Vereinbarung zwischen

Robert Koch-Institut, Bundesinstitut im Geschäftsbereich des Bundesministeriums für Gesundheit der Bundesrepublik Deutschland

und

dem Eidgenössischen Departement des Innern der Schweizerischen Eidgenossenschaft

betreffend Corona-Apps (Austausch von Schlüsseln über einen auf schweizerischer Seite betriebenen Gateway Server zur grenzüberschreitenden Interoperabilität)

Das Robert Koch-Institut, Bundesinstitut im Geschäftsbereich des Bundesministeriums für Gesundheit der Bundesrepublik Deutschland, als Verantwortlicher im Sinne des Datenschutzrechts für die „Corona-Warn-App", nachfolgend „**RKI**" genannt und das Eidgenössische Departement des Innern der Schweizerischen Eidgenossenschaft, vertreten durch das Bundesamt für Gesundheit, als Verantwortlicher im Sinne des Datenschutzrechts für die „SwissCovid-App", nachfolgend „**BAG**" und zusammen „**Partner**" genannt, schließen die vorliegende Vereinbarung zum Austausch von Schlüsseln ihrer jeweiligen Corona-Apps über einen auf schweizerischer Seite betriebenen Gateway Server zur grenzüberschreitenden Interoperabilität ab.

§ 1 – Geltungsbereich und Zweck dieser Vereinbarung

1. Diese Vereinbarung beschränkt sich auf die unter § 3 beschriebene Verarbeitung von personenbezogenen Daten durch das Gateway mit dem Ziel, länderübergreifende Warnungen zwischen Corona-positiv getesteten Nutzern der Corona-Warn-App des RKI und Corona-positiv getesteten Nutzern der SwissCovid-App des BAG zu ermöglichen. Soweit die Partner in Bezug auf diese Verarbeitung datenschutzrechtlich gemeinsam Verantwortliche im Sinne von Artikel 26 Datenschutz-Grundverordnung (DSGVO) oder äquivalenten nationalen Bestimmungen sind, gelten die folgenden Vereinbarungen.

2. Die Verarbeitung durch das Gateway dient ausschließlich dem Zweck, das RKI als Betreiberin der Corona-Warn-App und das BAG als Betreiberin der SwissCovid-App technisch in die Lage zu versetzen, ihre Nutzer effizient zu warnen, wenn diese durch den Aufenthalt in der Nähe eines Nutzers der jeweils anderen nationalen Corona-App, der eine Warnung ausgelöst hat, potenziell SARS-CoV-2 ausgesetzt waren. Der genannte Zweck umfasst auch die nachgelagerte statistische Auswertung der Protokolldaten, um die Funktionsfähigkeit des Gateways sicherzustellen und dessen Auslastung und allgemeine Nutzung statistisch erfassen zu können.

3. Der Zweck dieser Vereinbarung ist es, die Zwecke und Mittel der gemeinsamen Verarbeitung festzulegen und die diesbezüglichen Rechte und Pflichten der Partner als gemeinsame Verantwortliche zu regeln. Für Verarbeitungstätigkeiten außerhalb des Geltungsbereichs dieser Vereinbarung, bei denen keine gemeinsame Festlegung der Zwecke und Mittel der Verarbeitung erfolgt, ist jeder Partner ein eigenständiger Verantwortlicher.

§ 2 – Definitionen

1. „Nutzer" ist eine Person, die eine Corona-App auf einem Mobiltelefon verwendet.

2. „Corona-Apps" sind die von den Partnern unter den Bezeichnungen „Corona-Warn-App" und „SwissCovid-App" jeweils herausgegebenen Softwareanwendungen für Mobiltelefone (Apps), die Annäherungen zwischen Nutzern aufzeichnen und diese benachrichtigen, wenn sie potenziell dem Coronavirus Sars-CoV-2 ausgesetzt waren.

3. „Back-End-Server" ist ein national betriebenes Serversystem, das der jeweiligen nationalen App (Corona-App oder entsprechende App) seinen Inhalt im Abrufverfahren zur Verfügung stellt. Dieser Inhalt besteht namentlich aus den Schlüsseln sowie Metadaten, welche von den „Corona-Apps" übermittelt oder aus dem Gateway heruntergeladen werden.

4. „Gateway" ist ein vom BAG betriebenes Serversystem, an das ein Back-End-Server über eine Schnittstelle angeschlossen werden kann, um die Schlüssel seiner nationalen App hochladen und die bereitgestellten Schlüssel entsprechender ausländischer Apps herunterzuladen.

5. „Schlüssel" sind eindeutige tagesgültige Kennungen, die vom Betriebssystem des Mobiltelefons erzeugt werden, sowie die darauf bezogenen Metadaten, für einen Nutzer, der über die von ihm verwendete Corona-App meldet, positiv auf eine Infektion mit SARS-CoV-2 getestet worden zu sein. Sie gelten als Gesundheitsdaten im Sinne der DSGVO.

6. „Metadaten" sind mit einem Schlüssel verknüpfte oder darin enthaltene Informationen, die Angaben zum Gültigkeitstag, zur Infektionsverifizierung, zum Ursprungsland des Schlüssels und weitere aus epidemiologischer Sicht relevante Angaben enthalten können und die von einer Corona-App für die Bewertung der Infektiosität eines Nutzers, der über die von ihm verwendete Corona-App meldet, positiv auf eine Infektion mit SARS-CoV-2 getestet worden zu sein, verwendet werden.

7. „Infektionsverifizierung" ist die zur Bestätigung einer Infektion mit SARS-CoV-2 verwendete Methode, d. h. die Bestätigung durch eine nationale Gesundheitsbehörde oder einen Labortest.

8. „Protokolldaten" sind eine automatische Aufzeichnung eines Zugriffs im Zusammenhang mit der Verarbeitung von Daten über das Gateway, aus der insbesondere die Art der Verarbeitung, das Datum und die Uhrzeit der Verarbeitung hervorgehen.

9. „Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") innerhalb des Anwendungsbereichs dieser Vereinbarung beziehen.

§ 3 – Grenzüberschreitender Datenaustausch zwischen der Corona-Warn-App und der SwissCovid-App durch das Gateway

1. Die gemeinsame Verarbeitungstätigkeit der Partner auf dem Gateway beschränkt sich auf folgende Prozessschritte:

   a) Authentifizierung der nationalen Back-End-Server.

   b) Empfang der Schlüssel über eine bereitgestellte Anwendungsprogrammierschnittstelle, die es den nationalen Back-End-Servern ermöglicht, diese Daten hochzuladen.

   c) Speicherung der von den nationalen Back-End-Servern hochgeladenen Schlüssel im Gateway.

   d) Bereitstellung der gespeicherten Schlüssel, deren Ursprungsland die Bundesrepublik Deutschland ist, auf dem Gateway zum Herunterladen durch den schweizerischen Back-End-Server.

   e) Bereitstellung der gespeicherten Schlüssel, deren Ursprungsland die Schweizerische Eidgenossenschaft ist, auf dem Gateway zum Herunterladen durch den deutschen Back-End-Server.

   f) Prüfen der Vertraulichkeit und Integrität der Schlüssel bei Empfang und Bereitstellung.

   g) Unwiederbringliche Löschung bzw. Vernichtung der gespeicherten Schlüssel, sobald der empfangende Back-End-Server sie heruntergeladen und geprüft hat, oder 14 Tage nach ihrem Empfang vom übermittelnden Back-End-Server, wobei der frühere der beiden Zeitpunkte maßgebend ist.

   h) Unwiederbringliche Löschung bzw. Vernichtung aller verbleibenden personenbezogenen Daten nach Einstellung des Betriebs des Gateways oder einseitiger, endgültiger Einstellung der Übermittlung der Schlüssel durch einen Partner an das Gateway.

2. Nationale Back-End-Server dürfen an das Gateway ausschließlich Schlüssel ihrer nationalen App, deren Gültigkeitstag im Zeitpunkt der Übertragung zum Gateway nicht länger als 14 Tage zurückliegt, übermitteln.

3. Die Übermittlung von Schlüsseln an das Gateway darf nur erfolgen, soweit der Nutzer in die grenzüberschreitende Verarbeitung seiner Daten zu den diesbezüglichen Zwecken dieser Vereinbarung ausdrücklich eingewilligt hat.

4. Die Verarbeitung erfolgt grundsätzlich orientiert an den allgemein öffentlich zugänglichen technischen Interoperabilitätsvorgaben im europäischen eHealth Netzwerk, soweit diese Vereinbarung keine anderen Vorgaben macht und soweit dies für die Partner im Rahmen des nationalen Rechts möglich ist. Diese ergeben sich insbesondere aus den Interoperabilitätsspezifikationen für den Abgleich grenzüberschreitender Übertragungsketten zwischen zugelassenen Apps vom 16. Juni 2020.[1]

5. Die Verarbeitung erfolgt unter der beidseitigen Annahme der Partner und nur unter der Bedingung, dass im Land des anderen Partners ein mit dem im eigenen Land äquivalentes Schutzniveau bei der Verarbeitung personenbezogener Daten gewährleistet ist und sofern ein gültiger Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO oder geeignete Garantien gemäß Art. 46 DSGVO vorgesehen sind und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

§ 4 – Zuständigkeiten und Pflichten des BAG

1. Die Zuständigkeit für die Einrichtung und den Betrieb des Gateways liegt beim BAG. In dieser Funktion gewährleistet das BAG die Sicherheit und den Schutz der Verarbeitung der ausgetauschten Daten im Gateway, einschließlich ihrer Übermittlung und Bereithaltung und nimmt die in Absatz 3 festgelegten Aufgaben wahr. Das BAG trägt sämtliche hieraus entstehenden Kosten selbst. Die Kosten für die Anpassung an den eigenen Corona-Apps werden hingegen durch jeden Partner selbst getragen.

2. Die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung im Gateway wird vom BAG unter Beteiligung des Nationalen Zentrums für Cybersicherheit NCSC und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) regelmäßig mindestens jedes halbe Jahr und anlassbezogen geprüft, beurteilt und bewertet. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) wird vom BAG über die Beurteilung und Bewertung informiert.

3. Das BAG

   a) schafft und gewährleistet eine sichere Kommunikationsinfrastruktur, die den Back-End-Servern der Partner den Austausch der in § 3 Absatz 2 genannten Daten nach Maßgabe dieser Vereinbarung ermöglicht.

---

[1] abrufbar unter: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

b) darf mit Zustimmung des RKI Dritte als Auftragsverarbeiter im Sinne Art. 4 Nr. 8 der DSGVO beiziehen. Die vertragliche Vereinbarung mit dem Auftragsverarbeiter muss den Anforderungen aus Artikel 28 DSGVO entsprechen. Das BAG stellt sicher, dass im Fall der Beauftragung eines Auftragsverarbeiters in Bezug auf die Verarbeitung von personenbezogenen Daten von Nutzern der Corona-Warn-App dieselben Datenschutzverpflichtungen, wie sie in dieser Vereinbarung festgelegt sind, auch für diese Auftragsverarbeiter gelten und eingehalten werden. Eine Unterbeauftragung sollte grundsätzlich nur einmal möglich sein, auch dafür hat das RKI seine Zustimmung zu erteilen. Das RKI hat das Recht, die Zustimmung zur Beauftragung oder Unterbeauftragung bei Vorliegen eines wichtigen Grundes zu verweigern. Ein wichtiger Grund ist insbesondere dann anzunehmen, wenn durch die Unterbeauftragung die Rechtsposition des RKI nach dieser Vereinbarung verschlechtert wird, wenn das RKI begründeten Anlass zu Bedenken hinsichtlich der Einhaltung der vertraglichen und/oder gesetzlichen Pflichten des Datenschutzes und/oder der Informationssicherheit durch den jeweiligen Unterauftragsverarbeiter hat oder wenn gewichtige Anhaltspunkte für ein nicht rechtskonformes Verhalten des Unterauftragsverarbeiters vorliegen, das geeignet ist, das Vertrauen in seine generelle Zuverlässigkeit zu erschüttern.

c) stellt im Falle der Anbindung weiterer Länder an das Gateway sicher, dass die von dem Back-End-Server der Corona-Warn-App an das Gateway übermittelten Schlüssel weiterhin nur mit dem Back-End-Server der SwissCovid-App zu den Zwecken dieser Vereinbarung ausgetauscht und insbesondere nicht an die Systeme der anderen Länder übermittelt werden.

d) trifft alle organisatorischen, physischen und logischen Sicherheitsmaßnahmen auf Grundlage der Vorgaben der Bundesverwaltung der Schweizerischen Eidgenossenschaft für IKT (IKT-Grundschutz in der Bundesverwaltung)[2], um den Betrieb des Gateways aufrechtzuerhalten. Zu diesem Zweck wird das BAG:

aa) eine für das Sicherheitsmanagement beim Gateway zuständige Stelle benennen, dem RKI deren Kontaktdaten mitteilen und deren Verfügbarkeit zur Reaktion auf Sicherheitsbedrohungen gewährleisten;

bb) die Verantwortung für die Sicherheit des Gateways übernehmen;

cc) sicherstellen, dass alle Personen, denen der Zugriff auf das Gateway gewährt wird, vertraglichen, beruflichen oder gesetzlichen Vertraulichkeitsverpflichtungen unterliegen, die auch in Bezug auf die Einstufung der Schlüssel als Gesundheitsdaten gemäß Datenschutz-Grundverordnung oder äquivalenten nationalen Bestimmungen und dieser Vereinbarung ausreichend sind.

---

[2] Insbesondere Si001 - IKT-Grundschutz in der Bundesverwaltung, Si003 – Netzwerksicherheit in der Bundesverwaltung, abrufbar unter: www.bk.admin.ch > Digitale Transformation und IKT Lenkung > Vorgaben > Sicherheit.

e) trifft alle erforderlichen Sicherheitsmaßnahmen, damit das reibungslose Funktionieren der Back-End-Server der Partner nicht beeinträchtigt wird. Zu diesem Zweck richtet das BAG besondere Verfahren für den Anschluss der Back-End-Server an das Gateway ein. Dazu gehören:

aa) ein Verfahren zur Risikobewertung, um potenzielle Bedrohungen des Systems zu ermitteln und abzuschätzen,

bb) ein Audit- und Überprüfungsverfahren

i. zur Überprüfung der Übereinstimmung der umgesetzten Sicherheitsmaßnahmen mit den für die Verarbeitung – die in Bezug auf die Schlüssel Gesundheitsdaten umfasst – maßgeblichen Sicherheitsvorgaben gemäß IKT-Grundschutz in der Bundesverwaltung und der schweizerischen Datenschutzgesetzgebung,

ii. zur regelmäßigen Kontrolle der Integrität der Systemdateien, der Sicherheitsparameter und der erteilten Genehmigungen;

iii. zur Überwachung zwecks Feststellung von Sicherheitsverstößen und von unbefugtem Eindringen;

iv. zur Umsetzung von Änderungen zur Behebung bestehender Sicherheitslücken und

v. zur Ermöglichung — auch auf Anfrage des RKI— und zur Mitwirkung an der Durchführung unabhängiger Audits, einschließlich Inspektionen, sowie von Überprüfungen von Sicherheitsmaßnahmen (bspw. BSI-Grundschutz) und Prüfungen der für das RKI zuständigen Datenschutzaufsichtsbehörde zur Erfüllung ihrer jeweiligen gesetzlich zugewiesenen Aufgaben,

cc) ein Änderungskontrollverfahren, um die Auswirkungen einer Änderung vor ihrer Umsetzung zu dokumentieren und abzuschätzen und die Verantwortlichen über alle Änderungen auf dem Laufenden zu halten, die sich auf die Kommunikation mit ihren Infrastrukturen und/oder deren Sicherheit auswirken können;

dd) die Festlegung eines Wartungs- und Reparaturverfahrens mit Regeln und Bedingungen für die Wartung und/oder Reparatur von Ausrüstungen;

ee) die Festlegung eines Verfahrens in Bezug auf Sicherheitsvorfälle (Melde- und Eskalationsprogramm), welches sicherstellt, dass der behördliche Datenschutzbeauftrage des RKI unverzüglich über jegliche Verletzung des Schutzes personenbezogener Daten unter Angabe der Art, Umfang und Umstände sowie den wahrscheinlichen Folgen der Verletzung und den ergriffenen und geplanten Maßnahmen zur Behebung der Verletzung und Abmilderung der möglichen nachteiligen Auswirkungen unterrichtet wird.

ff) Festlegung eines Disziplinarverfahrens, sofern nicht bereits vorhanden, um gegen Sicherheitsverletzungen vorzugehen

gg) ein unabhängig durchgeführter Penetrationstest inklusive einer Quelltextanalyse

f) ergreift physische und/oder logische Sicherheitsmaßnahmen auf Grundlage des aktuellen Stands der Technik für die Einrichtungen, in denen die Ausrüstung für das Gateway untergebracht ist, und für die Kontrollen der logischen Daten und der Zugriffssicherheit. Als Grundlage wird der IKT-Grundschutz (siehe §4 Abs. 3 Bst. e bb) i.) vereinbart, weitere technisch-organisatorische Sicherheitsmaßnahmen sollen in dem Sicherheitskonzept dokumentiert werden.

g) ergreift Maßnahmen zum Schutz seiner Netzdomäne, einschließlich der Trennung von Anschlüssen;

h) führt einen Risikomanagementplan in Bezug auf das Gateway;

i) überwacht — in Echtzeit — die Leistung aller Dienstkomponenten des Gateways, erstellt regelmäßige Statistiken und führt Aufzeichnungen über die Aktivitäten des Gateways;

j) leistet Unterstützung für alle Dienste des Gateways über Telefon, E-Mail und nimmt Anrufe von autorisierten Anrufern entgegen;

k) ergreift alle erforderlichen Maßnahmen, damit der technische Betreiber des Gateways keinen unbefugten Zugriff auf übermittelte Daten hat;

l) ergreift Maßnahmen, um die Kommunikation zwischen den Partnern zu erleichtern;

m) führt gemäß Artikel 30 Absatz 1 der Datenschutz-Grundverordnung oder gemäß äquivalenten nationalen Bestimmungen und dieser Vereinbarung ein Verzeichnis aller durchgeführten Verarbeitungsvorgänge.

n) ergreift Maßnahmen, die in regelmäßigen Abständen sicherstellen, dass physische und logische Sicherheitsmaßnahmen weiterhin dem Stand der Technik entsprechen.

o) ermöglicht dem RKI oder vom RKI beteiligte Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Absprache mit dem Bundesamt für Informatik und Telekommunikation (BIT) eigene sicherheitstechnische Untersuchungen des Gateways vorzunehmen und diese bei physischen oder logischen Änderungen des Gateways teilweise oder vollständig zu wiederholen.

4. Das BAG teilt dem RKI unverzüglich alle wichtigen Vorkommnisse und Änderungen in Bezug auf das Gateway mit, die Auswirkungen auf die Verarbeitung der ausgetauschten Daten im Gateway haben, insbesondere:

a) potenzielle oder tatsächliche Risiken für die Verfügbarkeit, Vertraulichkeit und/oder Integrität der im Gateway verarbeiten Daten;

b) Sicherheitsvorfälle;

c) jede Verletzung des Schutzes personenbezogener Daten, die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen sowie alle Maßnahmen, die ergriffen wurden, um gegen die Verletzung des Schutzes personenbezogener Daten vorzugehen und das Risiko für die Rechte und Freiheiten natürlicher Personen zu mindern;

d) jeden Verstoß gegen die gemäß dieser Vereinbarung getroffenen technischen und/oder organisatorischen Vorkehrungen für die Verarbeitungsvorgänge im Gateway.

e) jede physische oder logische Änderung des Gateways, welche direkten oder indirekten Einfluss auf die Verfügbarkeit, Vertraulichkeit und/oder Integrität der Daten, die im Gateway verarbeitet werden, hat.

5. Das BAG informiert darüber hinaus in Fällen von Sicherheitsvorfällen unverzüglich direkt auch den behördlichen Datenschutzbeauftragen des RKI, um das weitere Vorgehen abzustimmen. Sofern den Partnern infolge eines Sicherheitsvorfalls Melde- und Benachrichtigungspflichten gemäß Art. 33, 34 DSGVO treffen, stellt das BAG dem RKI und gesondert dem behördlichen Datenschutzbeauftragten des RKI unverzüglich alle zur Prüfung des eventuellen Vorliegens einer Melde- oder Benachrichtigungspflicht notwendigen Informationen zur Verfügung.

6. Sofern den Partnern Benachrichtigungspflichten gemäß Art. 34 DSGVO obliegen, ist für die Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen auf schweizerischer Seite, einschließlich der Nutzer der SwissCovid-App, das BAG zuständig.

7. Für die Bearbeitung einschließlich Beantwortung von Anfragen/Anträgen eines Nutzers der SwissCovid-App im Zusammenhang mit der Ausübung der Rechte betroffener Personen im Einklang mit der Datenschutz-Grundverordnung oder gemäß äquivalenten nationalen Bestimmungen und dieser Vereinbarung ist das BAG zuständig.

8. Das BAG informiert die Nutzer der SwissCovid-App im Einklang mit den Artikeln 13 und 14 sowie 26 Absatz 2 Satz 2 der Datenschutz-Grundverordnung im Rahmen der Datenschutzerklärung der SwissCovid-App über die Verarbeitung ihrer personenbezogenen Daten auf Grundlage dieser Vereinbarung zu Zwecken der länderübergreifenden Warnung.

§ 5 – Zuständigkeiten und Pflichten des RKI

1. Das RKI unterstützt das BAG im Rahmen seiner Möglichkeiten bei der Ermittlung und Behandlung von Sicherheitsvorfällen, einschließlich Verletzungen des Schutzes personenbezogener Daten, im Zusammenhang mit der Verarbeitung im Gateway.

2. Insbesondere teilt das RKI dem BAG im Rahmen seiner Kenntnisse und Möglichkeiten Folgendes mit:

   a) potenzielle oder tatsächliche Risiken für die Verfügbarkeit, Vertraulichkeit und/oder Integrität der personenbezogenen Daten, die im Gateway verarbeitet werden;

   b) Sicherheitsvorfälle, die mit der Verarbeitung im Gateway in Verbindung stehen;

   c) jede Verletzung des Schutzes personenbezogener Daten, die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und die Bewertung der Risiken für die Rechte und Freiheiten natürlicher Personen sowie alle Maßnahmen, die ergriffen wurden, um gegen die Verletzung des Schutzes personenbezogener Daten vorzugehen und das Risiko für die Rechte und Freiheiten natürlicher Personen zu mindern;

   d) jeden Verstoß gegen die technischen und/oder organisatorischen Vorkehrungen für die Verarbeitungsvorgänge im Gateway.

3. Für die Bearbeitung einschließlich Beantwortung von Anfragen/Anträgen eines Nutzers der Corona-Warn-App im Zusammenhang mit der Ausübung der Rechte betroffener Personen im Einklang mit der Datenschutz-Grundverordnung oder gemäß äquivalenten nationalen Bestimmungen und dieser Vereinbarung ist das RKI zuständig.

4. Das RKI informiert die Nutzer der Corona-Warn-App im Einklang mit den Artikeln 13 und 14 sowie 26 Absatz 2 Satz 2 der Datenschutz-Grundverordnung im Rahmen der Datenschutzerklärung der Corona-Warn-App über die Verarbeitung ihrer personenbezogenen Daten auf Grundlage dieser Vereinbarung.

5. Melde- oder Benachrichtigungspflichten gemäß Artikel 33 und 34 DSGVO, die den Partnern obliegen, werden federführend durch das RKI bearbeitet. Für die Durchführung von Meldungen und Benachrichtigungen sowie die Kommunikation mit der zuständigen Aufsichtsbehörde i.S.v. Art. 33 und 34 DSGVO ist das RKI zuständig.

6. Sofern den Partnern Benachrichtigungspflichten gemäß Artikel 34 DSGVO obliegen, ist für die Benachrichtigung der von der Verletzung des Schutzes personenbezogener Daten betroffenen Personen auf deutscher Seite, einschließlich der Nutzer der Corona-Warn-App, das RKI zuständig.

§ 6 – Zuständigkeiten und Pflichten beider Partner

1. Jeder Partner richtet eine Anlaufstelle mit einem Funktionspostfach ein, das der Kommunikation zwischen den Partnern im Zusammenhang mit dieser Vereinbarung dient. Kenntnisnahme der eingehenden Nachrichten sowie Reaktionen sollten grundsätzlich in einem sehr kurzen Zeitraum erfolgen. In dringenden Fällen hat auch eine telefonische Kontaktaufnahme des jeweils anderen Partners zu Zwecken der Information und Abstimmung zu erfolgen. Jeder Partner benennt zu diesem Zweck jeweils einen direkten Ansprechpartner (E-Mail, Telefon).

2. Jeder Partner nimmt die von einem Nutzer bei ihm eingehenden Anfragen/Anträge im Zusammenhang mit der Ausübung der Rechte betroffener Personen im Einklang mit der Datenschutz-Grundverordnung oder gemäß äquivalenten nationalen Bestimmungen und dieser Vereinbarung entgegen. Jeder Partner bestimmt eine spezielle Anlaufstelle für Anfragen/Anträge von Nutzern. Erhält ein Partner eine Anfrage/einen Antrag eines Nutzers im Zusammenhang mit der Ausübung der Rechte betroffener Personen, die/der nach Maßgabe dieser Vereinbarung oder des für den jeweiligen Partner anwendbaren Rechtsvorschriften nicht seiner Zuständigkeit oder Verantwortlichkeit unterliegt, so leitet er sie/ihn umgehend an den zuständigen Partner weiter. Auf Anfrage unterstützen sich die Partner gegenseitig bei der Bearbeitung von Anfragen/Anträgen betroffener Personen im Zusammenhang mit der Ausübung der Rechte betroffener Personen und antworten einander unverzüglich, spätestens jedoch innerhalb von 15 Tagen nach Eingang eines Amtshilfeersuchens.

3. Jeder Partner stellt diese Vereinbarung auf seiner Website zur Verfügung.

4. Benötigt ein Partner zur Erfüllung seiner Pflichten nach den Artikeln 35 und 36 DSGVO oder gemäß äquivalenten nationalen Bestimmungen und dieser Vereinbarung Informationen von dem anderen Partner, so übermittelt er eine besondere Anfrage an das Funktionspostfach des anderen Partners. Letzterer bemüht sich nach besten Kräften, diese Informationen zur Verfügung zu stellen.

5. Jeder Partner ist verpflichtet, auf die Richtigkeit der an das Gateway zu übermittelnden personenbezogenen Daten zu achten. Erweist sich, dass ein Partner unrichtige personenbezogene Daten oder personenbezogene Daten, die nicht hätten übermittelt werden dürfen, an das Gateway übermittelt hat, so teilt er dies dem anderen Partner unverzüglich mit.

6. Personenbezogene Daten von Nutzern einer Corona-App, die von den Partnern an das Gateway übermittelt werden, dürfen nur in anonymisierter oder pseudonymisierter Form übermittelt werden. Jeder der Partner bestätigt hiermit, dass es ihm nach heutigen Kenntnisstand nicht möglich ist,

   a) Rückschlüsse auf die Identität von konkreten Nutzern anhand der Schlüssel auf dem eigenen Back-End-Server zu ziehen; und

   b) Rückschlüsse auf die Identität von konkreten Nutzern anhand der Schlüssel, die er über das Gateway vom anderen Partner erhalten hat, und allfällig weiteren Datensätzen zu ziehen.

7. Kann ein Partner die Anfragen/Anträge einer betroffenen Person im Zusammenhang mit der Ausübung ihrer Rechte aufgrund der bewusst ausgeschalteten Rückführbarkeit mangels Identifikationsmöglichkeit nicht bearbeiten, so unterrichtet er die betroffene Person hierüber, sofern dies anhand der vorliegenden Kontaktdaten (z. B. E-Mail-Adresse, Postanschrift) möglich ist. In diesem Fall finden die Rechte betroffener Personen keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer gesetzlichen Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

8. Jeder Partner stellt sicher, dass der jeweils andere Partner oder sein Rechtsträger nach Maßgabe des innerstaatlichen Rechts demjenigen gegenüber haftet, der aufgrund von Datenübermittlungen nach dieser Vereinbarung rechtswidrig geschädigt wird. Es gelten die Vorgaben der Art. 82 Abs. 4 und Abs. 5 DSGVO oder äquivalenten nationalen Bestimmungen, wonach die Haftung gemeinsam Verantwortlicher gegenüber Dritten gesamtschuldnerisch erfolgt, im Innenverhältnis wird die Haftung aber nach Anteil der Verantwortung für das schädigende Ereignis aufgeteilt.

§ 7 – Streitbeilegung

1. Streitigkeiten zwischen den Partnern über die Auslegung oder Anwendung dieser Vereinbarung sollen, soweit möglich, durch die Partner einvernehmlich beigelegt werden.

2. Kann eine Streitigkeit auf diese Weise nicht beigelegt werden, so wird sie auf Verlangen eines Partners einem Schiedsgericht unterbreitet.

3. Das Schiedsgericht wird von Fall zu Fall gebildet, indem jeder Partner ein Mitglied bestellt und beide Mitglieder sich auf ein drittes Mitglied als Obmann oder Obfrau einigen, der oder die von beiden Partnern bestellt wird. Die Mitglieder werden innerhalb von zwei Wochen bestellt, nachdem der eine Partner dem anderen mitgeteilt hat, dass der die Streitigkeit einem Schiedsgericht unterbreiten will.

4. Das Schiedsgericht entscheidet mit Stimmenmehrheit. Seine Entscheidungen sind bindend und endgültig. Jeder Partner trägt die Kosten seines Mitglieds sowie seiner Vertretung in dem Verfahren vor dem Schiedsgericht; die Kosten des Obmanns oder der Obfrau sowie die sonstigen Kosten werden von den Partnern zu gleichen Teilen getragen. Das Schiedsgericht kann eine andere Kostenregelung treffen. Im Übrigen regelt das Schiedsgericht sein Verfahren selbst.

§ 8 – Schlussbestimmungen

1. Die Vereinbarung tritt in Kraft, sobald sich die Partner mitgeteilt haben, dass die innerstaatlichen Voraussetzungen dafür erfüllt sind. Der Betrieb des Gateways wird aufgenommen, sobald alle nötigen Einrichtungen gemacht sind.

2. Die Vereinbarung kann jederzeit durch Übereinkunft zwischen den Partnern geändert, aufgehoben oder verlängert werden.

3. Die Vereinbarung gilt für die Dauer des Austauschs der Schlüssel beider Partner über das Gateway und solange das Gateway besteht, längstens aber bis zum 30. Juni 2022.

4. Die für den Schutz von personenbezogenen Daten einschlägigen Bestimmungen dieser Vereinbarung gelten auch bei Aufhebung, Kündigung oder Auslaufen dieser Vereinbarung in Bezug auf die bereits übermittelten Daten fort.

5. Jeder Partner kann die Übermittlung von Schlüsseln von Nutzern der von ihm herausgegebenen Corona-App an das Gateway jederzeit einstellen. Eine solche Absicht ist dem anderen Partner, soweit zumutbar, so früh wie möglich im Voraus mitzuteilen, so dass dieser rechtzeitig die erforderlichen Maßnahmen, etwa die Anpassung von Datenschutzinformationen für die Nutzer der von ihm herausgegebenen Corona-App, ergreifen kann.

6. Diese Vereinbarung kann von jedem Partner einseitig schriftlich gekündigt werden. Die Kündigung wird nach Ablauf eines Monats nach ihrem Eingang beim anderen Partner wirksam.

Für das Eidgenössische Departement des Innern:

Bern, den 17.3.21

[redacted]

Direktorin des Bundesamtes für Gesundheit, Anne Lévy

Für das Robert Koch-Institut:

Berlin, den 19.3.2021

[redacted]

Präsident, Prof. Dr. Lothar H. Wieler