Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 3. April 2020

Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

- Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.
- Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.
- Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder - wie eine vorherige Anonymisierung - sogar gar nicht in die Rechte der Menschen eingreifen, müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten **nicht** - wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung - **außer**

Verhältnis zum angestrebten legitimen Zweck stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen - etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

- Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.
- Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie

Gültigkeit vorerst bis zum 19.4.2020

Insbesondere die effiziente Behandlung von Corona-Patienten sowie die Schulschließungen machen in deutlich größerem Umfang elektronische Kommunikation zwingend erforderlich. Da es in der Kürze der Zeit für die öffentlichen Stellen schwierig ist, hierfür dienstliche Geräte zur Verfügung zu stellen, akzeptiert der Bayerische Landesbeauftragte vorübergehend die Verwendung von Privatgeräten sowie die Nutzung von Messengern und Clouddiensten unter gewissen Rahmenbedingungen:

Videokonferenzen und Messengerdienste zur Kommunikation von Beschäftigten in öffentlichen Stellen (Ärzte, Pflegepersonal, Lehrer etc.) untereinander sowie mit Personen außerhalb öffentlicher Einrichtungen (Patienten, Schüler, Studierende, Antragsteller etc.): Dafür dürfen auch nicht-dienstliche Geräte genutzt werden, wenn folgende technische Bedingungen eingehalten werden:

- Idealerweise sollte keine Speicherung von sensiblen Daten auf dem Privatgerät erfolgen, ansonsten muss die Möglichkeit zur unkomplizierten Löschung der Daten bestehen.
- Die Kommunikation sollte möglichst datensparsam erfolgen.
- Mobile Geräte müssen mindestens durch eine PIN oder ein Passwort geschützt werden.
- Sobald die Nutzung dieser Dienste nicht mehr erforderlich ist, sind die damit verarbeiteten personenbezogenen Daten zu löschen, insbesondere die zu diesem Zweck gespeicherten Telefonnummern von privaten Geräten.

Krankenhäuser, Gesundheitsbereich

Für Krankenhäuser und den Gesundheitsbereich gibt es darüber hinaus folgende Einschränkungen:

- Für die Verarbeitung von sensiblen Daten ist in jedem Fall ist eine Ende-zu-Ende-Verschlüsselung der Kommunikation umzusetzen.
- Die Anforderungen des "Whitepaper" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 07.11.2019 "Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich" sollte weitestgehend umgesetzt werden.
- Es darf in Abweichung zu Nr. IV.8 keine Anbindung an die sonstigen IT-Systeme des Krankenhauses, Gesundheitsamts etc. erfolgen, um die IT-Sicherheit nicht zu gefährden.
- Zugriff auf das KIS und Fachverfahren der öffentlichen Stelle:
    - In Abweichung zu den Ausführungen im 25. Tätigkeitsbericht unter Nr. 2.2.5 dürfen Privatgeräte genutzt werden, wenn die dort formulierten Anforderungen auf den Privatgeräten umgesetzt werden.
    - Insbesondere muss eine zugriffsgeschützte virtuelle Arbeitsumgebung zum Einsatz kommen, so dass auf dem Privatgerät keine medizinischen Daten gespeichert werden können.
    - Ein Zugriff auf den E-Mail-Server kann auf Privatgeräten (z.B. OWA) ermöglicht werden, wenn sichergestellt ist, dass keine Speicherung der E-Mails oder von Anhängen auf

dem Privatgerät möglich ist.

- Vor einer Nutzung auf Privatgeräten muss die IT-Abteilung oder der IT-Sicherheitsbeauftragte prüfen, ob damit Sicherheitsrisiken für die IT der öffentlichen Stellen entstehen, z.B. durch Schadsoftware auf dem Privatgerät. Der behördliche Datenschutzbeauftragte ist frühzeitig zu beteiligen.
- Die Mitarbeiter müssen eine Erlaubnis zur Nutzung von Privatgeräten beantragen und die Erforderlichkeit dokumentiert werden. Der Zugang soll nicht pauschal allen Mitarbeitern eröffnet werden. Zudem sind Regelungen aufzustellen, um die Pflichten für die Nutzer festzulegen.

Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder erreichen vermehrt Anfragen von Arbeitgebern/Dienstherren, ob und wie personenbezogene Daten von Mitarbeitern sowie Gästen und Besuchern bei im Zusammenhang mit der Corona-Pandemie stehenden Maßnahmen verarbeitet werden können. Dazu einige allgemeine Hinweise:

Werden im Zusammenhang mit der Corona-Pandemie personenbezogene Daten erhoben, werden in den meisten Fällen Bezüge zwischen Personen und deren Gesundheitszustand hergestellt. Ab diesem Zeitpunkt handelt es sich um Gesundheitsdaten, die nach Artikel 9 Datenschutz-Grundverordnung (DSGVO) besonders geschützt sind.

Auch wenn eine Verarbeitung von Gesundheitsdaten grundsätzlich nur restriktiv möglich ist, können für verschiedene Maßnahmen zur Eindämmung der Corona-Pandemie oder zum Schutz von Mitarbeiterinnen und Mitarbeitern datenschutzkonform Daten erhoben und verwendet werden. Dabei ist der Grundsatz der Verhältnismäßigkeit und der gesetzlichen Grundlage stets zu beachten.

Beispielsweise können die folgenden Maßnahmen zur Eindämmung und Bekämpfung der Corona-Pandemie als datenschutzrechtlich legitimiert betrachtet werden:

- Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Beschäftigten durch den Arbeitgeber oder Dienstherren um eine Ausbreitung des Virus unter den Beschäftigten bestmöglich zu verhindern oder einzudämmen. Hierzu zählen insbesondere Informationen zu den Fällen:
    - in denen eine Infektion festgestellt wurde oder Kontakt mit einer nachweislich infizierten Person bestanden hat.
    - in denen im relevanten Zeitraum ein Aufenthalt in einem vom Robert-Koch-Institut (RKI) als Risikogebiet eingestuften Gebiet stattgefunden hat.
- Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern, insbesondere um festzustellen, ob diese
    - selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen.
    - sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben.
- Die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von Kontaktpersonen ist demgegenüber nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen ausnahmsweise erforderlich ist.

Rechtliche Hintergrundinformationen:

Die vorstehenden Maßnahmen lassen sich rechtlich auf Grundlage der DSGVO und des BDSG (ggf. in Verbindung mit Landesdatenschutz- und weiteren Fachgesetzen) legitimieren. Je nach Maßnahme

können die einschlägigen Rechtsgrundlagen dabei leicht variieren. Ungeachtet dessen gelten aber die folgenden allgemeinen Grundsätze:

Die Berechtigung zur Verarbeitung personenbezogener Mitarbeiterdaten ergibt sich in diesen Fällen für öffentlich-rechtliche Arbeitgeber grundsätzlich aus Art. 6 Abs. 1 Satz 1 lit. e) DSGVO und für Arbeitgeber im nicht-öffentlichen Bereich aus § 26 Abs 1 BDSG bzw. Art. 6 Abs. 1 Satz 1 lit. f) DSGVO jeweils i.V.m. den einschlägigen beamtenrechtlichen sowie tarif-, arbeits- und sozialrechtlichen Regelungen des nationalen Rechts. Soweit Gesundheitsdaten verarbeitet werden, sind zudem auch § 26 Abs. 3 BDSG und Art. 9 Abs. 2 lit. b) DSGVO einschlägig. Bei Art. 9 Abs. 2 lit. b) DSGVO umfasst der Begriff "Arbeitsrecht" nach Auffassung der Datenschutzaufsichtsbehörden auch das deutsche Beamtenrecht. Zugunsten des öffentlich-rechtlichen Arbeitgebers könnte zusätzlich Art. 9 Abs. 2 lit. g) DSGVO herangezogen werden, da die Fürsorgepflicht im Sinne der Gesundheitsvorsorge hier auch einem wichtigen öffentlichen Interesse dient.

Maßnahmen gegenüber Dritten können bei öffentlichen Stellen auf Art. 6 Abs. 1 Satz 1 lit. c) und e) ggf. in Verbindung mit den jeweiligen Landesdatenschutzgesetzen gestützt werden. Im nicht-öffentlichen Bereich kann Art. 6 Abs. 1 Satz 1 lit. f) DSGVO als Rechtsgrundlage herangezogen werden. Soweit besonders sensible Daten wie Gesundheitsdaten betroffen sind, findet zudem Art. 9 Abs. 2 lit. i) i.V.m. § 22 Abs. 1 Nr. 1 lit. c) BDSG Anwendung.

Die Fürsorgepflicht der Arbeitgeber bzw. der Dienstherren verpflichtet diese den Gesundheitsschutz der Gesamtheit ihrer Beschäftigten sicherzustellen. Hierzu zählt nach Ansicht der unabhängigen Datenschutzaufsichtsbehörden auch die angemessene Reaktion auf die epidemische bzw. inzwischen pandemische Verbreitung einer meldepflichtigen Krankheit, die insbesondere der Vorsorge und im Fall der Fälle der Nachverfolgbarkeit (also im Grunde nachgelagerte Vorsorge gegenüber den Kontaktpersonen) dient. Diese Maßnahmen müssen dabei natürlich immer auch verhältnismäßig sein. Die Daten müssen vertraulich behandelt und ausschließlich zweckgebunden verwendet werden. Nach Wegfall des jeweiligen Verarbeitungszwecks (regelmäßig also spätestens dem Ende der Pandemie) müssen die erhobenen Daten unverzüglich gelöscht werden.

Eine Einwilligung der von Maßnahmen Betroffenen allein sollte hingegen vorliegend nur als datenschutzrechtliche Verarbeitungsgrundlage in Betracht gezogen werden, wenn die Betroffenen über die Datenverarbeitung informiert sind und freiwillig in die Maßnahme einwilligen können.

Zusätzlich zu den bestehenden Rechtsgrundlagen für die Datenverarbeitung auf Seiten des Arbeitgebers ergeben sich aus dem Beamtenrecht, aus dem Tarifrecht bzw. dem Arbeitsrecht für Beschäftigte verschiedene Nebenpflichten, unter anderem auch Rücksichts-, Verhaltens- und Mitwirkungspflichten gegenüber ihrem Arbeitgeber und Dritten. Vorliegend stellt nach Auffassung der Datenschutzaufsichtsbehörden beispielsweise die Pflicht zur Information des Dienstherrn bzw. des Arbeitgebers über das Vorliegen einer Infektion mit dem Corona-Virus eine solche Nebenpflicht zum Schutz hochrangiger Interessen Dritter dar, aus der unter gewissen Voraussetzungen auch eine Offenlegungsbefugnis gemäß Art. 6 Abs. 1 lit. c) und f) DSGVO bezüglich personenbezogener Daten der Kontaktpersonen folgt.