DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE (EDSB)

Orientierungspunkte des Europäischen Datenschutzbeauftragten zu den Reaktionen der EU-Institutionen in ihrer Rolle als Arbeitgeber auf die COVID-19-Krise

15. Juli 2020

Zusammenfassung

Die Organe, Einrichtungen und sonstigen Stellen der Union mussten auf die COVID-19-Krise reagieren, nicht nur in der Wahrnehmung ihrer Kernaufgaben, sondern auch in ihrer Rolle als Arbeitgeber. Änderungen der betrieblichen Abläufe, zum Beispiel der Wechsel eines Großteils der Mitarbeiter in die Telearbeit, warfen zahlreiche Fragen auf, zu denen der Europäische Datenschutzbeauftragte von EU-Institutionen konsultiert wurde.

Dieses Dokument enthält eine Zusammenstellung der Ratschläge, die zu Tools für die Telearbeit, Personalverwaltung, Gesundheitsdaten betreffenden Aspekten und der Beantwortung von Auskunftsersuchen betroffener Personen erteilt wurden.

Das Dokument, das auf der Erfahrung der vergangenen Monate gründet, behandelt die uns gestellten Fragen bzw. uns aufgefallenen Probleme, die auch nach wie vor relevant sind, da die Telearbeit in der „neuen Normalität“ der Arbeit der EU-Institutionen höchstwahrscheinlich eine große Rolle spielen wird.

INHALTSVERZEICHNIS

Inhalt

1. Einleitung

Angesichts des Ausbruchs von COVID-19 waren viele EU-Institutionen gezwungen, ihren Betrieb für die meisten Mitarbeiter fast ausschließlich auf Telearbeit umzustellen. Die EU-Institutionen haben darüber hinaus weitere Anpassungen ihrer Betriebsabläufe vorgenommen und sind jetzt dabei, für die Zeit der Rückkehr ins Büro Maßnahmen zum Schutz von Mitarbeitern und Besuchern zu planen. Dass es sich um eine Notsituation handelt, bedeutet nicht, dass die für die EU-Institutionen geltenden Datenschutzvorschriften außer Acht gelassen werden könnten. **Die für die EU-Institutionen geltenden Datenschutzvorschriften sind flexibel genug, Spielraum für verschiedene Maßnahmen zu lassen, die die Aufrechterhaltung des Geschäftsbetriebs der EU-Institutionen ermöglichen. Der Europäische Datenschutzbeauftragte ist sicher allerdings dessen bewusst, dass einige der sich aus der Notsituation ergebenden Anpassungen unter Umständen nicht von einem Tag auf den anderen vorgenommen werden können.** Allerdings steht außer Zweifel, dass die wesentlichen Datenschutzanforderungen, die in Artikel 8 der Charta der Grundrechte der Europäischen Union und in der Verordnung (EU) 2018/1725 (im Folgenden: Verordnung) niedergelegt sind, etwa die Grundsätze der Rechenschaftspflicht, des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, der Sicherheit und Transparenz nach wie vor Anwendung finden. Als öffentliche Einrichtungen müssen die EU-Institutionen hier mit gutem Beispiel vorangehen, um das Vertrauen, das ihre Mitarbeiter, Interessenträger und die Allgemeinheit in sie setzen, zu schützen.

Auch wenn die EU-Institutionen bereits planen, wie eine schrittweise Rückkehr ins Büro möglich wäre, wird die Telearbeit wahrscheinlich auch in nächster Zukunft noch die neue Normalität prägen. Dieses Dokument gründet auf der Erfahrung der vergangenen Monate und behandelt die Fragen, die uns gestellt wurden, sowie die Probleme, die uns aufgefallen sind.

Adressaten dieses Dokuments sind die Verantwortlichen und Datenschutzbeauftragten (DSB) in den EU-Institutionen. Bei der Ausarbeitung der Krisenreaktionen ihrer Organisation sollten die Verantwortlichen frühzeitig den Datenschutzbeauftragten ihrer EU-Institution konsultieren. Die Datenschutzbeauftragten geben den Verantwortlichen Orientierung und Beratung; letzten Endes sind es jedoch die Verantwortlichen, die für die Einhaltung der Verordnung rechenschaftspflichtig sind; diese Verantwortlichen werden in diesem Dokument mit Pronomen der 2. Person angesprochen (für dieses Dokument bedeutet das, dass sich zum Beispiel das Wort „Sie“ in dem Satz „Sie müssen X tun“ auf den Verantwortlichen bezieht).

2. Tools für die Telearbeit

Der Bedarf an Tools für die Telearbeit – etwa für Konferenzschaltungen, Remote-Zusammenarbeit, Audio- und Videokonferenzen sowie Onlinekurse – zur Aufrechterhaltung des Geschäftsbetriebs ist in extrem kurzer Zeit dramatisch gestiegen. Einige EU-Institutionen besaßen bereits die erforderlichen Tools, während andere noch Lösungen suchen. Wenn Sie wegen der Dringlichkeit der Situation bereits Verträge mit externen Anbietern neuer Produkte und Dienstleistungen unterzeichnet haben, sollten Sie die vereinbarten Konditionen daraufhin überprüfen, ob sie mit der Verordnung in Einklang bestehen, bzw. feststellen, was getan werden kann, um Nichtkonformitätsrisiken auszuschalten.

Der Markt und die Anzahl der angebotenen Tools sind so groß, dass es dem Europäischen Datenschutzbeauftragten nicht möglich ist, einen vollständigen „Einkaufsführer“ für derartige Tools zu erstellen. Wenn Sie Tools für verschiedene EU-Institutionen liefern oder sich der

Auswahl von Services oder Software einer Gruppe von EU-Institutionen anschließen, müssen Sie diese Punkte auch für alle anderen der betreffenden EU-Institutionen prüfen. Besondere, auf der Verordnung beruhende Konditionen sind unter Umständen nicht erforderlich, wenn es bereits ähnliche, den Anforderungen nach der Verordnung (EU) 2016/679 (DSGVO) genügende Vertragsbestandteile gibt, die für Ihre Zwecke genügen (sofern diese nicht mit zusätzlichen oder abweichenden Anforderungen in der Verordnung in Konflikt stehen).

Für die Auswahl datenschutzfreundlicher Tools können wir Ihnen jedoch einige hilfreiche Tipps geben, sowohl zu allgemeinen Fragen als auch zu Gefahren, die Sie besser meiden sollten.

2.1 Entscheidungsprozess

Außergewöhnliche Umstände bringen neue betriebliche Erfordernisse mit sich. Bei der Suche nach angemessenen Tools für die Telearbeit dürfen sich EU-Institutionen dadurch jedoch nicht dazu verleiten lassen, die Datenschutz- und Sicherheitsanforderungen außer Acht zu lassen. Häufig wird es nicht ein einziges Tool sein, das alle Bedürfnisse deckt. Den EU-Institutionen wird deshalb geraten, die Anwendungsfälle zu benennen und deren Anforderungen (einschließlich der Datenschutzvorkehrungen) festzulegen und dann nach den Tools zu suchen, die diesen am besten gerecht werden.

Auch wenn in der derzeitigen Lage unter Umständen schnell entschieden werden muss, **sind die bestehenden Prozesse der IT-Governance Ihrer EU-Institution möglichst einzuhalten**; gleichzeitig ist es erforderlich, auf proaktive Weise etwaige Datenschutzprobleme, die sich aus der vorgesehenen Implementierung der Tools ergeben könnten, festzustellen und Gegenmaßnahmen zu ergreifen (Datenschutz durch Technikgestaltung). In diesen Prozess müssen Sie Ihren **Datenschutzbeauftragten** einbeziehen. Achten Sie darauf, dass es einen Überblick über die eingesetzten Tools sowie eine Vorabbewertung der in den Tools vorgesehenen Funktionalitäten in Bezug auf Sicherheit, Geheimhaltung und Schutz der Privatsphäre gibt und dass Ihre IT-Abteilung darüber Auskunft geben kann, damit die Entscheidung von Ihrer EU-Institution auf guter Informationsgrundlage getroffen werden kann, vorzugsweise auf der höchsten Verwaltungsebene.

Andernfalls bestünde die **Gefahr, dass Teile Ihrer Organisation beginnen, frei erhältliche Tools zu benutzen, die unter Umständen nicht mit der IT-Strategie Ihrer EU-Institution in Einklang stehen**. Dadurch könnten personenbezogene Daten oder sonstige vertrauliche Informationen Dritten oder externen Angreifern bekannt werden, was wiederum Reputations- und sonstige Risiken für Ihre EU-Institution zur Folge haben könnte, die man besser vermeiden würde. Wenn diese Probleme nicht jetzt schon behoben werden, könnten sich auf lange Sicht Lock-in-Effekte ergeben, die zu gravierenden Datenschutzproblemen und zusätzlichen Sicherheitsrisiken führen.

Näheres zu diesen Prozessen ist in den Leitlinien des Europäischen Datenschutzbeauftragten für die Bereiche IT-Governance und IT-Management sowie in der EDPS Preliminary Opinion on privacy by design. [Vorläufige Stellungnahme des EDSB zum Grundsatz des eingebauten Datenschutzes] zu finden.

2.2 Unternehmensgeräte und Privatgeräte

Bei der Benutzung von Privatgeräten für die Telearbeit ist nicht nur an die IT-Sicherheit zu denken, sondern vor allem auch an den Datenschutz. Wenn Mitarbeiter Privatgeräte (Laptops,

Tablets usw.) benutzen, wäre es ratsam, dass Sie Ihre IT-Abteilung wegen möglicher Sicherheitsprobleme oder spezifischer Konfigurationseinstellungen auf den Geräten konsultieren. Werden auf den privaten Geräten personenbezogene Daten verarbeitet, sollte Ihre Institution **den Benutzern klare Regeln vorgeben und Anweisungen dazu erteilen**, wie mit personenbezogenen Daten umzugehen ist (z. B. in Form von IT-Leitlinien zur Telearbeit für Mitarbeiter). Umgekehrt hat Ihre EU-Institution größere Kontrolle über die von den Mitarbeitern verwendete IT-Umgebung, wenn Unternehmensgeräte zur Verfügung gestellt werden; dadurch gibt es auch weniger Anreize zur Bildung einer sogenannten „Schatten-IT".

Darüber hinaus muss Ihre EU-Institution, was die Verwaltung von Anträgen auf Unternehmensgeräte angeht, den Grundsatz der Datenminimierung beachten und jede unnötige Weitergabe personenbezogener Daten vermeiden.

Nähere Information zum Mobile Device Management (MDM), sowohl für Unternehmensgeräte als auch für eigene Geräte der Mitarbeiter, finden Sie in den vom Europäischen Datenschutzbeauftragten erlassenen Leitlinien zum Schutz personenbezogener Daten auf von den EU Organen genutzten mobilen Geräten.

2.3 Rollen des Verantwortlichen / Auftragsverarbeiters

Achten Sie darauf, dass keinerlei personenbezogene Daten von Ihren Mitarbeitern oder deren Kommunikationspartnern für die Verkäufer bzw. Hersteller der Software aus der Software bzw. den Services ersichtlich sind.

EU-Institutionen, die neue Produkte oder Services von externen Anbietern beziehen, sollten stets bestrebt sein, **den datenschutzfreundlichsten Tools den Vorzug zu geben und sicherzustellen, dass sie selbst angemessene Kontrolle darüber haben, wie die externen Anbieter mit den ihnen anvertrauten Daten umgehen**. Selbst wenn sich der Vertrag (z. B. bei den meisten Online-Diensten) auf Allgemeine Geschäftsbedingungen stützt, die für alle Kunden gleichermaßen gelten, ist es wegen der Rolle der EU-Institutionen als Teil der öffentlichen Verwaltung erforderlich, die vorgesehenen Rollen und Kontrollen zu überprüfen. In der Regel wird Ihre EU-Institution die meiste Kontrolle haben, wenn es sich um ein Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter handelt, bei dem Ihre EU-Institution der Verantwortliche ist. Zur Vermeidung von Unklarheit darüber, wer für die Datenverarbeitungstätigkeit verantwortlich ist, ist darauf zu achten, dass die Rollen und Zuständigkeiten des Verantwortlichen und des Auftragsverarbeiters klar angegeben werden. **Sie müssen auch sicherstellen, dass Ihre Verträge, die der Verantwortliche mit dem Auftragsverarbeiter schließt, alle gemäß Artikel 29 Absatz 3 der Verordnung vorgeschriebenen Vertragsbedingungen enthalten**, z. B., dass Ihnen alle erforderlichen Angaben über die in der Datenverarbeitungsvereinbarung vorgesehenen Unterauftragsverarbeiter vorliegen.

Nähere Informationen entnehmen Sie bitte Artikel 29 der Verordnung sowie Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725.

2.4 Datenverarbeitung in der EU / im EWR und Datenübermittlungen

Wenn Sie sich auf einen externen Anbieter stützen müssen, sollten Sie zunächst prüfen, ob es einen Anbieter mit Sitz in der EU bzw. im EWR gibt, der Ihre Anforderungen erfüllt, und darauf achten, dass Ihre Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter den oben in Abschnitt 2.3 genannten Anforderungen genügt.

Auch wenn Sie Anbieter mit Sitz in der EU / im EWR nutzen, müssen Sie überprüfen, ob deren Dienstleistungen möglicherweise die Übermittlung personenbezogener Daten in Länder außerhalb der EU / des EWR umfassen, etwa für Zwecke wie die Anfertigung von Sicherungskopien (Back-ups), Fehlersuche und -behebung (Troubleshooting) / Kundendienst usw. Sollte dies der Fall sein, ist darauf zu achten, dass Ihr Anbieter angemessene Schutzvorkehrungen hat, die den in Kapitel V der Verordnung genannten Anforderungen genügen, zum Beispiel genehmigte verbindliche interne Datenschutzvorschriften.

Sollte Ihr externer Anbieter keinen Sitz in der EU / im EWR haben und auch nicht dem Anwendungsbereich eines Angemessenheitsbeschlusses der Europäischen Kommission unterliegen, müssen Sie **geeignete Garantien** im Sinne von Artikel 48 der Verordnung einholen.

Nähere Information dazu sind den vom Europäischen Datenschutzbeauftragten herausgegebenen Informationen über internationale Datenübermittlungen nach dem Brexit (EDPS Information Note on international data transfers after Brexit) zu entnehmen, die einen Überblick über die verschiedenen Übermittlungsinstrumente geben, die den EU-Institutionen über diesen spezifischen Kontext hinaus zur Verfügung stehen.

2.5 Funktionalitäten für die Überwachung durch Arbeitgeber oder Provider

Tools für die Remote-Zusammenarbeit und Videokonferenzen sehen häufig mehr Möglichkeiten zur Überwachung der Mitarbeiter vor, als dies bei der „Offline"-Zusammenarbeit der Fall ist. Grundsätzlich sollte es **keine Überwachung durch Arbeitgeber oder Provider** geben.

Hinsichtlich der **Überwachung durch den Provider ist die Beschreibung der von ihm zu erbringenden Dienstleistungen daraufhin zu prüfen, dass diese keinerlei Überwachung vorsehen; erforderlichenfalls sind zusätzliche vertragliche Schutzmaßnahmen zu vereinbaren**.

Hinsichtlich der **Überwachung durch den Arbeitgeber sind die Tools auf eine Weise zu konfigurieren, die jede derartige Datenerhebung vermeidet, und dies ist den Mitarbeitern in transparenter Weise offenzulegen**. Sollte eine wie auch immer geartete Überwachung durch den Arbeitgeber erforderlich sein, müssen Sie angeben, inwiefern derartig eingreifende Maßnahmen in angemessenem Verhältnis zu dem zu erreichenden Ziel stehen. Diesbezüglich können Sie die Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit nachlesen und Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen anwenden, um Ihr Ziel auf eine Weise zu erreichen, die das Recht Ihrer Mitarbeiter auf den Schutz ihrer Privatsphäre wahrt. Darüber hinaus ist zu bedenken, dass Ihre Mitarbeiter zu Hause arbeiten, zuweilen mit ihrem Privatgerät. Eingriffe in die eigene Wohnung der Mitarbeiter und ihre eigene digitale Privatsphäre sind nicht zulässig. Auch wenn es in den Leitlinien zur Videoüberwachung (Video-Surveillance Guidelines) vorwiegend um die Videoüberwachung geht, enthalten die Abschnitte über die Mitarbeiterüberwachung (Seite 20), die Bereiche mit erhöhten Erwartungen an den Privatsphärenschutz (Seite 21) und die verdeckte Überwachung (Seite 23) unter Umständen allgemeine, auch für die Mitarbeiterüberwachung im Rahmen der Telearbeit nützliche Leitlinien.

Noch ein letzter praxisrelevanter Punkt: Videokonferenz-Tools sollten die Möglichkeit bieten, das Meeting aufzuzeichnen. Dabei gilt **für Aufzeichnungen dieselbe Vorgehensweise wie bei**

persönlichen Treffen: In der Regel wird dazu die Einwilligung der Personen, die aufgezeichnet werden sollen, einzuholen sein.

2.6 Datenspeicherung

Egal ob neue Tools intern oder von externen Anbietern geliefert werden, ist darauf zu achten, dass sie jeweils mit **angemessenen Speicherungsfristen** konfiguriert werden, die mit dem Zweck der Datenverarbeitungstätigkeit in Einklang stehen. Von **externen Anbietern ist eine klare und verbindliche Verpflichtung einzuholen, dass die Informationen Ihrer EU-Institution bei Vertragsbeendigung entweder an Sie zurückgegeben oder gelöscht werden** (siehe dazu auch den obigen Abschnitt „Verantwortlicher / Auftragsverarbeiter“; dies ist gemäß Artikel 29 Absatz 3 Buchstabe g der Verordnung eine zwingende Anforderung, die Sie Ihren Auftragsverarbeitern auferlegen müssen).

2.7 Datensicherheit

Wenn Tools für die Telearbeit neu eingeführt werden oder ihr Gebrauch ausgeweitet wird, können sich zusätzliche Datensicherheitsprobleme ergeben.

Ihre IT-Abteilung muss dann in Zusammenarbeit mit dem Beauftragten für die lokale IT-Sicherheit (LISO) die erforderlichen Maßnahmen ergreifen, um die Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitung personenbezogener Daten zu schützen, die über die verschiedenen elektronischen Kommunikationsmittel erfolgt: Instant-Messaging-Plattformen, Tools für die Online-Zusammenarbeit, Webmail, Videokonferenz-Tools usw. **Sicherheit setzt voraus, dass die IT-Abteilungen, der LISO, der DSB und alle Nutzer zusammenarbeiten.**

Wegen der COVID-19-Situation haben die Telearbeit und die Beanspruchung der externen Verbindungen des Unternehmensnetzes stark zugenommen, was zu **Abweichungen von den Standardprozessen** führen könnte, möglicherweise auch dazu, dass der Zugriff auf automatisierte Tools bei der Telearbeit nicht möglich ist und sich dadurch die **Gefahr von Datenschutzverletzungen durch menschliche Fehler erhöht**. An den Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten ändert dies nichts. Die Leitlinien des EDSB zur Meldung von Verletzungen des Schutzes personenbezogener Daten enthalten diesbezüglich praktischen Rat.

Sie müssen die zu befolgenden alternativen Prozesse festlegen und dokumentieren und dafür sorgen, dass alle Ihre Mitarbeiter einen klaren Kommunikationsweg zum LISO haben. **Klären Sie die Mitarbeiter darüber auf, auf welche Weise es häufig zu Datenschutzverletzungen kommt, z. B. durch Spoofing, Phishing und Social-Engineering-Angriffe mit COVID-19 betreffenden Mitteilungen**. Es gibt auch etliche Berichte über Angriffe auf Tools für Online-Konferenzen, bei denen sich Hacker unbefugt in Gespräche eingeschlichen und Phishing-E-Mails verschickt haben, um sich Anmeldedaten zu verschaffen.

Auch bei neuen Tools gelten die allgemeinen Anforderungen an die Datensicherheit, die sich aus Artikel 33 der Verordnung ergeben, sowie die sonstigen mit der Informationssicherheit verbundenen Verpflichtungen. So sollten zum Beispiel nach einem risikobasierten Ansatz auf bewährten Verfahren beruhende kryptografische Technologien eingesetzt werden, um die Ende-zu-Ende-Verschlüsselung (im Gegensatz zur Punkt-zu-Punkt-Verschlüsselung), die Authentizität des Senders und die Informationsintegrität sicherzustellen.

Bei neuen Verträgen und bei Dienstgütevereinbarungen mit externen Providern, die IT-Dienstleistungen anbieten, ist zu prüfen, dass genügend Sicherheitsmaßnahmen implementiert werden.

Dies wäre auch eine Gelegenheit, zu überprüfen, ob die bestehenden Tools all diese Anforderungen erfüllen, sowie die jeweils geltenden Grundsätze (wie etwa die Sicherheitsgrundsätze) zu aktualisieren.

Auch die Leitlinien des EDSB zur Nutzung von Cloud-Computing-Diensten durch die Organe und Einrichtungen der Union sind hier nach wie vor relevant. Die Leitlinien des Europäischen Datenschutzbeauftragten zu mobilen Apps (EDPS Guidelines on mobile apps) könnten ebenfalls nützlich sein. Obgleich die Leitlinien für EU-Institutionen gedacht sind, die eigene Apps entwickeln, sind die dort behandelten Fragen doch auch Fragen, die Sie den Anbietern der Apps, die Ihre EU-Institution möglicherweise zu nutzen beabsichtigt, stellen sollten.

3. Probleme in Bezug auf Gesundheitsdaten

3.1 Die Rolle medizinischer Dienste.

Grundsätzlich ist es allein qualifiziertem Medizinpersonal vorbehalten, auf Gesundheitsdaten zuzugreifen und sie zu verarbeiten.

Ihr medizinischer Dienst wird Ihnen sicherlich über die intern getroffenen Präventivmaßnahmen Auskunft geben können. Mitarbeiter, bei denen Verdacht auf eine COVID-19-Infektion besteht, müssen in angemessenem Umfang mit ihrem eigenen Arzt, den für die öffentliche Gesundheit zuständigen Behörden im betreffenden Land sowie mit dem medizinischen Dienst ihrer EU-Institution kooperieren.

Für die Verfolgung der Entwicklung des Krankheitsfalls ist vornehmlich der behandelnde Arzt zuständig. Jedoch wird, wie in jedem Fall krankheitsbedingter Fehlzeiten, auch der medizinische Dienst Ihrer EU-Institution eingeschaltet werden, soweit dies erforderlich und notwendig ist.

Die EU-Institutionen müssen allerdings auf den Schutz der medizinischen Daten ihrer Mitarbeiter sowie die Einhaltung der in Artikel 10 der Verordnung niedergelegten Anforderungen an die Verarbeitung von Gesundheitsdaten achten. Wegen der hohen Infektionsrate bei COVID-19 und den Sorgfaltspflichten der EU-Institutionen gegenüber ihren Mitarbeitern können die EU-Institutionen bei Verdachtsfällen oder bestätigten Fällen jedoch zusätzliche Folgemaßnahmen vorsehen.

Dasselbe gilt, wenn eine andere EU-Institution aufgrund einer Dienstgütevereinbarung oder auf ähnlicher Grundlage medizinische Dienste für Sie erbringt. Es kann sinnvoll sein, den medizinischen Dienst, der diese Dienste für Ihre EU-Institution erbringt, daran zu erinnern.

In seinem Aufruf vom 6. April 2020 hat der Europäische Datenschutzbeauftragte bereits darauf hingewiesen, dass die Krise unter Umständen zeitlich begrenzte Maßnahmen erfordert und dass deshalb jede Speicherung von Daten im Zusammenhang mit dieser Krise zeitlich begrenzt sein sollte. Es ist bewährte Praxis, diese Frage bereits frühzeitig zu behandeln und zu beschließen, dass derartige Daten gelöscht werden, sobald in der Krise ein bestimmter Meilenstein der öffentlichen Gesundheit erreicht wird.

3.2 Expositionsmeldung und Kontaktverfolgung

Die Kontaktverfolgung ist eines der Instrumente, das den Gesundheitsbehörden zur Bekämpfung von Infektionskrankheiten zur Verfügung steht.

Wie bereits in früheren Leitlinien erklärt wurde[1], **dürfen die EU-Institutionen, falls sich die zuständigen Gesundheitsbehörden im Zuge ihrer Kontaktverfolgung auf nationaler Ebene an die EU-Institutionen wenden, relevante Informationen offenlegen** (z. B. welche Personen bei einem Treffen anwesend waren, Büroräume teilen usw.), wobei jedoch die Vertraulichkeit der medizinischen Daten, wie in Abschnitt 3.1 ausgeführt, zu wahren ist. Was geschieht, wenn die Daten den zuständigen nationalen Gesundheitsbehörden offengelegt werden? Die nationalen Behörden müssen die Daten nach den für sie geltenden Gesetzen verarbeiten.

In manchen Mitgliedstaaten der EU ist COVID-19 eine meldepflichtige Ansteckungskrankheit, die der Arzt, der die Diagnose stellt, dem Gesundheitsamt melden muss (unter Angabe des Namens der betreffenden Person, die dann zwecks Kontaktverfolgung vom Gesundheitsamt kontaktiert wird). Mitteilung der Identität der in einem bestätigten Fall betroffenen Personen die Kollegen: Bei der Kontaktverfolgung nach „alter Schule“ sind die Gesundheitsbehörden sehr darauf bedacht, diese Information nicht preiszugeben.

In diesem Fall gelten für die weitere Datenverarbeitung die DSGVO und die Gesetze, durch die diese Aufgaben den zuständigen nationalen Behörden übertragen werden. Hier handeln die zuständigen Behörden als von den EU-Institutionen separate Verantwortliche. Die Speicherungsfristen, Rechte der betroffenen Person usw. richten sich nach den von den zuständigen Behörden beschlossenen Verfahren. Die Einhaltung der DSGVO unterliegt der Aufsicht durch die zuständige nationale Datenschutzbehörde.

3.3 Soziale und private Belange

In bestätigten Fällen darf die EU-Institution die Identität nicht allgemein den Mitarbeitern mitteilen. Wenn jedoch ein Mitarbeiter seinen eigenen Gesundheitszustand freiwillig Kollegen mitteilt, stehen die Datenschutzvorschriften **etwaigen von den Kollegen organisierten Aktionen, etwa der Übersendung von Blumengrüßen oder Karten mit Genesungswünschen, nicht entgegen**.

4. Rechte der betroffenen Person

Die Coronavirus-Krise **bewirkt keine Aussetzung der Rechte betroffener Personen, so dass diese berechtigt bleiben, von ihren Rechten Gebrauch zu machen**, sofern nicht spezifische, ordnungsgemäß erlassene und dokumentierte Beschränkungen im Sinne von Artikel 25 der Verordnung Anwendung finden.

Sie müssen sicherstellen, dass Sie Fernzugriff auf die Informationssysteme für Auskunftsersuchen haben. Sollte es dennoch so sein, dass Ihre EU-Institution die Auskunftsersuchen nicht zeitnah beantworten kann, sind die Gründe dafür und für die getroffene Entscheidung zu dokumentieren, wobei den betroffenen Personen vor Ablauf der gesetzlichen Frist mitzuteilen ist, dass sich die Beantwortung Ihres Ersuchens verzögern wird, was der Grund dafür ist und wie lange die Verzögerung voraussichtlich dauern wird.

5. Unterstützung von EU-Institutionen durch den Europäischen

[1] Mitteilung an alle Datenschutzbeauftragten der EU-Institutionen vom 12. März 2020.

Datenschutzbeauftragten

Auch in der Krise ist es unbedingt erforderlich, die in der Verordnung niedergelegten Anforderungen zu erfüllen. So müssen Sie bitte darauf achten, Ihr Register der Verarbeitungsvorgänge regelmäßig zu aktualisieren und alle erforderlichen Datenschutz-Folgenabschätzungen durchzuführen. Zur Einhaltung des Grundsatzes der Rechenschaftspflicht muss es schriftliche Nachweise für die in Bezug auf Datenschutzfragen getroffene Entscheidungen geben.

Der Europäische Datenschutzbeauftragte ist sich bewusst, dass dies für alle EU-Institutionen schwere Zeiten sind. Wie bereits gesagt und in diesem Dokument anschaulich dargestellt wurde, findet die Verordnung Anwendung, wobei sie jedoch flexibel genug ist, sich den derzeitigen Bedingungen anpassen zu lassen.

Wenn die Krise abklingt (oder aber in Reaktion auf eingehende Beschwerden), kann es sein, dass der Europäische Datenschutzbeauftragte die in der Krise getroffenen Datenschutzmaßnahmen Ihrer Institution überprüft.

Wir stehen Ihnen weiterhin mit Hilfe und informellem oder förmlichem Rat zu allen diese Krise betreffenden Fragen zur Seite.