از برنامه‌ها بردارند. این گام‌ها، مشتمل بر انتخاب‌های توسعه و طراحی، پادمان‌ها و آیین‌های دادرسی در کنار هم به عنوان بخشی از راهبرد وسیع‌تر سلامت عمومی، اعتماد به و موفقیت استفاده از برنامه‌های کووید-۱۹ را تسهیل می‌کنند.

در عمل، ویژگی‌های فنی و طراحی برنامه‌های کووید اثری بر جمع‌آوری و استفاده از داده‌های شخصی افراد، و همچنین برخورداری از حقوق بنیادین، از جمله حق حریم خصوصی دارند.

به عنوان نمونه، در دسترس قرار دادن کد برنامه به صورت عمومی اعتماد جامعه مدنی و عموم مردم را ترغیب می‌کند. بکار گرفتن اصول حریم خصوصی مبتنی بر طراحی می‌تواند از خزش عملکرد و دیگر پیامدهای ناخواسته جلوگیری کند که منجر به از دست رفتن اعتماد و آسیب‌های ناشی از معرفی برنامه می‌شود. بکارگیری این اصول همچنین شامل محدود کردن استفاده از داده‌های غیر ضروری مانند داده‌های مکان می‌شود، که معمولاً برای آن جایگزین‌هایی وجود دارد. مدیریت داده‌های (شخصی) باید به صورت واضح، با معطوف کردن توجه خاص به هدف، حساسیت داده‌ها، ذخیره‌سازی، امنیت، و محدودیت اشتراک‌گذاری تعریف شود. هر نوعی از اشتراک‌گذاری، بویژه با بخش خصوصی، با امکان استئنا بودن داده‌های پژوهشی، باید نقش روشنی در استراتژی سلامت عمومی ایفا کند، بویژه در جهت‌بخشی به سیاست‌های سلامت عمومی آتی.

درون چنین چارچوب‌هایی که به حقوق افراد احترام می‌گذارند، برنامه‌ها نیز باید از طریق پیش‌بینی تخلفات بالقوه نسبت به تغییرات آتی مقاوم باشند. عملکرد برنامه تنها در صورتی می‌تواند تضمین شود که هر گونه تخلف صورت گرفته بتواند به صورت شفاف رسیدگی شود.

<p>از نظر شفافیت در تمامی برنامه‌های تحلیل شده نقصان‌هایی وجود دارد، اگرچه تفاوت‌های چشمگیری نیز در بین آن‌ها هست. تنها سه برنامه منبع کد خود را برای بازرسی در دسترس می‌گذارند. عمده آن‌ها از میهم‌سازی کد، پژواک و دیگر تکنیک‌های ضد-تحلیل استفاده می‌کنند که تعیین و تأیید اطمینان‌پذیر حضور برخی رفتارها را دشوار می‌کنند. چنین اقدام‌هایی بر اعتماد اثر منفی می‌گذارند و با شفافیت بین‌المللی و توصیه‌های مهندسی حریم خصوصی ناسازگار هستند.</p>	<p>ارزیابی</p>	
<p>همه برنامه‌های موجود و مرتبط با کووید را در همه پلتفرم‌ها به صورت متن‌باز ایجاد کنید. با دسترس‌پذیر و بازرسی‌پذیر ساختن عمومی کدهای سمت سرور، افراد می‌توانند همکاری کنند، کدهای خود را برای آسیب‌پذیری و ارسی کنند، و یک سیستم داوری برای بازبینی راه‌اندازی کنند.</p>	<p>توصیه</p>	<p>همه برنامه‌ها کدهای خود را در دسترس عموم قرار نمی‌دهند</p>
<p>چگونه توصیه را پیاده‌سازی کنیم؟</p>		
<p><input type="checkbox"/> کد منبع را در گیت‌هاب (GitHub) یا در وبسایت/پلتفرم متن‌باز مشابه دیگری منتشر کنید</p> <p><input type="checkbox"/> از هیچ‌گونه تکنیک مبهم‌سازی برای پنهان کردن یا تحریف کد منبع استفاده نکنید، چرا که این تکنیک‌ها و ارسی مستقل کد را دشوار می‌کنند.</p>		

<p>برخی از این همکاری‌ها به صورت توافق‌نامه‌های اشتراک‌گذاری-داده شکل می‌گیرند. سایر همکاری‌ها حول مساعدت شرکت‌های خصوصی به دولت‌ها برای اجرای عملیات دیدبانی و نظارتی شکل گرفتند. اشکال اصلی این مشارکت‌ها غفلت از بازرسی‌های تنظیمی و مقرراتی مناسب است. بعلاوه، تمامی کشورهای تحت بازبینی فاقد یک چارچوب جامع برای محافظت از داده‌ها هستند، که بیش از پیش مشروعیت مشارکت‌های دولتی-خصوصی را زیر سؤال می‌برد. این امر به ایجاد زمینه‌هایی برای خزش عملکرد و استفاده نامتوازن از قدرت می‌انجامد.</p>	<p>ارزیابی</p>	
<p>فعالیت‌های اشتراک‌گذاری-داده میان نهادهای دولتی و بخش خصوصی را در چارچوب روشنی قرار دهید.</p>	<p>توصیه</p>	
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p>اعزام و استقرار راهکارهای فناورانه با همکاری بخش خصوصی</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> به مشخصات الزامات نرم‌افزاری مرتبط مراجعه کنید تا ضرورت اشتراک‌گذاری داده‌ها برای عملکرد یا ویژگی‌های برنامه یا سامانه مشخص شود.</li> <li><input type="checkbox"/> برای مستند کردن داده‌های به اشتراک‌گذاشته شده با نهادهای دولتی و اهدافی که بخاطر آن، داده‌ها به اشتراک گذاشته می‌شوند، نقشه‌های جریان داده و سوابق عملیات پردازشی ایجاد کنید. قالب ارائه شده در پایین را در قسمت «ابزارهای پیاده‌سازی» به عنوان مثالی از اینکه چنین مستندی می‌تواند دربرگیرنده چه مواردی باشد، ملاحظه کنید.</li> </ul>		



□ با متخصصین حقوقی برای تهیه پیش‌نویس بندهایی در رابطه با داده‌هایی که قرار است با نهادهای دولتی به اشتراک گذاشته شوند، اهداف این اشتراک‌گذاری و سایر تعهدات مربوطه و قابل اطلاق به آن مشورت کنید. این موارد باید در هر قراردادی میان توسعه‌دهنده و دولت برای آماده‌سازی خدمات گنجانده شوند.

### ابزارهای پیاده‌سازی مرتبط

- قالب مشخصات الزامات نرم‌افزار
- قالب نقشه جریان داده برای برنامه گذرنامه و اکسن

### خزش عملکرد و پیامدهای ناخواسته

روند ۲

<p>می‌توان ادعا کرد که سامانه‌های متمرکز نسبت به سامانه‌های تمرکززدایی شده از انطباق کمتری با مفهوم حریم خصوصی مبتنی بر طراحی برخوردارند. در یک سامانه متمرکز، بیشتر پردازش مورد نیاز روی یک سرور مرکزی تحت تصدی مرجع عمومی رخ می‌دهد، که داده‌های شخصی حساس را برای آن مراجع دسترس‌پذیرتر می‌کند. در مقابل، در یک سامانه تمرکززدایی شده، بیشتر پردازش روی دستگاه کاربر انجام می‌گیرد، به نحوی که داده‌های شخصی با بالاترین میزان حساسیت به صورت محلی باقی می‌مانند و تنها داده‌های شبه‌نام‌واره‌ای شده با دستگاه‌های دیگر و سرور مرکزی به اشتراک گذاشته می‌شوند. این امر در مورد کشورهایی که از GAEN API (واسط برنامه‌نویسی اعلان در معرض قرارگیری گوگل/اپل) استفاده می‌کنند صادق است.</p>	<p>ارزیابی</p>	<p>بیشتر کشورها سامانه‌های متمرکز را برای برنامه‌های ردیابی تماس خود انتخاب می‌کنند</p>
<p>رهیافت خود را بر اساس توسعه برنامه با استفاده از یک چارچوب حریم خصوصی مبتنی بر طراحی اتخاذ کنید.</p>	<p>توصیه</p>	

چگونه توصیه‌ها را پیاده‌سازی کنیم؟

<p>□ مشخصات الزامات نرم افزار را برای فرایند توسعه نرم افزار توسعه دهید که عملکردهای پیشنهادی برنامه کووید را همراستا با اصول حریم خصوصی مرتبط یا الزامات قانونی قرار می دهد. قالب ارائه شده را در پایین در قسمت «ابزارهای پیاده سازی» مشاهده کنید.</p> <p>□ برای ارزیابی مخاطرات حریم خصوصی یا حفاظت از داده ها، در خلال توسعه برنامه های کووید، توصیه یک متخصص شخص ثالث و مستقل را جویا شوید تا اطمینان حاصل کنید، اصول حفاظت از داده ها و حریم خصوصی در هر مرحله از چرخه توسعه، پیش از استقرار برنامه، بدرستی تفسیر و پیاده سازی می شوند.</p>	
ابزارهای پیاده سازی مرتبط	
● قالب مشخصات الزامات نرم افزار	

خزش عملکرد و پیامدهای ناخواسته		
روند ۳		
جمع آوری داده های موقعیت مکانی به مراجع ملی اجازه می دهد تا کاربران را ردیابی کنند و نظارت ها و دیدبانی های مزاحمت آمیز دیگری را انجام دهند که فراتر از نیازهای سلامت عمومی است. این امر هنگامی که داده های مکان می توانند «عادت های کاربران، نشانی منزل، داده های محل کار، و حتی اعتقادات مذهبی (به عنوان مثال محل عبادت)» را آشکار سازند، محل نگرانی ویژه است.	ارزیابی	استفاده متداول از داده های مکان
میزان داده های جمع آوری شده، به طور خاص داده های شخصی یا قابل شناسایی را؛ را به میزانی که اکیداً لازم است کاهش دهید، این کار حذف نیازمندی به موقعیت مکانی GPS را نیز در بر می گیرد.	توصیه ها	

<p>درخواست‌ها برای داده‌های مکان را از هر برنامه‌ی ردیابی تماسی برای حفاظت از حریم خصوصی حذف کنید.</p> <p>یک گزینه‌ی واضح با دسترسی آسان برای حذف حساب کاربری و اطلاعات از برنامه و هم از سرور ارائه دهید.</p>		
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p><input type="checkbox"/> در طول فرایند تبدیل طراحی سطح بالا به سطرهایی از کد، بازبینی‌های منظمی از کد به عمل آورید.</p> <p><input type="checkbox"/> متخصصان و کارشناسان حفاظت از داده و حریم خصوصی را دخیل کنید تا اطمینان حاصل کنید عملکرد برنامه از مشخصات الزامات نرم‌افزار که دربردارنده‌ی الزامات و اصول قابل اطلاق است، پیروی می‌کند.</p>		

<p>خزش عملکرد و پیامدهای ناخواسته</p>		
<p>روند ۴</p>		
<p>اصل حریم خصوصی مبتنی بر طراحی، به طور کامل در ارتباط با کیت‌های توسعه‌ی نرم‌افزاری (SDKs) که در کشورهای مورد توجه اعزام شده‌اند، دنبال نمی‌شود. به طور خاص، استفاده از کتابخانه‌ی فایربیس گوگل (Google Firebase Library)، یا در واقع کیت‌های توسعه‌ی نرم‌افزاری (SDKs) دیگر، به صورت واضح در سیاست‌های حریم خصوصی مربوطه ترسیم نشده است.</p>	<p>ارزیابی</p>	<p>استفاده متداول از ابزارها برای ردیابی و تجزیه و تحلیل</p>
<p>اطلاعات روشنی در رابطه با نوع داده‌های جمع‌آوری شده و هدف از آن، محل ذخیره داده‌ها و طول مدت ذخیره‌سازی آن‌ها، افرادی که داده‌ها با آن‌ها به اشتراک گذاشته می‌شود و اهداف آن، و پروتکل‌های امنیتی تمامی این عملکردها فراهم کنید.</p>	<p>توصیه‌ها</p>	

<p>سیاست‌های حفظ حریم خصوصی دقیق‌تری را (نوشته شده به همه زبان‌های محلی) منتشر کنید و از هر شخص ثالث دیگری که به داده‌ها دسترسی دارد به صراحت نام ببرید.</p>		
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p>□ ارزیابی‌هایی از سازندگان شخص ثالثی بعمل آورید که ارائه‌دهنده کیت‌های توسعه نرم‌افزار (SDKs) و کتابخانه‌های نرم‌افزاری دیگری هستند که قرار است در برنامه کوید استفاده شوند. این ارزیابی‌ها باید شامل یک بازبینی از سیاست‌های حریم خصوصی و مستندسازی‌های مرتبط دیگر در رابطه با حفاظت از داده‌ها، و نیز یک بازرسی از کدهای شخص ثالث وارد شده در فضای کاری جهت توسعه برنامه باشند.</p>		

تأثیرگذاری بر سلامت عمومی

روند ۱

<p>تا قسمتی به خاطر اطلاعات نادرست و نظریات توطئه درباره کووید-۱۹، مواردی وجود دارند که در آن‌ها افراد تلاش برای دستیابی به کدهای QR جعلی کردند تا بتوانند به مکان‌ها دسترسی داشته باشند یا سفر کنند. در برخی کشورها، تعداد موارد تخلف به ده‌ها هزار می‌رسید.</p>	<p>ارزیابی</p>	
<p>تلاش‌ها برای تخلف را پیش‌بینی کنید و از ارزیابی مناسب همه طرفین دخیل، شامل شرکای بخش خصوصی اطمینان حاصل کنید.</p> <p>در حدود اصول حریم خصوصی مبتنی بر طراحی، اجازه حذف گواهی‌های بدست آمده به صورت جعلی را بدهید و اطمینان حاصل کنید این فرآیند در بیانیه حریم خصوصی به صورت شفاف تبیین شده است.</p>	<p>توصیه‌ها</p>	<p>تخلف در دستیابی به گواهی‌های کووید</p>
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p>□ آزمون‌های صحت‌سنجی بیشتری انجام دهید تا مطمئن شوید سامانه مطابق با الزامات عمل می‌کند. این کار باید آزمون واحد (توجه به عملکردها و اجزای منفرد سامانه)، آزمون یکپارچه‌سازی (توجه به تعاملات میان دسته‌هایی از اجزا)، آزمون سامانه (توجه به بخش‌های کامل شده از کل سامانه)، و آزمون مقبولیت (ارائه سامانه به کاربران انتخابی، یعنی آزمایش‌کنندگان آلفا و بتا) را پوشش دهد.</p>		

<p>برنامه‌های کووید دارای سطوح متفاوتی از موفقیت به لحاظ دستیابی به حریم خصوصی مبتنی بر طراحی هستند. اگر پایبندی به این مفهوم رعایت نشود، کاربران ممکن است به نحوی نامتناسب صدمه ببینند. چنین صدماتی می‌توانند به این منجر شوند که توسعه‌دهندگان برنامه، و نیز دولت‌هایی که خواستار خدمات آن‌ها هستند، نتوانند بدرستی حقوق حریم خصوصی و حقوق حفاظت از داده‌های افراد را حفظ کنند. برخی برنامه‌ها از کیت‌های توسعه نرم‌افزاری (SDKs) استفاده می‌کنند که داده‌ها را برای اهداف دیگری، منقطع از هدف اصلی برنامه (سلامت عمومی) پردازش کنند یا داده‌ها را با اشخاص ثالث دیگری به اشتراک بگذارند. بعلاوه، بیشتر توسعه‌دهندگان برنامه درباره کیت‌های توسعه نرم‌افزاری (SDKs) شخص ثالث یا کتابخانه‌های نرم‌افزاری مورد استفاده در برنامه‌هایشان شفاف نیستند یا کد منبع خود را عمومی نمی‌کنند و یا بالعکس آن را مبهم‌سازی می‌کنند. علاوه بر این، بیشتر برنامه‌های کووید بدون اینکه یک ارزیابی قبلی از اثرگذاری بر حفاظت از داده‌ها یا حریم خصوصی صورت از آن‌ها صورت گرفته باشد، اعزام و مستقر می‌شوند تا از مخاطرات بالقوه حفاظت از داده‌ها یا حریم خصوصی کاسته شود. هر چند، برخی از کشورها تلاشی در جهت فراهم کردن راهنمای حفاظت از داده‌ها برای مکان‌های عمومی که ملزم به جمع‌آوری داده‌های شخصی مشخص برای اهداف ردیابی تماس بودند، صورت ندادند.</p>	<p>ارزیابی</p>	<p>فقدان حریم خصوصی مبتنی بر طراحی در برنامه‌های کووید</p>
<p>تنها از کیت‌های توسعه نرم‌افزاری (SDKs) استفاده کنید که داده‌های شخصی لازم برای اهداف برنامه (یعنی ردیابی تماس و/یا نمایش اطلاعات سلامت) را پردازش می‌کنند.</p> <p>اطلاع‌رسانی‌هایی برای حریم خصوصی تهیه کنید که کاربران برنامه را با زبانی روشن و موجز درباره اینکه چگونه داده‌های آن‌ها جمع‌آوری و پردازش می‌شود، مطلع می‌کند و چنین اطلاع‌رسانی‌هایی را به شیوه‌ای کاربرپسند ارائه کنید.</p>	<p>توصیه‌ها</p>	

<p>کد منبع برنامه‌ها را منبع‌باز کنید تا امکان صحت‌سنجی مستقل عملکردها و عملیات پردازش برنامه فراهم شود.</p> <p>هنگامی که سازمان‌دهندگان مکان‌های عمومی داده‌های شخصی را پردازش می‌کنند (به عنوان مثال هم به کمک ردیابی تماس دیجیتال و هم به صورت دستی)، راهنمایی‌هایی دربارهٔ چگونگی پردازش داده‌ها ارائه کنید به نحوی که مروج و منتفع حفاظت صحیح از داده‌ها باشد.</p> <p>قبل از استقرار و اعزام برنامه، ارزیابی‌هایی از اثرگذاری بر حریم خصوصی یا حفاظت از داده‌ها بعمل آورید تا مخاطرات بالقوهٔ حریم خصوصی و حفاظت از داده‌ها را شناسایی کنید، و اقدامات کاهندهٔ مناسبی را برای مخاطرات شناسایی شده توسعه دهید.</p>		
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<ul style="list-style-type: none"> <li>□ برای ارزیابی مخاطرات حریم خصوصی یا حفاظت از داده‌ها، در خلال توسعهٔ برنامه‌های کووید، توصیهٔ یک متخصص شخص ثالث و مستقل را جویا شوید تا مطمئن شوید، اصول حفاظت از داده‌ها و حریم خصوصی در هر مرحله از چرخهٔ توسعه، پیش از استقرار برنامه، بدرستی تفسیر و پیاده‌سازی شده‌اند.</li> <li>□ مشخصات الزامات نرم‌افزار را برای فرایند توسعهٔ نرم‌افزار توسعه دهید که عملکردهای پیشنهادی برنامهٔ کووید را هم‌راستا با اصول حریم خصوصی مرتبط یا الزامات قانونی قرار می‌دهد. قالب ارائه شده را در پایین در قسمت «ابزارهای پیاده‌سازی» مشاهده کنید.</li> <li>□ ارزیابی‌هایی از سازندگان شخص ثالثی بعمل آورید که ارائه‌دهندهٔ کیت‌های توسعهٔ نرم‌افزار (SDKs) و کتابخانه‌های نرم‌افزاری دیگری هستند که قرار است در برنامهٔ کووید استفاده شوند. این ارزیابی‌ها باید شامل یک بازبینی از سیاست‌های حریم خصوصی و مستندسازی‌های مرتبط دیگر در رابطه با حفاظت از داده‌ها، و نیز یک بازرسی از کدهای شخص ثالث وارد شده در فضای کاری جهت توسعهٔ برنامه باشند.</li> </ul>		

- پیش‌نویسی از اطلاع‌رسانی‌های حریم خصوصی، به همراه یک اطلاع‌رسانی با قالبی کوتاه تهیه کنید که به کاربران برای بار اول نشان داده می‌شود و از آن پس نیز در دسترس است. قالب ارائه شده در پایین را در قسمت «ابزارهای پیاده‌سازی» مشاهده کنید.
- منبع را در گیت‌هاب (GitHub) یا در وبسایت/پلتفرم مشابه دیگری منتشر کنید.
- از تکنیک‌های مبهم‌سازی که بازرسی کد به صورت مستقل را دشوار می‌سازند برای پنهان ساختن یا تحریف کد منبع استفاده نکنید.
- پیش‌نویسی از راهنمای حفاظت از داده‌ها برای متصدیان محل آماده کنید، از جمله (۱) چه داده‌هایی را باید جمع‌آوری کنند و چرا، (۲) داده‌ها چگونه باید جمع‌آوری و نگهداری شوند، (۳) الزام حفظ محرمانه داده‌ها، و (۴) داده‌ها فقط باید با اشخاص ثالث مشخصی که با اهداف جمع‌آوری آن‌ها مرتبط هستند، به اشتراک گذاشته شوند.
- از قالب تهیه شده در پایین، در قسمت «ابزارهای پیاده‌سازی» به عنوان نقطه آغاز برای تکمیل ارزیابی اثرگذاری بر حفاظت از داده‌ها یا حریم خصوصی در طول توسعه برنامه استفاده کنید.

#### ابزارهای پیاده‌سازی مرتبط

- قالب مستندات برای مشخصات الزامات نرم‌افزار
- قالب اطلاع‌رسانی برای حریم خصوصی برنامه‌های ردیابی تماس
- قالب ارزیابی برای اثرگذاری بر حریم خصوصی / محافظت از داده‌ها



<p>دولت‌ها تمایل دارند از روابط خود با بخش خصوصی برای نیل به اهداف و سیاست‌های مختلف بهره ببرند. کووید-۱۹ از این قاعده مستثنی نیست؛ بسیاری از دولت‌ها از سامانه‌ی اعلان در معرض قرارگیری گوگل/اپل (Google/Apple Exposure Notification System) یا به اختصار (GAES) برای ساخت برنامه‌های ردیابی تماس دیجیتال خود استفاده می‌کنند؛ برخی کشورها به شرکت‌های مخابراتی مراجعه می‌کنند تا به داده‌ها جهت ایجاد نقشه‌های حرارتی و ردیابی شیوع ویروس دستیابی پیدا کنند؛ حکومت‌ها همچنین از سامانه‌هایی دوربینی به منظور پایش تبعیت از قوانین قرنطینه استفاده می‌کنند و بدین ترتیب موجب گسترش دستگاه دیدبانی دولت می‌شوند. هرچند، این همکاری‌ها اغلب در ابری از محرمانگی مخفی شده‌اند، یا در زمینه‌ی کووید-۱۹، از شرایط اضطراری برای فرار از محدودیت‌های مقرراتی معمول استفاده می‌کنند، محدودیت‌هایی که وظیفه دارند تا از محفوظ ماندن حقوق افراد اطمینان حاصل کنند.</p>	<p>ارزیابی</p>	<p>ظهور همکاری‌های دولتی-خصوصی و فقدان شفافیت</p>
<p>شرایط همکاری و مشارکت را برای تمامی برنامه‌هایی که در مشارکت دولتی-خصوصی توسعه داده شده‌اند را در عرصه‌ی عمومی منتشر کنید.</p>	<p>توصیه</p>	
<p>چگونه توصیه‌ها را پیاده‌سازی کنیم؟</p>		
<p>□ دولت‌ها باید از شفافیت همکاری‌های دولتی-خصوصی اطمینان بعمل آورند (به عنوان مثال از طریق پذیرش درخواست‌های آزادی اطلاعات)</p>		

### ۳. ابزارهای پیاده‌سازی

در پایین قالب‌ها و همچنین مثال‌هایی از بهترین شیوه‌ها برای تسهیل پیاده‌سازی برخی از توصیه‌های ارائه شده در جعبه ابزار برنامه‌های کووید-۱۹ موجود است.

## حریم خصوصی مبتنی بر طراحی برای برنامه‌های ردیابی تماس

این مثال مدلی از یک برنامه ردیابی تماس بهبوددهنده حریم خصوصی را ارائه می‌دهد، که کد QR خود را تولید می‌کند تا افراد (با رضایت خود) برای ورود و خروج از محل‌هایی که در این برنامه ثبت شده اند («محل‌های ثبت شده»)، از آن استفاده کنند.

این برنامه‌ها باید به گونه‌ای طراحی شوند که تنها ضبط ورود-خروج از محل‌های ثبت شده را تسهیل کنند در حالی که از حریم خصوصی و داده‌های شخصی محافظت می‌کنند. یعنی:

۱. برنامه کمترین میزان ممکن داده‌های شخصی را پردازش می‌کند؛
۲. داده‌های شخصی تا بالاترین میزان ممکن رمزگذاری شده‌اند و در صورتی که یک مورد ابتلا به کووید مثبت تشخیص داده شود، داده‌ها تنها می‌توانند از جانب مرجع سلامت عمومی بازگشایی شوند.
۳. مرجع سلامت عمومی تنها داده‌های لازم برای ردیابی افراد خاصی را دریافت می‌کند که در محلی مشخص و در بازه زمانی مشخصی که خطر انتقال کووید-۱۹ تشخیص داده شده است، حضور داشته‌اند؛
۴. همه داده‌های ورود-خروج به محض اینکه دیگر برای اهداف ردیابی تماس ارزشی نداشته باشند، حذف خواهند شد.

### دسترسی به و انتقال داده‌ها

- توسعه‌دهنده/متصدی برنامه نباید به داده‌های شخصی جمع‌آوری شده از فرد پردازش شده توسط محل‌های ثبت شده یا انتقال یافته به مسئول سلامت عمومی دسترسی داشته باشد.
- آن محل‌هایی که از برنامه برای ضبط ورود و خروج افراد استفاده می‌کنند، به طور اکید دسترسی محدودی به داده‌های شخصی دارند، که فقط در نقطه ورود و در صورت نیاز به منظور تسهیل و ارسی هویت قابل رؤیت است. تنها کارکنان مجاز در محل به این داده‌ها دسترسی دارند.
- مسئول سلامت عمومی مجاز است تا داده‌هایی در رابطه با افرادی که از یک محل ثبت شده همزمان با شخصی که دارای تشخیص کووید-۱۹ است بازدید کرده‌اند دریافت کند (به منظور تماس با آنها).

هدف تعیین شده

داده‌های شخصی ممکن است با اهداف زیر پردازش شوند:

۱. ارائه یک کد QR به افراد.
۲. ارائه ابزارهای جمع‌آوری داده امن به محل‌های ثبت شده درباره کسانی که در محل حاضر هستند.
۳. ارائه داده‌های مورد نیاز به مرجع سلامت عمومی برای شناسایی و تماس با افرادی که ممکن است در مجاورت شخصی با تشخیص کووید-۱۹ بوده باشند.

داده‌های پردازش شده

۱. درباره افرادی که از برنامه استفاده می‌کنند:

آ. نام و نام خانوادگی و سال تولد، استفاده شده برای اهداف شناسایی و ردیابی تماس.  
ب. شماره تلفن همراه، مورد استفاده برای دریافت QR کد برنامه و در صورت لزوم، دریافت تماس از مرجع سلامت عمومی.  
پ. مهرهای مبتنی بر کد QR ورود و خروج محل، ذخیره شده روی دستگاه فرد و سرورهای برنامه، در صورتی که یک محل ثبت شده بدنیاال درخواست مرجع سلامت عمومی آن را افشا کند، رمزگشایی شده و برای اهداف ردیابی تماس مورد استفاده قرار می‌گیرد.

## ۲. توسط محل‌های ثبت شده

آ. ایمیل، نام کاربری، رمز عبور دارنده حساب کاربری که برای ایجاد و مدیریت حساب کاربری مورد استفاده قرار می‌گیرند.  
ب. نام، ایمیل و شماره‌تلفن سه نقطه محل وقوع تماس، که از سوی مرجع سلامت عمومی برای مکاتبه درخواست‌های افشا برای اهداف ردیابی تماس مورد استفاده قرار می‌گیرند.

## ۳. توسط مرجع سلامت عمومی

آ. نام و نام خانوادگی، سال تولد و شماره همراه کسانی که در یک محل خاص در یک بازه زمانی خاص، به منظور تشخیص هویت و تماس با آن اشخاص برای جلوگیری از گسترش کووید-۱۹.

## حفظ و حذف داده‌ها

### ۱. افراد و کدهای QR ثبت شده:

آ. داده‌های شخصی ارائه شده برای اهداف ثبت‌نام و رسیدن کد QR، به محض اینکه فرد پیوند به کد QR را دریافت کند، حذف می‌شوند.

ب. کد QR شامل داده‌های شخصی رمزگذاری شده در مورد فرد در دو مکان نگهداری می‌شود:

- i. روی دستگاه فرد، تا محل‌ها بتوانند آن را اسکن کنند.
- ii. روی سرور توسعه‌دهنده/متصدی، تا افراد بتوانند تصویر را از طریق پیوند پیامکی (SMS) دریافت کنند.

پ. کاربران می‌توانند کد QR / پیوند میان خود و کد QR خودشان را در هر زمانی حذف کنند، اگرچه هر گونه ضبط ورود و خروجی از آن کد QR همچنان به مدت ۱۴ روز برای اهداف ردیابی تماس حفظ خواهد شد.

ت. هنگامی که مرجع سلامت عمومی الزام قانونی برای محل‌ها را جهت جمع‌آوری داده‌های ورود-خروج باطل می‌کند، همه کدهای QR و ابزار رمزگشایی آن‌ها حذف خواهند شد.

### ۲. داده‌ها درباره محل‌ها و بازدیدکنندگان آن‌ها:

آ. داده‌های شخصی مربوط به یک محل تا زمانی نگهداری می‌شود که:

۱. محل حساب کاربری خود را غیرفعال کند (که در آن صورت داده‌ها در مورد محل و داده‌های ورود-خروج مربوطه تا ۱۴ روز پیش از حذف شدن، برای اهداف ردیابی تماس نگهداری می‌شوند)، یا

۲. مرجع سلامت عمومی الزام قانونی برای محل‌ها را جهت جمع‌آوری داده‌های ورود-خروج باطل می‌کند و همه حساب‌های کاربری حذف می‌شوند.

ب. داده‌های ورود-خروج محل ثبت شده به صورت خودکار پس از ۱۴ روز حذف می‌شوند.  
پ. داده‌های افشا شده برای مرجع سلامت عمومی مطابق با مقررات، سیاست‌ها و رویه‌های کشوری پردازش می‌شوند.

۳. برنامه داده‌های پیامکی (SMS) را حذف می‌کند و پردازنده‌هایی که برنامه از آن‌ها برای ارسال پیام‌ها استفاده می‌کند، داده‌ها را به محض تحویل از روی سرورهایشان پاک می‌کنند.

#### افشای داده به مرجع سلامت عمومی

۱. داده‌های افراد در کد QR آن‌ها رمزگذاری می‌شود. داده‌ها هنگامی که کد QR آنان اسکن شود به محل‌های بازدید شده پیوند داده می‌شوند. مرجع سلامت عمومی می‌تواند فقط در صورت لزوم برای ردیابی تماس، داده‌ها را بازگشایی و به آن‌ها دسترسی پیدا کند.

۲. در شرایطی که، فردی با تشخیص کووید-۱۹ در یک محل ردیابی می‌شود، مرجع سلامت عمومی می‌تواند افشای اطلاعات را از آن محل در رابطه با اشخاص حاضر در همان زمان درخواست کند. محل می‌تواند اجازه انتقال داده‌ها را در رابطه با اشخاص مرتبط تأیید کند، یا در صورت نیاز به تصدیق درخواست اطلاعات بیشتری را از مرجع سلامت عمومی درخواست کند.

۳. مجوز افشا به مرجع سلامت عمومی تنها اجازه دسترسی به داده‌ها در مورد افراد مربوطه را می‌دهد - کسانی که تنها در دوره زمانی معین شده در محل حاضر بودند.

#### امنیت اطلاعات

۱. امنیت اطلاعات از طریق تفکیک داده‌ها، کنترل دسترسی و رمزگذاری قدرتمند محقق می‌شود. ویژگی‌های امنیت اطلاعات، معماری و منبع کد را دانشمندان رایانه مستقل بازرسی و اعتبارسنجی کرده‌اند.

#### کوکی‌ها

۱. وب‌گاه برنامه از کوکی‌های اکیداً ضروری زیر، با هدف تسهیل ایجاد حساب کاربری و ضمانت امنیت داده‌ها استفاده می‌کند:

آ. "csrf\_token" به منظور حفاظت سرویس در برابر جعل درخواست میان وب‌گاهی استفاده می‌شود.

ب. "sessionid" به منظور اختصاص صحیح نشست‌ها از سوی سرور به کاربران اصالت‌سنجی شده و دارای دسترسی به داشبورد استفاده می‌شود.

## قالب مشخصات الزامات نرم افزار

مشخصات الزامات نرم افزار مستندی است که به تفصیل تمام الزاماتی را توصیف می کند که برنامه یا سامانه در حال توسعه باید آن ها را رعایت کند. این مستند می تواند هم می تواند شامل الزامات فنی و قانونی باشد. در پایین مثالی از بخشی از یک مشخصات الزامات نرم افزار است که الزامی قانونی را که یک برنامه ردیابی تماس باید پیاده سازی کند، ارائه می کند.

شناسه الزام	الزام-۳۱
شرح الزام	این برنامه باید از Google/Apple Exposure Notification Framework برای مدل ردیابی تماس استفاده کند.
نویسنده	[نام]
ویراست	۱.۱
تاریخ عرضه	[تاریخ]
کلیدواژه ها	ردیابی تماس تمرکززدایی شده، کمینه سازی داده ها
الزام قانونی	اصل محدودسازی جمع آوری (FIPPS) (اصول کاربری منصفانه اطلاعات) - باید محدودیت هایی برای جمع آوری داده های شخصی وجود داشته باشد و هر گونه داده ای باید از راه های قانونی و منصفانه، و در جای مناسب، با آگاهی یا رضایت شخص صاحب داده ها بدست آورده شود.
<p><u>توصیف سناریو</u></p> <p>برنامه های استفاده کننده از GAEN شناسه های تصادفی تولید می کنند (نشان های رمزنگارانه موسوم به شناساگرهای مجاورت لغزنده) که هر ۱۰-۲۰ دقیقه تغییر می کنند تا مکان دستگاه را انعکاس دهند. هنگامی که کاربر در تماس نزدیک با دستگاه دیگری قرار می گیرد که دارای برنامه ایست که از سامانه GAEN استفاده می کند، آن دو دستگاه شناسه های تصادفی مربوط به خود را از طریق بلوتوث تبادل و ضبط می کنند. کاربران همچنین نتایج مثبت آزمایش کووید-۱۹ خود را نیز در برنامه وارد می کنند، بدین ترتیب فهرستی از شناسه های تصادفی که دستگاه شان طی ۱۴ روز گذشته ضبط کرده است به یک سرور مرکزی تحت تصدی یک مرجع عمومی مخابره می شود.</p> <p>دستگاه موبایل سپس به صورت دوره ای آن شناسه های تصادفی را که ضبط کرده است، با پایگاه داده ای از شناسه های تصادفی متناظر با یک نتیجه مثبت آزمایش کووید-۱۹ مقایسه می کند. اگر تطابقی یافت شود، آنگاه برنامه کاربر را از اینکه ممکن است در معرض شخصی مبتلا به کووید-۱۹ قرار گرفته باشد، مطلع می سازد و به آن ها توصیه می کند که از دستورالعمل مرجع عمومی مربوطه، نظیر دادن آزمایش کووید-۱۹ و/یا قرنطینه کردن خود برای مدتی معین، پیروی کنند.</p> <p><u>مفروضات طراحی</u></p> <p>نشان های رمزنگارانه، روی دستگاه به طور منظم و مطابق با مکان دستگاه تغییر می کنند. سرور مرکزی که متصدی آن مرجع سلامت عمومی است، داده های شخصی کاربران را تنها به شکل شبه ناموارهای (شناسه های رمزنگارانه تصادفی) نگهداری می کند.</p>	

## نقشه جریان داده برای قالب برنامه گذرنامه واکسن

هنگامی که داده‌ها در حال جمع‌آوری و پردازش هستند، یک نقشه جریان داده می‌تواند برای متصل کردن الزامات قانونی به مراحل مشخص چرخه عمر داده‌ها استفاده شود تا پیروی کامل از الزامات تضمین گردد. در پایین مثالی از یک نقشه داده وجود دارد که رؤس کلی الزامات قانونی خاصی که در هر مرحله از چرخه عمر داده‌ها اعمال می‌شوند و عملکرد متناسبی که برنامه به عنوان نتیجه باید داشته باشد را ترسیم می‌کند. شناسه الزام باید با شناسه مشخص شده در مشخصات الزامات نرم‌افزار مرتبط با برنامه تناظر داشته باشد، که مثالی از آن در بالا قابل مشاهده است.

چرخه عمر داده‌ها برای اطلاعات سلامت کاربر		
شرح الزام	شناسه الزام	مرحله چرخه عمر داده
برنامه، وضعیت واکسیناسیون کووید-۱۹، نتایج آزمایش کووید-۱۹ و اطلاعات مصونیت طبیعی کووید-۱۹ کاربر را پردازش خواهد کرد. این اطلاعات سلامت هنگام ثبت نام و متعاقباً هنگامی که کاربر اطلاعات را درون برنامه وارد می‌کند جمع‌آوری خواهد شد.	REQ-51	جمع‌آوری
برنامه اطلاعات سلامت کاربر را به یک کد QR تبدیل می‌کند که کاربر می‌تواند به گردانندگان محل نشان دهد تا بتواند به محل ورود پیدا کند.	REQ-78	استفاده
کد QR کاربر برای متصدیان محل تولید خواهد شد تا آن را اسکن کنند.	REQ-09	افشا
اطلاعات سلامت کاربر تا زمانی که کاربر برنامه را روی دستگاه خود نصب شده نگه می‌دارد، حفظ می‌شود. برنامه داده‌ای در ارتباط با مکانی که کد QR کاربر در آن اسکن شده نگه نمی‌دارد.	REQ-12	نگهداری
اطلاعات سلامت کاربر هنگامی که برنامه حذف می‌شود از بین می‌رود.	REQ-34	نابودی



## قالب اطلاع‌رسانی حریم خصوصی برای برنامه ردیابی تماس

در پایین نمونه‌ای از یک اطلاع‌رسانی با قالبی کوتاه است که می‌تواند برای برنامه‌های ردیابی تماس استفاده شود و به کاربران هنگامی که برای اولین بار در برنامه ثبت نام می‌کنند ارائه شود. هدف رساندن مهم‌ترین اطلاعات دربارهٔ پردازش‌هایی است که برنامه، به همراه گزینه‌ای برای رؤیت اطلاع‌رسانی کامل و یا ارسال یک سؤال به توسعه‌دهنده انجام داده است.

### Your Privacy

-  This app was developed by Company A on behalf of Government 1.
-  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.
-  We use your data because it is necessary for the performance of a task carried out for public health purposes.
-  We collect your data when you first register on the app and as you continue to use the app.
-  We use your data to notify you if you have been in close contact with a person potentially infected with Covid-19.
-  We store your data in Country X and we use servers that are certified for health data hosting.
-  We use SDKs from the following third party providers:
  - Provider 1
  - Provider 2
-  This privacy notice was last updated on 1/1/22.

[See Full Privacy Notice](#) [Have a Question?](#)



English Text	Translated Text
Your Privacy	حریم خصوصی شما
This app was developed by [Company A] on behalf of [Government 1].	این برنامه را [شرکت الف] به نمایندگی از [دولت ۱] توسعه داده است.
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.	هنگامی که از برنامه ما استفاده می‌کنید، ما نام، نشانی، شماره تلفن و اطلاعات سلامت شما را جمع‌آوری می‌کنیم. این داده‌های سلامت به عنوان مثال دربردارنده نتایج آزمایش کووید-۱۹ شما هستند.
We use your data because it is necessary for the performance of a task carried out for public health purposes.	ما از داده‌های شما استفاده می‌کنیم چون داده‌ها برای انجام وظیفه‌ای ضروری است که برای اهداف سلامت عمومی لازم هستند.
We collect your data when you first register on the app and as you continue to use the app.	ما داده‌های شما را هنگامی که شما برای اولین بار از برنامه استفاده می‌کنید یا در حین استفاده از برنامه جمع‌آوری می‌کنیم.
We use your data to notify you if you have been in close contact with a person potentially infected with Covid-19.	ما از داده‌های شما استفاده می‌کنیم تا در صورتی که در تماس نزدیک با یک شخص مبتلا به کووید-۱۹ قرار داشتید، به شما اطلاع دهیم.
We store your data in [Country X] and we use servers that are certified for health data hosting.	ما داده‌های شما را در [کشور ب] نگهداری می‌کنیم و از سرورهایی استفاده می‌کنیم که برای میزبانی از داده‌های سلامت تأیید شده‌اند.
We use SDKs from the following third party providers: <ul style="list-style-type: none"> <li>• [Provider 1]</li> <li>• [Provider 2]</li> </ul>	ما از کیت‌های توسعه نرم‌افزاری (SDK) از ارائه‌دهندگان شخص ثالث زیر استفاده می‌کنیم: <ul style="list-style-type: none"> <li>• [ارائه‌دهنده ۱]</li> <li>• [ارائه‌دهنده ۲]</li> </ul>
This privacy notice was last updated on 1/1/22.	این اطلاع‌رسانی حریم خصوصی آخرین بار در تاریخ ۲۲/۰۱/۲۰۲۲ به‌روزرسانی شد.
See Full Privacy Notice	اطلاع‌رسانی کامل حریم خصوصی را ببینید
Have a Question?	سوالی دارید؟

## قالب ارزیابی اثرگذاری بر حریم خصوصی / محافظت از داده‌ها

در پایین قالبی برای ارزیابی اثرگذاری بر حریم خصوصی / محافظت از داده‌ها قرار دارد، که باید قبل از اعزام یک برنامه کامل شود.

[...]	سامانه/برنامه
[...]	نسخه سامانه/برنامه
[...]	تاریخ ارزیابی اثرگذاری بر حریم خصوصی / محافظت از داده‌ها (DPIA)

پیش‌زمینه پروژه توسعه	
[...]	چه سامانه/برنامه‌ای در حال توسعه است؟
[...]	چرا سامانه/برنامه توسعه داده می‌شود؟
[...]	چه کسی در توسعه سامانه/برنامه دخیل است؟
[...]	چه نوع آزمایشی بر روی سامانه/برنامه صورت گرفته است؟
[...]	تاریخ برنامه‌ریزی شده برای استقرار کامل چه زمانی است؟

توصیف عملکرد پردازش	
[...]	سامانه/برنامه از چه داده‌های شخصی استفاده می‌کند؟
[...]	داده‌های شخصی برای چه اهدافی استفاده می‌شوند؟
[...]	داده‌های شخصی برای چه کسانی افشا می‌شوند؟
[...]	چه کیت‌های توسعه نرم‌افزاری (SDK) یا کتابخانه‌های نرم‌افزاری شخص ثالث دیگری برای توسعه سامانه/برنامه استفاده می‌شوند؟

شناسایی خطرپذیری			
خطرپذیری	رویداد	آسیب‌پذیری	تهدید
[پایین، متوسط، بالا]	[...]	[...]	[...]

مدیریت خطرپذیری			
مبنای عقلانی	نوع پاسخ	پاسخ	خطرپذیری
[...]	[فنی، سازمانی یا قراردادی]	[پذیرش، انتقال، تقلیل یا اجتناب]	[...]