Statement

Erklärung zur Verarbeitung personenbezogener Daten im Zusammenhang mit COVID-19

Angenommen am 19. März 2020

Der Europäische Datenschutzausschuss hat folgende Erklärung abgegeben:

In ganz Europa ergreifen Staaten sowie öffentliche und private Organisationen Maßnahmen, um die Ausbreitung von COVID-19 einzudämmen und abzumildern. Dies kann auch die Verarbeitung verschiedener Arten von personenbezogenen Daten beinhalten.

Die Datenschutzvorschriften (wie die DSGVO) stehen der Ergreifung von Maßnahmen gegen die Coronavirus-Pandemie nicht entgegen. Die Bekämpfung übertragbarer Krankheiten ist ein wichtiges Ziel, dem sich alle Nationen verschrieben haben und das daher bestmöglich unterstützt werden sollte. Es liegt im Interesse der Menschheit, dass die Ausbreitung von Krankheiten eingedämmt wird und Seuchen, die weite Teile der Welt betreffen, mit moderner Technik bekämpft werden. Dennoch möchte der EDSA unterstreichen, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter den Schutz der personenbezogenen Daten der betroffenen Personen auch in dieser Ausnahmesituation sicherstellen müssen. Um die rechtmäßige Verarbeitung personenbezogener Daten zu gewährleisten, sollte daher eine Reihe von Erwägungen berücksichtigt und stets beachtet werden. Insbesondere ist darauf zu achten, dass jede in diesem Zusammenhang ergriffene Maßnahme den allgemeinen Rechtsgrundsätzen entsprechen und reversibel sein muss. Ein Notfall kann als rechtliche Bedingung eine Einschränkung von Freiheiten rechtfertigen, sofern diese Beschränkungen verhältnismäßig und zeitlich auf die Notlage befristet sind.

1. Rechtmäßigkeit der Verarbeitung

Die **DSGVO ist ein umfassender Rechtsakt und enthält Vorschriften, die auch für die Verarbeitung personenbezogener Daten in Fällen wie der COVID-19-Krise gelten**. **Die DSGVO gibt den zuständigen Gesundheitsbehörden und den Arbeitgebern die Möglichkeit, personenbezogene Daten bei einer Epidemie nach Maßgabe des nationalen Rechts und der darin festgelegten Bedingungen zu verarbeiten**, beispielsweise wenn die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist. Unter diesen Umständen ist die Einwilligung der betroffenen Personen nicht erforderlich.

1.1 Was die Verarbeitung personenbezogener Daten, einschließlich besonderer Datenkategorien, durch zuständige Behörden (z. B. Gesundheitsbehörden) angeht, so vertritt der EDSA die Auffassung, dass die Artikel 6 und 9 DSGVO die Verarbeitung personenbezogener Daten gestatten, insbesondere

wenn diese im Rahmen des im nationalen Recht vorgesehenen rechtlichen Auftrags der Behörde erfolgt und die in der DSGVO festgelegten Bedingungen erfüllt sind.

1.2 Im Beschäftigungskontext kann die Verarbeitung personenbezogener Daten erforderlich sein, damit rechtliche Pflichten des Arbeitgebers erfüllt werden können, beispielsweise im Hinblick auf die Gesundheit und Sicherheit am Arbeitsplatz oder ein öffentliches Interesse wie die Bekämpfung von Krankheiten und anderen Gesundheitsgefahren. Die DSGVO sieht auch Ausnahmen vom Verbot der Verarbeitung bestimmter besonderer Kategorien personenbezogener Daten, wie von Gesundheitsdaten, vor, wenn die Verarbeitung aus Gründen eines wesentlichen öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Artikel 9 Absatz 2 Buchstabe i) auf der Grundlage des Unionsrechts oder des nationalen Rechts oder zum Schutz lebenswichtiger Interessen der betroffenen Person (Artikel 9 Absatz 2 Buchstabe c) erforderlich ist, wobei in Erwägungsgrund 46 ausdrücklich auf die Eindämmung einer Epidemie verwiesen wird.

1.3 Was die Verarbeitung von Telekommunikationsdaten wie Standortdaten angeht, müssen auch die nationalen Rechtsvorschriften zur Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation eingehalten werden. Standortdaten dürfen vom Betreiber grundsätzlich nur dann verwendet werden, wenn sie anonymisiert wurden oder die Betroffenen ihre Einwilligung erteilt haben. Nach Artikel 15 der **Datenschutzrichtlinie für elektronische Kommunikation dürfen die Mitgliedstaaten jedoch Rechtsvorschriften zum Schutz der öffentlichen Sicherheit erlassen.** Eine solche Sondergesetzgebung ist nur möglich, **wenn sie in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist**. Die Maßnahmen müssen mit der Charta der Grundrechte und der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen. Darüber hinaus **unterliegen sie der gerichtlichen Kontrolle durch den Europäischen Gerichtshof und den Europäischen Gerichtshof für Menschenrechte.** In einer Notsituation sollten sie außerdem zeitlich strikt auf deren Dauer beschränkt sein.

2. Zentrale Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten, die zur Erreichung der angestrebten Ziele erforderlich sind, dürfen nur für die festgelegten eindeutigen Zwecke verarbeitet werden.

Darüber hinaus sollten die betroffenen Personen transparente Informationen darüber erhalten, welche Verarbeitungstätigkeiten durchgeführt werden und wie diese gestaltet sind, insbesondere auch darüber, wie lange die erhobenen Daten gespeichert und für welche Zwecke sie verarbeitet werden. Diese Informationen sollten leicht zugänglich und in klarer und einfacher Sprache formuliert sein.

Wichtig ist die Einführung angemessener Sicherheitsmaßnahmen und Vertraulichkeitsvorschriften, die gewährleisten, dass personenbezogene Daten nicht an Unbefugte weitergegeben werden. Die Maßnahmen zur Bewältigung der aktuellen Notlage und der jeweilige Beschlussfassungsprozess sollten angemessen dokumentiert werden.

3. Verwendung der Standortdaten von Mobilfunknutzern

- **Dürfen die Regierungen der Mitgliedstaaten auf personenbezogene Daten von Handy-Nutzern zurückgreifen, um die Ausbreitung von COVID-19 zu überwachen, einzudämmen oder abzumildern?**

In einigen Mitgliedstaaten soll auf Standortdaten von Mobilfunknutzern zurückgegriffen werden, um die Ausbreitung von COVID-19 zu überwachen, einzudämmen oder abzumildern. Dadurch bestünde

beispielsweise auch die Möglichkeit, Einzelpersonen zu orten oder Mitteilungen zu Fragen der öffentlichen Gesundheit per Telefon oder Textnachricht an Menschen in bestimmten Regionen zu richten. **Die Behörden sollten Standortdaten vorzugsweise anonymisiert verarbeiten (d. h. Daten, die so aggregiert sind, dass Rückschlüsse auf die Identität von Personen nicht möglich sind). Auf diese Weise könnten Berichte über eine örtliche Häufung von Mobilfunkgeräten generiert werden („Kartografie").**

Ordnungsgemäß anonymisierte Daten fallen nicht unter die Vorschriften zum Schutz personenbezogener Daten.

Ist die ausschließliche Verarbeitung anonymisierter Daten nicht möglich, haben die Mitgliedstaaten nach der Datenschutzrichtlinie für elektronische Kommunikation die Möglichkeit, Rechtsvorschriften zum Schutz der öffentlichen Sicherheit zu erlassen (Artikel 15)**.**

Werden Maßnahmen eingeführt, die die Verarbeitung nicht anonymisierter Standortdaten ermöglichen, so muss der betreffende Mitgliedstaat **angemessene Garantien** vorsehen, z. B. indem er den Nutzern elektronischer Kommunikationsdienste das **Recht auf einen gerichtlichen Rechtsbehelf** einräumt.

Außerdem gilt der Grundsatz der Verhältnismäßigkeit. Lösungen, die im Verhältnis zum verfolgten Zweck den geringsten Eingriff bedeuten, sollten stets den Vorzug erhalten. Im Ausnahmefall und in Abhängigkeit von den konkreten Modalitäten der Verarbeitung könnten auch eingreifende Maßnahmen wie die Erstellung von „Bewegungsprofilen" für einzelne Personen (d. h. die Verarbeitung nicht anonymisierter historischer Standortdaten) als verhältnismäßig angesehen werden. Jedoch sollten hierbei eine verschärfte Überprüfung und verstärkte Garantien wirksam werden, um die Einhaltung der Datenschutzgrundsätze (Verhältnismäßigkeit der Maßnahme in Bezug auf Dauer und Anwendungsbereich, befristete Datenspeicherung und Zweckbindung) zu gewährleisten.

4. Beschäftigung

- **Kann ein Arbeitgeber im COVID-19-Kontext von Besuchern oder Mitarbeitern bestimmte Gesundheitsauskünfte verlangen?**

Der Grundsatz der Verhältnismäßigkeit und der Datenminimierung ist hier besonders wichtig. Der Arbeitgeber sollte Angaben zur Gesundheit nur verlangen, soweit dies nach nationalem Recht zulässig ist.

- **Dürfen Arbeitgeber ihre Belegschaft einer ärztlichen Untersuchung unterziehen?**

Das hängt vom nationalen Arbeitsrecht bzw. Arbeitsschutz ab. Arbeitgeber sollten Gesundheitsdaten nur dann abfragen und verarbeiten, wenn sie rechtlich dazu verpflichtet sind.

- **Darf ein Arbeitgeber die eigene Belegschaft oder Außenstehende darüber informieren, dass ein Belegschaftsmitglied mit COVID-19 infiziert ist?**

Die Arbeitgeber sollten ihr Personal über COVID-19-Fälle informieren und Schutzmaßnahmen ergreifen, jedoch nicht mehr Informationen preisgeben als nötig. Ist es (z. B. zur Prävention) erforderlich, den Namen des infizierten Belegschaftsmitglieds zu nennen, und ist dies nach nationalem

Recht zulässig, müssen die Betroffenen vorab unterrichtet und ihre Würde und Integrität gewahrt werden.

- **Welche im COVID-19-Kontext verarbeiteten Daten können Arbeitgeber einholen?**

Arbeitgeber können personenbezogene Daten einholen, um ihre Pflichten zu erfüllen und die Organisation der Arbeit gemäß den nationalen Rechtsvorschriften sicherzustellen.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)