AOK VERLAG

Datenschutz im Blick

Newsletter für den Datenschutz im Gesundheitswesen

Ausgabe Sep./Okt. 2020 | Seite 1

www.aok-verlag.info/ds-im-blick

INHALT

10 Tipps zu aktuellen Datenschutzthemen

Nicht nur die DSGVO hat in der Praxis die Umstellung von Prozessen und Arbeitsabläufen notwendig gemacht. Seit ihrer Einführung vergeht kaum ein Monat, ohne dass Aufsichtsbehörden Anforderungen konkretisieren oder Gerichtsurteile vermeintlich rechtskonforme Prozesse für unzulässig erklären. Dieser Beitrag soll einen kurzen Überblick zu einigen Punkten geben, die man aktuell im Blick haben sollte.

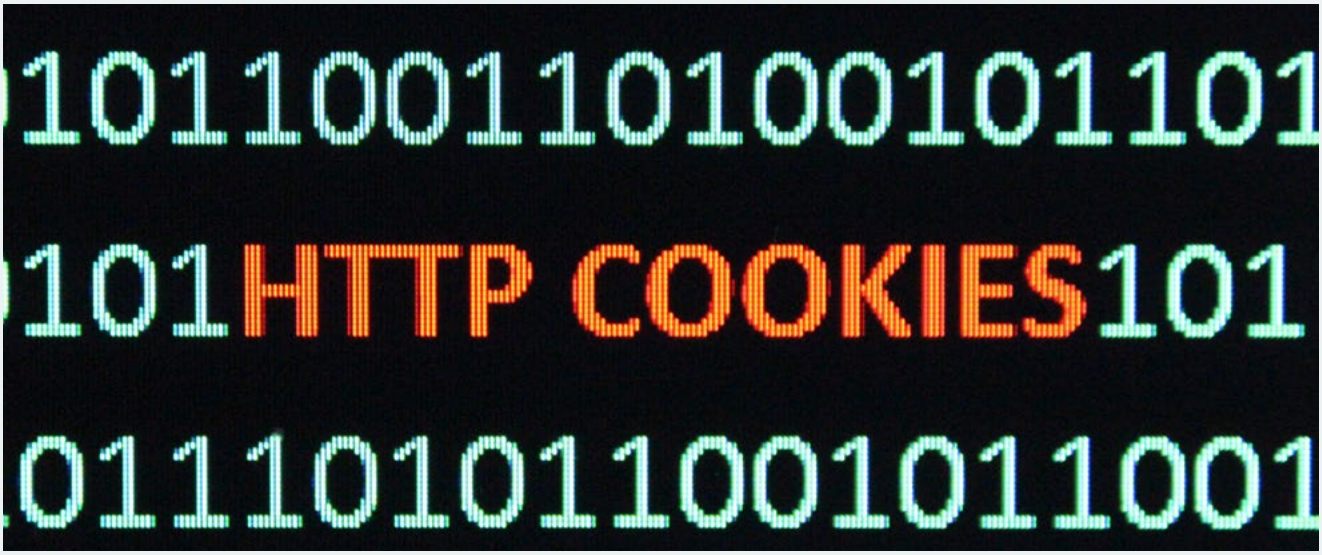
Sven Venzke-Caprarese

1. Datenverarbeitung außerhalb der EU prüfen

Kaum ein Datenschutzbeauftragter dürfte es verpasst haben: Der EuGH hat mit Urteil vom 16. Juli 2020 das Privacy Shield für unwirksam erklärt. Über das Privacy Shield konnte der Datentransfer in die USA rechtskonform gestaltet werden.

Besonders brisant dabei ist, dass der EuGH in einem Nebensatz auch die Standarddatenschutzklauseln erwähnt und hierzu ausführt: *„Da diese Standarddatenschutzklauseln ihrer Natur nach keine Garantien bieten können, die über die vertragliche Verpflichtung, für die Einhaltung des unionsrechtlich verlangten Schutzniveaus zu sorgen, hinausgehen, kann es je nach der in einem bestimmten Drittland gegebenen Lage erforderlich sein, dass der Verantwortliche zusätzliche Maßnahmen ergreift, um die Einhaltung dieses Schutzniveaus zu gewährleisten."*

Verantwortliche sollten daher in einem ersten Schritt prüfen, ob die Verarbeitung von Daten in den USA auf Grundlage des Privacy Shields erfolgt(e). Ist dies der Fall sollten als erste Sofort-



maßnahme Standarddatenschutzklauseln mit den beteiligten Stellen geschlossen werden.

In einem zweiten Schritt müssen dann alle Verarbeitungen klassifiziert werden, die in Drittländern unter Nutzung von Standarddatenschutzklauseln stattfinden. Jede dieser Verarbeitungen muss dann im Einzelfall überprüft werden. Welche Maßstäbe hierbei anzulegen sind, ist allerdings noch nicht ganz klar. Zum einen muss die Rechtslage in den betroffenen Drittländern mit Blick auf die dort geltenden Sicherheitsgesetze bewertet werden. Gibt es hier Gesetze, die einen staatlichen Zugriff auf die Daten erlauben, ohne dass Betroffene informiert werden oder Rechtsmittel gegen den Zugriff einlegen können bzw. sind die Hürden des Zugriffs so gering, dass eine gerichtliche Prüfung gar nicht erforderlich ist?

Darüber hinaus kann die Art der Dienstleistung und der Schutzbedarf der Daten eine Rolle spielen. Bestenfalls wird ein Zugriff durch Sicherheitsbehörden durch zusätzliche Maßnahmen des Dienstleisters, wie z.B. eine durchgängige Verschlüsselung der Daten ohne Möglichkeit des Dienstleisters diese zu entschlüsseln, verhindert.

Insgesamt ist dieses Thema in der Praxis derzeit schwierig zu handhaben. Insbesondere bei neuen Projekten sollte daher gleich zu Beginn beachtet werden, dass die Verarbeitung in unsicheren Drittländern rechtlich immer schwieriger wird.

2. Tracking im Internet auf den Prüfstand stellen

Ein Dauerbrenner seit Einführung der DSGVO ist die Frage, unter welchen Bedingungen Websitebetreiber die Aufrufe ihrer Seite messen dürfen bzw. sogar weitergehende Trackingtools einsetzen können, um Remarketing im Internet zu betreiben.

Hier haben sich die Anforderungen nicht nur durch die Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien aus März 2019 ständig verschärft.

Darüber hinaus gibt es auch ein Urteil des EuGHs vom 1. Oktober 2019 zum Thema Analyse und Tracking im Internet. Demnach ist für das Setzen von Werbecookies die ausdrückliche Einwilligung des Nutzers erforderlich, die im entsprechenden Einwilligungsbanner weder vorangekreuzt sein darf noch konkludent „durch Weitersurfen“ erteilt werden kann.

Im Anschluss an das Urteil des EuGHs hat dann der BGH mit Urteil vom 25. Mai 2020 noch einmal für Verwirrung gesorgt. Denn entgegen der Orientierungshilfe der Aufsichtsbehörden geht der BGH davon aus, dass die Messung von Besuchern zu Analyse- und Trackingzwecken nicht unter Art. 6 DSGVO (Einwilligung bzw. Interessenabwägung) fällt. Stattdessen sei § 15 TMG nach wie vor anwendbar, jedoch im Lichte der EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation wie ein Einwilligungserfordernis zu lesen. In der Praxis bedeutet dies insbesondere für Websitebetreiber, die sich bislang zur Besuchermessung auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO stützten, Anpassungsbedarf. Denn es spricht viel dafür, dass nach der Entscheidung des BGH sogar für ein cookieloses und nicht sessionübergreifendes Tracking (z.B. mit zurückhaltenden Fingerprints) eine Einwilligung über ein Einwilligungsbanner erforderlich ist.

Selbst Websitebetreiber, die lediglich die Nutzung bzw. den Aufruf der eigenen Seite messen wollen, kommen damit kaum noch um ein Einwilligungsbanner herum. Die einzige Möglichkeit, eine solche Messung ohne Einwilligungsbanner vorzunehmen, besteht derzeit in der Auswertung der anonymisierten Protokolldaten des Webservers.

3. Eingebundene Drittinhalte in Webseiten prüfen

Ein weiterer Punkt, der im Internet beachtet werden sollte, hat wiederum mit dem Wegfall des Privacy Shields zu tun. Denn dieses konnte oftmals herangezogen werden, wenn Websitebetreiber auf ihren Seiten die Dienste Dritter eingebunden hatten – z.B. Google Maps oder YouTube-Videos. Mit dem Wegfall des Privacy Shields ist es sinnvoll, eine etwaige Übermittlung personenbezogener Daten (IP-Adresse) ebenfalls auf Basis einer Einwilligung vorzunehmen und in diesem Rahmen auch die Übermittlung in ein unsicheres Drittland zu thematisieren.

Die entsprechende Einwilligung kann über ein Einwilligungsbanner eingeholt werden.

Als Alternative zum Einwilligungsbanner besteht die Möglichkeit, die entsprechenden Inhalte nicht sofort einzubinden, sondern zuerst eine Platzhaltergrafik anzuzeigen, die darauf hinweist, dass eine Aktivierung der Inhalte zur Einbindung von Drittinhalten führt, Drittanbieter in diesem Rahmen die IP-Adresse erhalten und eigene Trackingmechanismen ausrollen könnten sowie das Daten ggf. in ein unsicheres Drittland ohne angemessenes Datenschutzniveau übermittelt werden. Den Klick des Nutzers auf die Platzhaltergrafik müsste man dann als Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO beschreiben und die Übermittlung von personenbezogenen Daten in ein unsicheres Drittland könnte in diesem Rahmen auf die Grundlage von Art. 49 Abs. 1 lit. a DSGVO gestellt werden.

4. Löschfristen definieren und Umsetzung prüfen

Es wird immer deutlicher, dass die Aufsichtsbehörden Zähne zeigen und in diesem Rahmen auch Bereiche angehen, die vor der DSGVO in der Praxis oftmals eher stiefmütterlich behandelt wurden.

So wird z.B. das Thema „Löschfristen“ immer wichtiger. Verantwortliche sollten konkrete Löschfristen für einzelne Datenkategorien definieren und auch die (oftmals technischen) Prozesse zur Umsetzung der Löschfristen prüfen. Insgesamt zeigt sich, dass viele Löschprozesse ohne eine im Detail steuerbare elektronische Lösung kaum umsetzbar sind. Besonders deutlich zeigt sich dies am Beispiel der Personalakte. Vor dem Hintergrund der DSGVO wäre es oftmals zu kurz gegriffen, die Löschfrist pauschal auf „10 Jahre nach Ausscheiden des Mitarbeiters“ zu setzen. Tatsächlich greifen hier innerhalb einer Akte teilweise sehr verschiedene Aufbewahrungsfristen, z.B.:

- Abmahnungen für leichte Verstöße dürfen grundsätzlich nicht länger als 2-3 Jahre aufbewahrt werden
- lohnsteuerrelevante Daten können grundsätzlich 6 Jahre aufbewahrt werden
- Unterlagen zur Altersvorsorge können ggf. für 30 Jahre bzw. bis zum Tod des Beschäftigten relevant sein.

Will man diesen Anforderungen bei einer Vielzahl von Beschäftigten nachkommen, wird dies in der Praxis fast nur noch mit einer gut durchdachten Lösung zur elektronischen Aktenführung gewährleistet werden können. Hierauf sollte der Verantwortliche vom Datenschutzbeauftragten ggf. hingewiesen werden.

5. Berechtigungskonzept

Neben den Löschfristen legen Aufsichtsbehörden insbesondere im Bereich des Gesundheitswesens ein deutliches Augenmerk auf die Gewährleistung eines angemessenen Berechtigungskonzepts in Bezug auf den Zugriff auf Patientendaten. Einrichtungen des Gesundheitswesens sollten sich der hohen Anforderungen der Aufsichtsbehörden an dieser Stelle bewusst sein und ggf. auch noch einmal die eigenen Konzepte anhand der Orientierungshilfe der Aufsichtsbehörden für Krankenhausinformationssysteme (OH-KIS) aus dem Jahr 2014 überprüfen.

6. Datenschutz mit dem Betriebsrat besprechen

Das Thema Datenschutz macht auch vor der Arbeit des Betriebsrates nicht halt. Rechtlich ist es umstritten, ob der Betriebsrat datenschutzrechtlich insofern eine eigenverantwortliche Stelle neben der eigentlichen Gesundheitseinrichtung ist oder dieser datenschutzrechtlich zum Verantwortlichen gehört. Egal welche Ansicht man hier vertritt: In jedem Fall muss besprochen werden, wie die Prozesse rund um den Datenschutz der Betriebsratsarbeit gestaltet werden und wer hier welche Aufgaben übernimmt.

Ggf. kann es sogar sinnvoll sein, dass der Betriebsrat ein eigenes Verzeichnis der Verarbeitungstätigkeiten erstellt bzw. den Verantwortlichen für seinen Teilbereich hier unterstützt.

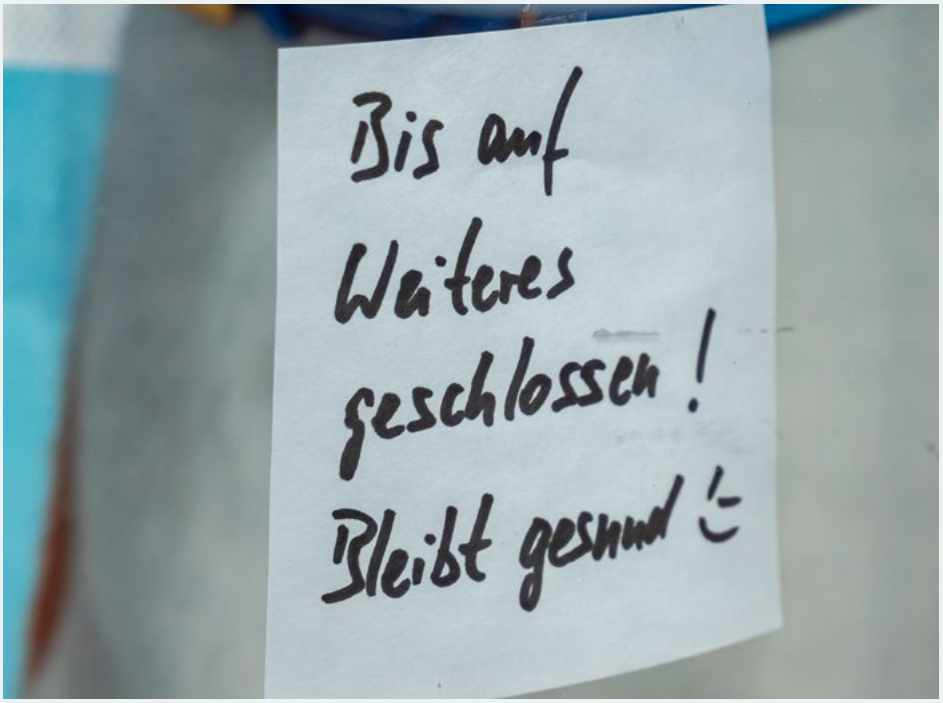
7. Webapplikationen

Es erscheint zwar manchmal als lästig bzw. zu zeit- und kostenintensiv – trotzdem ist es sinnvoll und ggf. sogar erforderlich: Sofern Gesundheitseinrichtungen Webapplikationen betreiben, bei denen personenbezogene Daten nach einem Login über das Internet abgerufen werden können, ist die Durchführung eines regelmäßigen Penetrationstests nicht zuletzt auf Grund von Art. 32 DSGVO ratsam.

Als Datenschutzbeauftragter sollte man das Thema gegenüber dem Verantwortlichen zumindest angesprochen haben. Trifft der Verantwortliche die Entscheidung, einen regelmäßigen Penetrationstest (z.B. aus Kostengründen) nicht durchzuführen, so ist man seiner Pflicht nachgekommen, den Verantwortlichen entsprechend zu beraten. Und bestenfalls wird ein solcher Test sogar durchgeführt und entweder keine Schwachstelle gefunden oder eine Schwachstelle im Nachgang des Tests behoben.

8. Zwei-Faktor-Authentisierung

Immer wenn ein Zugriff aus dem Internet auf personenbezogene Daten der Gesundheitseinrichtung mit einem gewissen Schutzbedarf möglich ist, sollte die Notwendigkeit einer Zwei-Faktor-Authentisierung geprüft und vom Datenschutzbeauftragten ggf. eingefordert werden. In der Praxis bietet sich hier oftmals der Einsatz von speziellen Tokens oder die Nutzung von sog. Authenticator-Apps an.



9. Corona-Maßnahmen im Blick behalten

Ein Teil dieser Ausgabe des Newsletters beschäftigt sich mit der Kontaktverfolgung nach Maßgabe der jeweiligen Corona-Verordnungen der Länder. Aber auch darüber hinaus entstehen in der Praxis zahlreiche Fragen oder Anforderungen, die der aktuellen Situation geschuldet sind.

Datenschutzbeauftragte sollten darauf achten, hier jeweils eng eingebunden zu werden. Problematisch sind in der Praxis regelmäßig folgende Vorhaben:

- Ein Arbeitgeber kann die Beschäftigten grundsätzlich nicht verpflichten, die Corona-WarnApp des Bundes zu nutzen. Selbst eine Nutzungspflicht auf Dienst-handys ist datenschutzrechtlich nicht vertretbar. Rechtsgrundlage der Nutzung der Corona-WarnApp ist die freiwillige Entscheidung des Nutzers und nicht die Anordnung des Arbeitgebers.
- Die Messung der Körpertemperatur vor Arbeitsantritt ist datenschutzrechtlich äußerst kritisch. In der Regel fehlt es bei einer solchen Maßnahme schon an der Geeignetheit.
- Gesundheitseinrichtungen müssen sich Gedanken über die Prozesse machen, die eingeleitet werden, wenn ein Beschäftigter mitteilt, dass er am Coronavirus erkrankt ist. Sofern nicht die Gesundheitsbehörden die Information von Kontaktpersonen innerhalb der Gesundheitseinrichtung übernehmen, sollte die Einrichtung selbst mit dieser Information nur vorsichtig umgehen. Dass bedeutet, dass man Kontaktpersonen zwar informieren darf, dass sie in Kontakt mit

einer erkrankten Person standen und daher selbst Kontaktperson einer bestimmten Kategorie sind. Der Name der erkrankten Person bzw. der Personenbezug sollte jedoch wo möglich nicht durch den Arbeitgeber gegenüber den Kollegen offenbart werden.

10. Videokonferenztools datenschutzrechtlich bewerten und dokumentieren

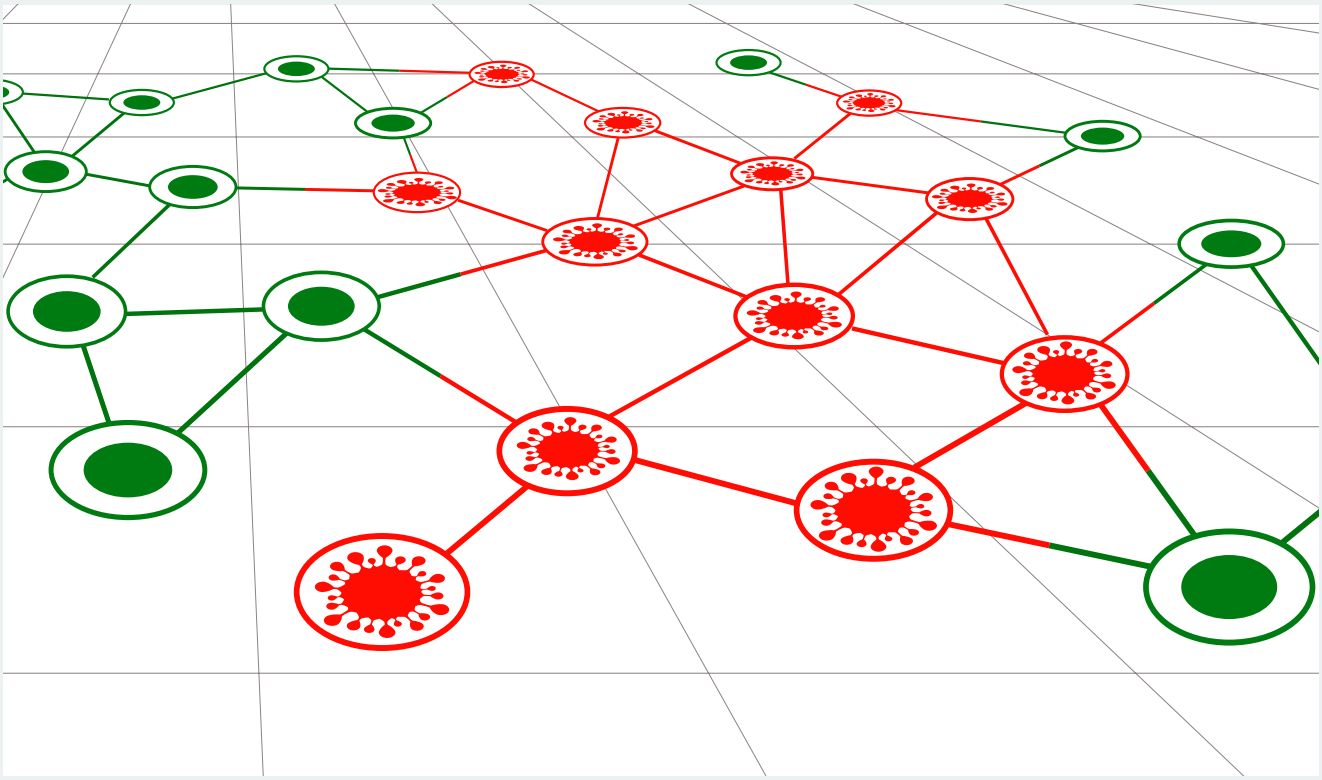
Einen wahren Boom erleben derzeit (aus gutem Grund) Videokonferenzlösungen. Diese sollten datenschutzrechtlich geprüft und dokumentiert werden. Zudem sollten Gesundheitseinrichtungen über eine Art. 13 DSGVO-Information für Teilnehmer verfügen, die z.B. zusammen mit dem Einladungslink versendet werden kann.

In der Praxis sollte insbesondere auf Folgendes geachtet werden:

- Nur die wenigsten Anbieter bieten eine echte Ende-zu-Ende Verschlüsselung an. Hier gehen die Anforderungen mancher Aufsichtsbehörde ggf. an der Praxis vorbei.
- Sofern externe Dienstleister eingesetzt werden, stellen sich eine Reihe von Fragen, u.a.: Ist mit dem Dienstleister ein Vertrag zur Auftragsverarbeitung geschlossen worden? Sofern Daten betroffen sind, die dem Berufsgeheimnis des § 203 StGB unterliegen, muss sogar geprüft werden, ob der Vertrag eine Verpflichtung des Dienstleisters und der mitwirkenden Personen i.S.d. § 203 StGB enthält. Sofern Daten die EU verlassen, muss das angemessene Datenschutzniveau gewährleistet werden – was angesichts des eingangs dargestellten Urteils des EuGHs nicht mehr ganz einfach sein wird. Ggf. müssen gerade Gesundheitseinrichtungen hier auf selbst gehostete Lösungen umschwenken und können Videokonferenzkonferenztools nicht als Software as a Service „von der Stange“ buchen.

Fazit

Die Arbeit des Datenschutzbeauftragen wird nicht weniger und selbst etablierte Prozesse müssen immer wieder hinterfragt werden. Es wird deutlich, dass auch gut zwei Jahre nach Einführung der DSGVO nicht wirklich Ruhe in den Themenbereich eingekehrt ist und es weiterhin wichtig ist, dass dem Datenschutzbeauftragten für seine Arbeit genügend zeitliche und materielle Ressourcen zur Verfügung gestellt werden.



Corona - Kontaktnachverfolgung

Nach dem Lockdown und der Schließung vieler Einrichtungen im Gesundheits- und Pflegebereich für den Publikumsverkehr im Frühjahr 2020 beschlossen die Landesgesetzgeber zum Sommeranfang allmähliche Lockerungen. Die aktuell steigenden Infektionszahlen zeigen, dass die Situation noch längst nicht überstanden ist und das Thema der Kontaktverfolgung die Einrichtungen noch lange beschäftigen wird.

Dr. Sebastian Ertel

Einheitliche Regelungen?

Nach § 32 Infektionsschutzgesetz (IfSG) sind die einzelnen Bundesländer ermächtigt, „durch Rechtsverordnungen […] Gebote und Verbote zur Bekämpfung übertragbarer Krankheiten zu erlassen." Dieses Recht haben alle 16 Landesregierungen wahrgenommen und für ihren räumlichen Zuständigkeitsbereich Landes-Corona-Verordnungen erlassen. Es gibt somit 16 Corona-Verordnungen (CoronaVO), mit zum Teil unterschiedlichen Anforderungen bezüglich der Kontaktnachverfolgung.

Datenverarbeitung zur Kontaktnachverfolgung

Jede CoronaVO regelt in einem der ersten Paragrafen, welche Daten zur Kontaktnachverfolgung zu verarbeiten sind. Bereits dabei zeigen sich Unterschiede, die hier anhand der Regelungen einiger Bundesländer exemplarisch dargestellt werden sollen:

Nach **§ 4 CoronaVO NDS** müssen Vor- und Familienname, Anschrift, Telefonnummer sowie Erhebungsdatum und -uhrzeit erhoben werden. Aufbewahrungsdauer: drei Wochen.

§ 6 CoronaVO BW: Vor- und Nachname, Anschrift, Datum und Zeitraum der Anwesenheit, Telefonnummer. Aufbewahrungsdauer: drei Wochen.

§ 8 CoronaVO HB: Name und Kontaktdaten (Telefonnummer oder E-Mail-Adresse), Zeitpunkt des Betretens und Verlassens der Einrichtung. Aufbewahrungsdauer: drei Wochen.

§ 3 Abs. 4 CoronaVO TH: Name und Vorname, Wohnanschrift oder Telefonnummer, Datum, Beginn und Ende der jeweiligen Anwesenheit. Aufbewahrungsdauer: drei Wochen.

Anlage 35 zu **§ 6 Abs. 3 CoronaVO MW:** Vor- und Familienname, Anschrift, Telefonnummer. Aufbewahrungsdauer: vier Wochen.

Weitere Datenverarbeitungen?

Häufig werden auch Daten zum Gesundheitszustand und zu Kontakten abgefragt. Dies erfolgt meist unter Verweis auf ein Dokument des Robert-Koch-Instituts (hier abrufbar). Bei diesen zusätzlichen Daten (insbesondere Krankheitssymptomen und Kontakten zu Personen, die an COVID-19 erkrankt sind) ist Vorsicht geboten. Die Verarbeitung dieser Daten ist von den CoronaVO nicht erfasst und kann wohl auch nicht auf eine andere Rechtsgrundlage gestützt werden.

Umsetzung der Kontaktnachverfolgung

Neben dem Umfang der Datenerhebung ist auch deren konkrete Umsetzung zu betrachten. Da die Datenerhebung grundsätzlich in Papierform erfolgt, muss gewährleistet sein, dass keine ausgefüllten Zettel unbeachtet herumliegen. Auch sollte auf Sammellisten verzichtet werden. In beiden Fällen besteht die Gefahr, dass die Daten zur Kenntnis unbefugter Personen gelangen und von diesen zweckwidrig genutzt werden.

Die ausgefüllten Meldungen sollten an zentraler Stelle dem Pflegepersonal übergeben oder mittels einer Box/Urne zugriffsgeschützt gesammelt werden. Auch sollte der Bereich, in dem die Meldungen ausgefüllt werden, regelmäßig in Augenschein genommen werden. Hierdurch können umherliegende Meldungen eingesammelt oder unzulässige Zugriffe bzw. Zugriffsversuche festgestellt werden.

Die Aufbewahrung der Meldungen sollte ebenfalls zentral erfolgen. Hier bietet es sich bei einer papierbezogenen Erhebung an, die Dokumente entsprechend der jeweiligen Aufbewahrungsfrist in einer nach Datum sortierten Registratur abzuheften. Dies erleichtert später die Aussortierung der Meldungen nach Ablauf der Aufbewahrungsfrist. Die Meldungen sind zugriffsgeschützt, in einem verschlossenen Schrank oder Büro mit eingeschränkten Zutrittsmöglichkeiten aufzubewahren.

Nach Ablauf der Aufbewahrungsfrist (je nach Bundesland in der Regel zwischen drei und vier Wochen) sind die Meldungen datenschutzkonform zu vernichten. Das kann einerseits über die Dokumentensammeltonnen zertifizierter Aktenvernichtungsunternehmen erfolgen. Andererseits können diese auch geschreddert werden. In diesem Fall sollte auf einen Schredder zurückgegriffen werden, der mindestens die Stufe P4 der DIN 66399 erfüllt.

Wenn eine Behörde anfragt?

Die CoronaVO stellen klar, dass die Meldungen auf Verlangen dem zuständigen Gesundheitsamt vorzulegen sind (z.B.: § 4 S. 3 CoronaVO NDS, § 6 Abs. 1 S. 1 CoronaVO BW). In der letzten Zeit häuften sich Pressemitteilungen, dass sich auch die Polizei vermehrt für die Meldungen zur Kontaktnachverfolgung interessiert, um Ordnungswidrigkeiten oder Straftaten aufzuklären (z.B. Abfrage von Gästedaten in einem Hamburger Restaurant). Dieses Vorgehen wird derzeit kontrovers diskutiert. In einzelnen Konstellationen kann ein Zugriff zulässig sein. Es gibt aber auch Sachverhalte, bei denen auf entsprechende Anfragen zurückhaltend zu reagieren ist. Beteiligen Sie bei derartigen Anfragen unbedingt den Datenschutzbeauftragten der Einrichtung.

Was sonst noch?

Werden erstmalig personenbezogene Daten für einen konkreten Zweck erhoben, löst dies eine Informationspflicht gegenüber dem Betroffenen nach Art. 13 DSGVO bzw. § 15 KDG (katholische Einrichtungen) oder § 17 DSG-EKD (evangelische Einrichtungen) aus. Die Einrichtungen müssen über den Zweck der Datenerhebung zur Kontaktnachverfolgung informieren. Ferner sind insbesondere die Rechtsgrundlagen der Datenverarbeitung, die Löschfristen, potentielle Datenempfänger (Gesundheitsamt und ggf. Polizei) sowie die Betroffenenrechte zu nennen.

Checkliste

Mit der nachfolgenden Checkliste können Sie selbst überprüfen, ob der Prozess der Kontaktnachverfolgung in

Ihrer Einrichtung gut umgesetzt ist (das ist der Fall, wenn Sie bei jedem Punkt einen Haken setzen können):

- Erhebung nur der Daten, die in der CoronaVO genannt sind
- Erfüllung von Informationspflichten nach Art. 13 DSGVO bzw. § 15 KDG oder § 17 DSG-EKD
- ausreichender Schutz der ausgefüllten Meldungen vor Zugriffen Unbefugter
- keine Nutzung von Sammelmeldungen
- zentrale Aufbewahrung der Meldungen für den vorgeschriebenen Zeitraum
- täglich Aussortierung der Meldungen, bei denen keine Aufbewahrungspflicht mehr besteht
- datenschutzkonforme Vernichtung der aussortierten Meldungen

Kurznotiz:

Die erste Aufsichtsbehörde veröffentlicht eine Orientierungshilfe zum internationalen Datentransfer

Wie bereits in dieser Ausgabe dargestellt, hat der EuGH mit Urteil vom 16. Juli 2020 das Privacy Shield für unwirksam erklärt und auch die Standarddatenschutzklauseln in Frage gestellt. In der Praxis führt dies für Stellen, die ihre Verarbeitungstätigkeiten eng mit Dienstleistern in unsicheren Drittstaaten verwoben haben, zu einer sehr herausforderungsvollen Situation.

Als erste Aufsichtsbehörde hat nun der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg unter dem Titel „Was jetzt in Sachen internationaler Datentransfer?“ eine Orientierungshilfe veröffentlicht.

Die Orientierungshilfe erklärt den Hintergrund der Entscheidung und stellt dar, dass diese nicht nur im Hinblick auf US-Dienstleister gilt, sondern allgemein die Verarbeitung in unsicheren Drittstaaten ohne angemessenes Datenschutzniveau betrifft. Wer dort Daten verarbeiten lässt, muss diese Datenverarbeitung nun im Einzelfall prüfen und ggf. zusätzliche Maßnahmen mit dem Datenimporteur vereinbaren. Solche Maßnahmen können nach der Orientierungshilfe z.B. sein:

- Verschlüsselung der Daten (ohne Entschlüsselungsmöglichkeit des Datenimporteurs)
- Pseudonymisierung von Daten

Die Orientierungshilfe rät zudem dazu, sich mit den betroffenen Dienstleistern in Verbindung zu setzen, die Lage zu besprechen und neben zusätzlichen Maßnahmen ggf. Anpassungen an den Standarddatenschutzklauseln vorzunehmen.

Die Orientierungshilfe weist zudem darauf hin, dass neben Clouddiensten in den USA auch die Nutzung von Videokonferenzsystemen von dem Urteil betroffen sein kann und sogar eine Datenverarbeitung im Vereinigten Königreich.

Datenschutz im Gesundheitswesen

Grundlagenwissen – Praxislösungen – Entscheidungshilfen

2 Ordner mit Register im Format DIN A5,
ca. 1.500 Seiten Inhalt
ISBN: 978-3-553-43000-5

Bis zum 31.12. 2020 nur 5% USt.

Preis: **173,88.-** inkl. MwSt.

3-4 kostenpflichtige Nachtragslieferungen pro Jahr zum Preis von jeweils 83,31 Euro inkl. MwSt. und versandkostenfreier Zusendung im Inland.

Peisinfo:
Die genannten Preise verstehen sich inkl. gesetzlicher Umsatzsteuer (bis 31.12.2020 = 5%; ab dem 1.1.2021 = 7%. Maßgeblich für die Bestimmung des Steuersatzes ist der Zeitpunkt der Leistungserbringung.)