Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 29. April 2021

(Stand: 29. April 2021)

Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19

1. Einleitung

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Stellungnahme vom 26.03.2021 *„Kontaktnachverfolgung in Zeiten der Corona-Pandemie – Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“* bereits darauf hingewiesen, dass digitale Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten (im Folgenden Kontaktnachverfolgungssysteme) datenschutzkonform betrieben werden müssen. Die vorliegende Orientierungshilfe erläutert die Anforderungen an derartige Systeme und ihren Betrieb, die sich aus den gesetzlichen Vorgaben ergeben. Sie richtet sich vorrangig an Entwickler und Verantwortliche i. S. v. Art. 4 Nr. 7 DS-GVO (siehe Abschnitt 3).
In Ergänzung zu der gesetzlich vorgeschriebenen Nachverfolgung von Kontakten infizierter Personen durch die Gesundheitsämter werden Systeme entwickelt und betrieben, die einen anderen Ansatz verfolgen. Sie zielen auf die Information von Personen über Infektionsrisiken, denen sie durch die Nähe zu einer infizierten Person ausgesetzt waren und den eigenverantwortlichen Umgang mit dieser Information. Dieser Ansatz ermöglicht datensparsame Lösungen, die mit pseudonymen Daten auskommen und deren Sicherheit nicht auf der Vertrauenswürdigkeit zentraler Systeme beruht. Eine ausschließliche Umsetzung dieses Ansatzes erfüllt jedoch die derzeitigen gesetzlichen Anforderungen nicht. Sollte der Gesetzgeber dagegen digitale Lösungen zulassen, die die Übermittlung der Anwesenheitsdokumentation durch Veranstalter an die Gesundheitsämter nicht verlangen, dann wären aus datenschutzrechtlicher Sicht Lösungen dieses Ansatzes vorzugswürdig.

2. Rechtliche Ausgangslage

Die von den Verantwortlichen (siehe Abschnitt 3) zu erfüllenden datenschutzrechtlichen Anforderungen für die rechtskonforme Verarbeitung personenbezogener Daten zur digitalen Kontaktnachverfolgung ergeben sich aus der Datenschutz-Grundverordnung (DS-GVO), insbesondere aus den Grundsätzen des Art. 5 DS-GVO. So ist für jede

Verarbeitung eine Rechtsgrundlage erforderlich, es ist die Transparenz des Verfahrens sicherzustellen, die Verarbeitung dem Zweck angemessen und auf das notwendige Maß zu beschränken (Datenminimierung), die Richtigkeit der Daten zu gewährleisten, eine Speicherbegrenzung für diesen erforderlichen Zweck sicherzustellen sowie die Integrität und Vertraulichkeit der Daten im gesamten Verfahren zu gewährleisten.
Unbeschadet allgemeiner bundesrechtlicher Grundlagen der Kontaktdatenerhebung nach § 28a Abs. 1 Nr. 17, Abs. 4 Infektionsschutzgesetz (IfSG) variieren bislang die Regelungen zur Kontaktnachverfolgung in den einzelnen Bundesländern hinsichtlich der zu erhebenden Kontaktdaten, hinsichtlich der Frage, wer in welchem Umfang wie Kontaktdaten erheben muss, um im Infektionsfall eine Kontaktnachverfolgung durch die Gesundheitsämter zu ermöglichen, und hinsichtlich der anlasslosen Kontrolle der Kontaktdaten durch die Gesundheitsämter.

3. Verantwortlichkeitssphären

Verantwortlichkeiten im Sinne des Art. 4 Nr. 7 DS-GVO müssen eindeutig geregelt sein. Verantwortliche können je nach Konstellation des Verfahrens der jeweilige Dienstanbieter, ein Veranstalter oder ein Gesundheitsamt sein. Bei gemeinsamen Verantwortlichkeiten gemäß Art. 26 DS-GVO ist vorab eindeutig zu regeln, welche Akteure für welche Verarbeitungsphase jeweils Verantwortliche sind. So ist dann z. B. konkret zu regeln, wer nach Art. 13 DS-GVO für die Informationspflicht, das Auskunftsrecht nach Art. 15 DS-GVO, das Recht auf Berichtigung und Löschung (Art. 16 und 17 DS-GVO), für die Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO und für die Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO verantwortlich ist. Dies muss dann in der Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 DS-GVO konkret schriftlich fixiert werden. Die genannten Pflichten müssen ebenfalls im jeweiligen Auftragsverarbeitungsvertrag i. S. d. Art. 28 Abs. 3 DS-GVO geregelt werden.

4. Rechtmäßigkeit der Verarbeitung

Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie in jeder Verarbeitungsphase durch den jeweiligen Verantwortlichen auf eine Rechtsgrundlage gestützt werden kann. Daher sind die einzelnen Akteure gesondert zu betrachten:

4.1. Dienstanbieter

Für die Durchführung folgender Verarbeitungsschritte ist grundsätzlich der Dienstanbieter datenschutzrechtlich Verantwortlicher i. S. d. Art. 4 Nr. 7 DS-GVO. Er kann mindestens folgende Verarbeitungen der personenbezogenen Daten des Nutzers – eine diesbezügliche vertragliche Vereinbarung vorausgesetzt – auf Art. 6 Abs. 1 Satz 1 lit. b DS-GVO stützen:

- die Registrierung für die Nutzung des Dienstes mit identifizierenden Angaben über die betroffene Person und den Veranstalter,
- die Speicherung von personenbezogenen Daten in den Endgeräten der betroffenen Personen und
- je nach Ausgestaltung die Übermittlung von Kontaktdaten an die Veranstalter im Zuge des Besuchs einer Veranstaltung, sowie
- die Speicherung von Daten über die Begegnung mit anderen Personen auf privaten Zusammenkünften.

Übermittelt der Dienstanbieter auf Wunsch einer infizierten Person die betroffene Besucherhistorie, handelt es sich um eine Datenübermittlung von Gesundheitsdaten i. S. v. Art. 9 Abs. 1 DS-GVO. Der Dienstanbieter kann diese Übermittlung auf Art. 6 Abs. 1 lit. a i. V. m. Art. 9 Abs. 2 lit. a DS-GVO stützen.
Soweit die Verarbeitung des Dienstanbieters zusätzlich zur Kontaktnachverfolgung auch andere Gesundheitsdaten, z.B. über Covid19- Symptome oder Testergebnisse umfasst, kann die insoweit erforderliche Verarbeitungsbefugnis nur aus einer ausdrücklichen Einwilligung der betroffenen Person nach Art. 6 Abs. 1 Lit. a, 9 Abs. 2 lit. a DS-GVO abgeleitet werden.

4.2. Veranstalter

Veranstalter sind gemäß § 28a Abs. 1 Nr. 17 IfSG i. V. m. den Corona-Schutzverordnungen oder -gesetzen der Länder dazu verpflichtet, die Kontaktdaten zu dokumentieren und für die gesetzlich vorgeschriebene Zeit aufzubewahren. Dieser Pflicht kann je nach Regelung in der jeweiligen Corona-Schutzverordnung oder -gesetz des Landes auch durch eine digitale Dokumentation entsprochen werden. Soweit Veranstalter gesetzlich zur Erhebung von Kontaktdaten und auf Aufforderung zu deren Übermittlung zum Zweck der Kontaktnachverfolgung an die Gesundheitsämter verpflichtet sind, werden sie vom Gesetzgeber als datenschutzrechtliche Verantwortliche angesehen (§ 28a Abs. 4 S. 1 IfSG i. V. m. der landesrechtlichen Regelung). Insofern besteht nach Art. 6 Abs. 1 Satz 1 lit. c und ggf. Art. 9 Abs. 2 lit. i DS-GVO auch eine Befugnis, diese personenbezogenen und unter Umständen gesundheitsbezogenen und damit besonders zu schützenden Daten zu verarbeiten.

Erfassen Privatpersonen Daten von anderen natürlichen Personen, die an von ihnen veranstalteten Zusammenkünften wie Familienfeiern teilnehmen, so fällt diese Erfassung unter die Haushaltsausnahme des Art. 2 Abs. 2 lit. c DS-GVO und somit nicht unter die Regelungen der DS-GVO. Soweit die Übermittlung der personenbezogenen Daten der Gäste der privaten Zusammenkunft durch die Privatperson an das zuständige Gesundheitsamt im Infektionsfall nicht mehr unter die Haushaltsausnahme fällt, ist sie jedenfalls nach Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. i DS-GVO zulässig, soweit die Privatperson damit ihren gesetzlichen Verpflichtungen gemäß § 25 Abs. 2 i. V. m. 16 Abs. 2 IfSG nachkommt.

4.3. Gesundheitsamt

Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch ein Gesundheitsamt zur Kontaktnachverfolgung findet sich im Infektionsschutzgesetz (IfSG) i. V. m. den Corona-Schutzverordnungen oder -gesetzen der Länder.
Sobald sich aus den verarbeiteten Daten selbst oder aus den Umständen der Verarbeitung ergibt, dass Daten einer infizierten Person verarbeitet werden – dies ist insbesondere dann der Fall, wenn die infizierte Person Angaben über den Aufenthalt bei Veranstaltungen und Einrichtungen, sowie ggf. über die Begegnungen mit anderen Personen im privaten Bereich an das Gesundheitsamt übergibt – ist von einer Verarbeitung von Gesundheitsdaten i. S. v. Art. 4 Nr. 15 DS-GVO auszugehen. Für das Gesundheitsamt ergibt sich die Erlaubnis zur Verarbeitung dieser Daten aus Art. 6 Abs. 1 lit. e, Abs. 3 lit. b, 9 Abs. 2 lit. i DS-GVO i. V. m. § 28a Abs. 4 Satz 4 IfSG.

5. Zwecksetzung und Zweckbindung

§ 28a Abs. 4 Satz 3 IfSG begründet eine gesetzliche, gegenüber allgemeinen Zweckänderungstatbeständen vorrangige Zweckbindung für die zur Kontaktdatenverarbeitung gesetzlich bestimmten Datenarten.
Die gesetzlich zur Erhebung verpflichteten *Veranstalter* dürfen die Kontaktdaten nicht zu einem anderen Zweck als der Aushändigung an die Gesundheitsämter verarbeiten, § 28a Abs. 4 Satz 3 IfSG. Eine Weitergabe der übermittelten Daten durch die *Gesundheitsämter* oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ebenfalls ausgeschlossen, § 28a Abs. 4 Satz 6 IfSG. Soweit der *Dienstanbieter* im Auftrag von Veranstaltern oder Gesundheitsämtern tätig ist, ist ihm eine Weiterverarbeitung der Kontaktdaten zu anderen Zwecken außerhalb einer Weisung der Auftraggeber nicht gestattet. Soweit der Dienstanbieter im Vorfeld der Datenerhebung durch die Veranstalter oder im Rahmen einer gemeinsamen Verantwortung eigenverantwortlich tätig ist, ist auch ihm in Anwendung der Regelungen des

§ 28a Abs. 4 IfSG unbeschadet der Frage einer insoweit tragfähigen Verarbeitungsbefugnis eine Verarbeitung zu anderen Zwecken ebenso wie den anderen Akteuren verwehrt.
Aufgrund der strengen gesetzlichen Festlegungen ist auch eine Anonymisierung der Kontaktdaten in Hinblick auf eine spätere Auswertung zu anderen Zwecken als der Kontaktnachverfolgung nicht gestattet.

6. Sicherstellung der Freiwilligkeit und Wahrung der Datenschutzgrundsätze

6.1. Freiwilligkeit

Die Nutzung von digitalen Kontaktnachverfolgungsdiensten durch betroffene Personen sollte freiwillig sein, um das Risiko der Diskriminierung bei der Teilnahme am gesellschaftlichen Leben zu vermeiden und eine hohe Kooperationsbereitschaft zu fördern.[1]
Eine freiwillige Entscheidung für eine Anwendung setzt ein hohes Maß an Transparenz voraus, damit die Besucherinnen und Besucher, die diese nutzen, eine informierte Entscheidung treffen können.
Freiwilligkeit setzt eine Wahlmöglichkeit voraus. Die DSK begrüßt die Vielzahl der Anbieter, die Verpflichtete und betroffenen Personen die Möglichkeit bietet, zwischen verschiedenen Diensten wählen zu können. Darüber hinaus sollte für betroffene Personen stets die Möglichkeit bestehen, bei Veranstaltungen, bei denen Kontaktdaten nach dem Infektionsschutzrecht verarbeitet werden müssen, Kontaktangaben ohne ein geeignetes eigenes Endgerät, ohne Eingehung eines Vertrages mit einem Anbieter und ohne Erteilung einer Einwilligung zu hinterlassen.
Bei einer Befragung durch das Gesundheitsamt kann die betroffene Person die Auskunft auf solche Fragen verweigern, deren Beantwortung ihr selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde (vgl. § 25 Abs. 2 i. V. m. 16 Abs. 2 S. 4 IfSG). Daher muss der Betreiber des Systems sicherstellen, dass diejenigen Daten, die eine betroffene Person im Rahmen ihrer eigenen Besuchs- und Kontakthistorie gespeichert

[1] „Die systematische und umfassende Überwachung des Standortes und/oder der Kontakte zwischen natürlichen Personen ist ein schwerwiegender Eingriff in deren Privatsphäre. Dieser ist nur dann legitim, wenn der Nutzer die App für jeden der vorgesehenen Zwecke freiwillig verwendet. Im Umkehrschluss bedeutet dies, dass Personen, die solche Apps nicht nutzen möchten oder können, keine Nachteile entstehen dürfen.“ Europäischer Datenschutzausschuss: Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19, https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_de

hat, erst nach einer Freigabe durch den Betroffenen an das Gesundheitsamt übermittelt werden und die nutzende Person zuvor die Möglichkeit hat, aus diesen Angaben eine Auswahl zu treffen.

6.2. Transparenz der Datenverarbeitung

Dienstanbieter und Veranstalter sowie die Gesundheitsbehörden müssen, soweit sie jeweils für die Verarbeitung Verantwortlicher sind, die betroffenen Personen gemäß der gesetzlichen Anforderungen der Art. 13 und 14 DS-GVO informieren. Soweit der Veranstalter Verantwortlicher und der Anbieter Auftragsverarbeiter ist, muss letzterer dem Veranstalter alle notwendigen Informationen zur Verfügung stellen, damit letzterer seiner Informationspflicht nach Art. 13 DS-GVO gegenüber den Besuchern nachkommen kann (Art. 28 Abs. 3 S. 2 lit. e DS-GVO).
Die betroffene Person muss dadurch darüber unterrichtet werden, wer für die jeweilige Verarbeitung datenschutzrechtlich verantwortlich ist, auf welcher Rechtsgrundlage die Verarbeitung erfolgt und welche Rechte ihr zustehen. Für die betroffene Person muss auf diese Weise klar erkennbar sein, an welchen Verantwortlichen sie sich zur Geltendmachung ihrer Rechte wenden kann und wer als Auftragsverarbeiter für die Sicherheit der personenbezogenen Daten einsteht. Gemäß Art. 13 Abs. 1 lit. a und c DS-GVO müssen die Nutzer digitaler Kontaktnachverfolgungsdienste insbesondere darüber informiert werden, welcher Akteur für welche Verarbeitung – angegeben nach ihrem Verarbeitungszweck – zuständig ist. Diese Information muss in präziser, transparenter, verständlicher und leicht zugänglicher Form erfolgen sowie eine klare und einfache Sprache verwenden.
Am besten für den Betroffenen wäre daher eine zentrale Kontaktstelle, die das Anliegen des Betroffenen an den jeweiligen Verantwortlichen weiterleitet.
Schließlich bieten digitale Lösungen eine einfache Möglichkeit, die Erfüllung der Informationspflichten nach Art. 14 DS-GVO für die Gesundheitsämter zu erleichtern. Wenn im Infektionsfall tatsächlich Kontaktdaten übermittelt werden müssen, können betroffene Personen im Gegensatz zu einer allgemeinen Vorabinformation (Art. 14 Abs. 5 lit. a DS-GVO) hiervon unmittelbar über die App konkret informiert werden. Diese Chance, Transparenz sicherzustellen, sollte bei der Konzeption entsprechender Dienste nicht ungenutzt bleiben.

6.3. Vertraulichkeit, Minimierung der Zugänglichkeit der Daten und Zweckbindung

Zur Gewährleistung der strengen Zweckbindung muss mit technischen und organisatorischen Maßnahmen ausgeschlossen werden, dass die von den Diensten bzw. mit ihrer Hilfe verarbeiteten personenbezogenen Daten für andere als die festgelegten Zwecke weiterverarbeitet werden können.

Um diese Zweckbindung wie auch die Vertraulichkeit der Kontaktdaten zu gewährleisten, muss festgelegt und durchgesetzt werden, dass nur das jeweils zuständige Gesundheitsamt Zugriff auf die jeweiligen personenbezogenen Daten erhält. Dies darf im Falle der im Falle der Befragung der infizierten Person nach § 25 Abs. 2 i. V. m. 16 Abs. 2 IfSG nur unter Beteiligung dieser Person (s.o.) und im Falle der Aushändigung der Kontaktdaten i. S. v. § 28a Abs. 4 Satz 3 IfSG nur unter Beteiligung des Veranstalters ermöglicht werden. Sofern eine zeitliche oder ortsbezogene Einschränkung der zu übermittelnden Kontaktdaten geboten ist (z. B. Kontaktdaten aller Personen eines Raumes, in dem sich eine infizierte Person aufhielt), soll der Dienst eine Beschränkung auf diese Daten vorsehen. Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit c i. V. m. Art. 25 Abs. 1 DS-GVO) ist bei der Technikgestaltung in der Planungsphase bereits ebenso zu beachten (data protection by design) wie im Betrieb.
Die Verantwortlichen haben nach Maßgabe des § 28a Abs. 4 S. 2 IfSG sicherzustellen, dass eine Kenntnisnahme und Weiterverarbeitung der erfassten Kontaktdaten durch unbefugte Personen oder Institutionen ausgeschlossen ist. In Verbindung mit Art. 32 DS-GVO ergibt sich, dass die Veranstalter zumindest die identifizierenden Angaben schon bei der Erhebung veranstaltungsbezogen (d.h. nach Veranstaltern und Zeiten getrennt) so verschlüsseln müssen, dass sie ohne Hinzuziehung zusätzlicher Informationen, die nur der jeweiligen betroffenen Person und den zuständigen Gesundheitsämtern bekannt sind, nicht entschlüsselt und verschiedene Aufenthalte ein und derselben Person nicht über die identifizierenden Angaben miteinander in Verbindung gebracht werden können.
Die Zuordnung der Kontaktdaten zu einer identifizierten oder identifizierbaren natürlichen Person darf nur einem zuständigen Gesundheitsamt im Zuge der Nachverfolgung der Kontakte einer infizierten Person ermöglicht werden. Das heißt insbesondere, dass weder den Veranstaltern, noch dem Dienstanbieter eine Entschlüsselung möglich sein darf. Das Vorhalten eines Generalschlüssels für die Entschlüsselung aller Datensätze widerspricht dieser Anforderung.

7. Rechte der betroffenen Personen auf Berichtigung, Löschung und Auskunft

Verantwortliche sind gehalten, sicherzustellen, dass die Bearbeitung von Betroffenenanträgen den gesetzlichen Anforderungen entsprechend erfolgen kann. Voraussetzung für die Gewährung von Betroffenenrechten ist als erster Schritt bei der Bearbeitung von Betroffenenanträgen die Identifizierung der Betroffenen. Die Notwendigkeit der Identifizierung berechtigt nicht zur Verarbeitung zusätzlicher Daten. Stellt eine betroffene Person die im Einzelfall erforderlichen Daten zur Identifizierung zur Verfügung, müssen Betroffenenanträge weiterbearbeitet werden (EG 57 S. 2 der DS-GVO). Tun Betroffene dies nicht, können nach Maßgabe des Art. 11 Abs. 1, Art. 12 Abs. 2 S. 2 DS-GVO Betroffenenanträge nicht weiterbearbeitet werden.

Sofern die personenbezogenen Daten durch die verantwortlichen Stellen pseudonymisiert vorgehalten werden, müssen Betroffenenanträge bearbeitet werden, wenn diese im Rahmen des Identifizierungsprozesses von sich aus den Verantwortlichen die Pseudonyme zur Verfügung stellen, unter denen die Daten im System gespeichert werden. Es ist dabei sicherzustellen, dass die Pseudonyme derart generiert und geschützt werden, dass diese nicht zu einer unbefugten Beauskunftung, Berichtigung oder Löschung mittels erratenen oder unbefugt erlangten Pseudonymkennungen verwendet werden können.
Dies gilt auch, wenn mehrere Akteure zur Rechtegewährung zusammenwirken müssen.

7.1. Recht auf Berichtigung gemäß Art. 16 DS-GVO

Es müssen Vorkehrungen getroffen werden, dass betroffene Personen unverzüglich die Berichtigung unrichtiger Angaben über ihre Person oder über einen Aufenthalt in einer Veranstaltung verlangen können.

7.2. Recht auf Löschung gemäß Art. 17 DS-GVO

Der Verantwortliche muss sicherstellen, dass einerseits die Kontaktdaten systemseitig automatisiert nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungspflicht gelöscht werden und andererseits, dass sämtliche personenbezogenen Daten des Nutzers, die nicht von Verantwortlichen zur Erfüllung einer gesetzlichen Verpflichtung im Rahmen der Kontaktnachverfolgung benötigt werden, gelöscht werden, wenn dieser den Dienst nicht mehr nutzen möchte. Von der Löschung werden die Daten nicht erfasst, für die noch eine gesetzliche Aufbewahrungspflicht besteht.

7.3. Recht auf Auskunft gemäß Art. 15 DS-GVO

Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob und welche sie betreffende personenbezogene Daten verarbeitet werden und eine Kopie dieser Daten zu erhalten (Art. 15 DS-GVO).

8. Technische und organisatorische Maßnahmen

Grundlegende Voraussetzung für den Betrieb von Kontaktdatenerfassungsdiensten bilden sichere Datenverarbeitungssysteme. Diese müssen dabei nach Art. 32 Abs. 1 DS-GVO den Stand der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Es muss ein

dem Risiko angemessenes Schutzniveau gewährleistet sein, d.h. die Auswahl der Sicherheitsmaßnahmen ist an den konkreten Verarbeitungstätigkeiten und den damit einhergehenden Gefahren für die Rechte und Freiheiten der Betroffenen auszurichten.
Der Datenschutz muss bereits in der Konzeptionsphase hinreichende Berücksichtigung finden und insbesondere die Grundsätze der Verarbeitung personenbezogener Daten nach Art. 5 DS-GVO gewährleisten (vgl. Abschnitt 2, Abs. 1 dieser Orientierungshilfe). Insoweit ist der Verantwortliche nach Art. 25 DS-GVO dazu verpflichtet, zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen umzusetzen.
Im Rahmen dieser Orientierungshilfe können keine vollumfänglichen technischen Prüfkriterien definiert werden, jedoch soll im Folgenden dargelegt werden, welche Anforderungen an Kontaktnachverfolgungssysteme die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Bezug auf technische und organisatorische Maßnahmen sowie deren Umsetzung für die Einhaltung der Datenschutzgrundsätze und die Wahrung der Betroffenenrechte für angemessen hält. Die Kriterien werden anschließend durch Best-Practice-Hinweise ergänzt.
Eine mögliche Methodik zur Umsetzung dieser Anforderungen enthält das Standard-Datenschutzmodell (SDM).[2]

8.1. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Verantwortliche haben gem. Art. 25 Abs. 1 und 2 DS-GVO sicherzustellen, dass sie Verfahren bereits datenschutzkonform planen und gestalten (Datenschutz durch Technikgestaltung) und zudem mit datenschutzfreundlichen Voreinstellungen betreiben. Hierbei gilt der Grundsatz, dass durch Voreinstellungen (bspw. einer App zur Kontaktdatenerfassung) nur Daten, die für den bestimmten Verarbeitungszweck erforderlich sind, verarbeitet werden (Grundsatz der Zweckbindung, Art. 5 Abs. 1 lit b DS-GVO). Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Dieses Verhalten muss ohne Eingreifen des Nutzenden sichergestellt sein.
Bei der Entwicklung von Kontaktdatenerfassungsdiensten muss gewährleistet sein, dass bereits in der Planungsphase eines Entwicklungsprozesses Belange des Datenschutzes mitbedacht und bei der Ausgestaltung der Prozesse berücksichtigt werden. Werden in Kontaktnachverfolgungssysteme weitere, nicht auf die Kontaktnachverfolgung ausgerichtete Funktionen integriert, so dürfen diese die datenschutzrechtlich wesentlichen Eigenschaften des Systems nicht beeinträchtigen und insbesondere diese Integration nicht zu höheren Risiken führen. Art. 25 Abs. 2 DS-GVO (Datenschutzfreundliche Voreinstellungen) verlangt, dass solche Funktionalitäten nur dann

[2] https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

aktiviert sein dürfen, wenn sie von der betroffenen Person ausdrücklich aktiviert wurden.

8.2. Risiken einer zentralen Datenspeicherung

Bei der Entwicklung von Kontaktnachverfolgungsdiensten kann grundsätzlich zwischen zwei verschiedenen Ansätzen unterschieden werden: Zum einen die Gruppe von Diensten, die die Kontaktdaten der betroffenen Personen in einer zentralen Server-Infrastruktur hinterlegen, und zum anderen Dienste, die die Daten soweit möglich zunächst dezentral halten, also auf den Endgeräten der betroffenen Personen und der Veranstalter speichern.
Beide Ansätze erlauben grundsätzlich die gleiche Funktionalität, sowohl im Hinblick auf die Erfüllung der infektionsschutzrechtlichen Anforderungen gemäß § 28a Abs. 4 IfSG, als auch auf die Einhaltung der datenschutzrechtlichen Vorgaben, die in Abschnitt 5 bis 7 dieser Orientierungshilfe erläutert wurden. Beide Ansätze benötigen zudem zentrale Dienste und Systeme, die diese Funktionalitäten bereitstellen.
Bei der Entscheidung für die Umsetzung des einen oder den anderen Ansatzes sind die Risiken zu betrachten, die mit ihr einhergehen. Eine Kompromittierung der zentralen Dienste und Systeme durch unbefugte Dritte, die mit einer Verletzung der Vertraulichkeit und Integrität dieser Dienste und Systeme einhergeht, kann zu besonders hohen Risiken führen, wenn diese Systeme nicht nur zur Steuerung der Verarbeitung, sondern auch zur umfangreichen Speicherung schützenswerter Daten über den Aufenthalt von Personen in Einrichtungen und ihre Teilnahme an Veranstaltungen verwendet werden.
Diesen Risiken kann grundsätzlich mit einer Verschlüsselung begegnet werden. In diesem Fall ist zu betrachten, wo die Schlüssel gespeichert werden, wer die Kontrolle über diese Schlüssel besitzt und wie diese durch unbefugte Handlungen erlangt oder genutzt werden können. Eine dezentrale Speicherung der Schlüssel stellt eine sinnvolle risikomindernde Maßnahme dar. Sie wird jedoch ihrerseits geschwächt, wenn die zum Schlüsselmanagement verwendeten Werkzeuge von den zentral betriebenen Systemen bereitgestellt werden und damit von Unbefugten, die Kontrolle über diese Systeme erlangt haben, manipuliert werden können.
Die Dienstanbieter sind verpflichtet vor Aufnahme des Betriebs des Dienstes, die Risiken des von ihnen gewählten Modells eingehend zu analysieren und die Wirksamkeit der vorgesehenen Maßnahmen nachzuweisen.

8.3. Sicherheit der Verarbeitung

Bei Kontaktnachverfolgungssystemen, die Kontaktdaten in großem Umfang verarbeiten, ist das Risiko für die Rechte und Freiheiten natürlicher Personen durch geeignete

technische und organisatorische Maßnahmen wirksam einzudämmen. Eine Datenschutz-Folgenabschätzung kann dazu dienen, die Wirksamkeit der technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten nachzuweisen. Sie ist entweder nach Art. 35 DS-GVO von einem Verantwortlichen durchzuführen, sofern die von ihm verarbeitenden personenbezogenen Daten voraussichtlich zu einem hohen Risiko der Rechte und Freiheiten führen, oder kann freiwillig von einem Dienstanbieter für viele, insbesondere kleine Verantwortliche durchgeführt werden. Besteht eine Pflicht zur Erstellung einer Datenschutzfolgenabschätzung, so ist diese vor Beginn der Verarbeitung abzuschließen. Eine Datenschutzfolgenabschätzung sollte jedoch möglichst früh im Planungs- und Entwicklungsprozess durchgeführt werden, damit die Erkenntnisse daraus in die Entwicklung zurückfließen können.
Bei der Auswahl der technischen und organisatorischen Maßnahmen ist insbesondere das Folgende zu beachten:

- Datenübermittlungen an Drittländer oder internationale Organisationen ohne Angemessenheitsbeschluss der EU-Kommission sind mit zusätzlichen Risiken verbunden und können sich als unzulässig erweisen, wenn die Vorgaben des Kapitels V der DS-GVO nicht eingehalten werden. Empfohlen ist insbesondere die Inanspruchnahme von Rechenzentren im räumlichen Geltungsbereich der DS-GVO.
- Maßnahmen zur Umsetzung des Grundsatzes der Datenminimierung sind zu veranlassen.
- Anwendungen und Systeme müssen über den gesamten Nutzungszeitraum bei Schwachstellen und anderen Fehlern zeitnah aktualisiert werden, bei kritischen Schwachstellen unverzüglich.
- Grundsätze der IT-Sicherheit sind einzuhalten. So müssen Vertraulichkeit, Integrität und Verfügbarkeit der Daten zu jeder Zeit gewährleistet sein. Dies umfasst sämtliche Datenverarbeitungen und gilt somit sowohl für gespeicherte Daten als auch für aktiv verarbeitete Daten. Maßnahmen zur Sicherstellung dieser Grundsätze sind unter anderem:
    - Nachträgliche Änderungen von Kontaktdaten sollten soweit überhaupt zulässig, nachvollziehbar gestaltet werden und sollten versioniert sein.
    - Zentrale Vertrauensanker (z. B. einer PKI) liegen bei einer vertrauenswürdigen externen Stelle.
    - Die Schlüsselerstellung der Nutzerzertifikate sollte lokal auf den Endgeräten erfolgen, wenn dies hinreichend sicher möglich ist.
    - Identifikatoren, Pseudonyme und Schlüssel sollten in kurzen Zeitabständen gewechselt werden, um eine Profilbildung über längere Zeiträume zu erschweren.
    - Die Authentizität der Gegenstelle sollte von allen an der jeweiligen Kommunikation Beteiligten überprüfbar sein.

- Die Übermittlung der individuellen Kontaktdatenerfassungs-Einträge als auch der Weiterverarbeitung über weitere Akteure muss über verschlüsselte Verbindungen durchgeführt werden, sodass Dritte keine Kenntnis der Kontaktdaten nehmen können.
- Der Abruf der Gesundheitsämter muss auf Basis gesundheitsamts-individueller Zertifikate erfolgen.
- Zugriffe der Gesundheitsämter müssen protokolliert werden. Protokolldaten sind ihrerseits vor unberechtigten Zugriffen zu schützen.
- Übermittlungen von Kontaktdaten sind zusätzlich zur Inhaltsverschlüsselung per Transportverschlüsselung unter Einhaltung der BSI TR 02102-2 oder anderen nach dem Stand der Technik gleich wirksamen Maßnahmen abzusichern, um auch Metadaten auf dem Transportweg zu schützen.
- Das Verfahren soll angemessenen Schutz gegen den Identitätsmissbrauch zulasten der betroffenen Personen und gegen den Eintrag von Anwesenheitsdaten, die keinem tatsächlichen Aufenthalt entsprechen, aufweisen.
- Daten, die für die Zweckerfüllung nicht mehr erforderlich sind, müssen sicher gelöscht werden. Dies gilt auch für nicht mehr erforderliche Versionen und Kopien von Daten.
- Bei dem Zugriff für Wartung und Administration von Systemen und Diensten, die für den Betrieb des Kontaktnachverfolgungssystems kritisch sind, oder für die Autorisierung des Abrufs von Kontaktdaten ist eine sichere Authentifizierung (bspw. Zwei-Faktor-Authentifizierung) nach dem Stand der Technik erforderlich.
- Maßnahmen zur Umsetzung des Grundsatzes der Datenminimierung sind zu veranlassen.
- Soweit innerhalb des Kontaktnachverfolgungssystems identifizierende Angaben vor ihrer Übernahme überprüft werden, muss diese Prüfung gegen Manipulation geschützt sein.
- Eine Verarbeitung von Metadaten (einschließlich Verkehrsdaten) muss auf das erforderliche Maß beschränkt werden und es darf keine Verknüpfung mit Kontaktdaten erfolgen.

- Apps zur Kontaktdatenerfassung dürfen grundsätzlich keine Übermittlungen personenbezogener Daten an Dritte vornehmen und insbesondere keine Tracking- und Analysedienste einbinden.
- Bei der Nutzung von externen Dienstleistern muss sichergestellt werden, dass durch diese keine Nutzungsdaten – außerhalb der zur erforderlichen Bereitstellung der vertraglich vereinbarten Dienstleistung – für weitere Zwecke (Telemetrie-Daten, Daten zur Verbesserung des Dienstes, Diagnose-Daten, etc.) ohne ausreichende Rechtsgrundlage verarbeitet werden.

8.4. Best-Practice-Hinweise

Die Beachtung nachfolgender datenschutzrechtlicher Best-Practice-Hinweise dient dem Schutz der Rechte und Freiheiten der betroffenen Personen, ohne andere Interessen zu beeinträchtigen.

- Der Dienstanbieter sollte den betroffenen Personen soweit möglich einfach benutzbare Funktionen zur Verfügung stellen, mit denen sie die ihnen zustehenden Rechte geltend machen oder umsetzen können. Insbesondere müssen Verantwortliche Berichtigungen (vgl. Punkt 7.1) nicht selbst vornehmen, sondern können über den Dienst den betroffenen Personen die technische Möglichkeit bereitstellen, eigenständig unrichtige Daten nach der Erhebung zu berichtigen, soweit dies ohne Verletzung der Vertraulichkeit der gespeicherten Daten geschehen kann und die Integrität der Aufenthaltsdokumentation (z. B. durch Versionierung der Einträge) unberührt bleibt.
- Der Dienstanbieter sollte betroffenen Personen, Veranstaltern und Gesundheitsämtern Anwendungen zur Verfügung stellen, deren Integrität durch Signaturprüfung verifiziert werden kann.
- Um die Akzeptanz der Anwendungen zu erhöhen, sollten der interessierten Öffentlichkeit Informationen über die technischen Maßnahmen, die der Verantwortliche zur Gewährleistung einer datenschutzkonformen Verarbeitung ergriffen hat, zur Verfügung stehen, soweit die Veröffentlichung selbst zu keinen Sicherheitsrisiken führt. Hierzu gehört auch die Veröffentlichung des Quellcodes der jeweiligen Anwendungen, die betroffene Personen, Veranstalter, Anbieter und Gesundheitsämter einsetzen. Um eine Überprüfung zu ermöglichen, sollte eine Reproduzierbarkeit der veröffentlichten Binärdateien möglich sein.
- Mobile Apps sollten auch auf Vertriebsplattformen angeboten werden, die nicht unter Kontrolle der großen Anbieter von mobilen Betriebssystemen stehen, da die Nutzung der Plattformen dieser Anbieter mit zusätzlichen zu rechtfertigenden Datenverarbeitungen verbunden ist.