SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Datenschutz und Corona-Pandemie

Die Auswirkungen der Corona-Pandemie und der dagegen getroffenen Maßnahmen auf die verschiedensten Lebensbereiche führten zu einer Vielzahl von Fragestellungen, die die Datenschutzaufsichtsbehörden des Bundes und der Länder erreichten. Den Medien ließen sich Schlagzeilen entnehmen, die Infektionsschutz statt Datenschutz fordern. Gerade in Krisen bleibt aber die Beachtung geltenden Rechts notwendig. Es ist grundrechtlich geboten, den Schutz der Gesundheit mit dem Schutz der Persönlichkeit Betroffener in Einklang zu bringen. Die hierfür notwendigen gesetzlichen Grundlagen sind gegeben, um im Rahmen der Erforderlichkeit und Verhältnismäßigkeit einen sachgerechten Infektionsschutz zu gewährleisten (DS-GVO, BDSG, DSAG LSA und die jeweiligen Fachgesetze, wie u. a. das IfSG). Dem Infektionsschutz steht der Datenschutz also nicht entgegen.

Beispielsweise können die zuständigen Behörden auf der Basis von Art. 6 Abs. 1 lit. c), Art. 9 Abs. 2 lit. i) DS-GVO, IfSG i. V. m. § 4 DSAG LSA die notwendigen Maßnahmen treffen und die dafür erforderlichen Daten verarbeiten. Erkrankte Personen, Ärzte oder Leiter von Einrichtungen (u. a. Schulen, Kindertageseinrichtungen, Justizvollzugsanstalten) können Meldepflichten nach dem IfSG unterliegen (Grundlage: Art. 6 Abs. 1 lit. c) DS-GVO). Soweit die gesetzlichen Grundlagen nicht tragfähig sind, z. B. weil die strengen Anforderungen der Erforderlichkeit nicht erfüllt sind, kommt eine Einwilligung der jeweils Betroffenen in Betracht. Dabei wären insbesondere die Anforderungen an die Freiwilligkeit zu beachten (siehe dazu das Kurzpapier Nr. 20 „Einwilligungen nach der DS-GVO“ der Datenschutzkonferenz, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf).

Gesundheitsdaten als besonders sensible Daten sind nach Art. 9 DS-GVO besonders geschützt und nur unter einschränkenden Bedingungen zu verarbeiten. Unter Berücksichtigung der Vorgaben der jeweiligen gesetzlichen Regelungen ist die Verarbeitung aber u. a. zum Schutz lebenswichtiger Interessen, zur Gesundheitsvorsorge, zur Versorgung und Behandlung und insbesondere aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit möglich (s. Art. 9 Abs. 2 DS-GVO). Dabei sind die europarechtlich vorgegebenen Grundsätze, u. a. der Datenminimierung, der Zweckbindung und der Erforderlichkeit und Verhältnismäßigkeit maßgeblich. Es ist stets das mildeste Mittel zu suchen. Auch die Vertraulichkeit ist zu beachten. Maßstab ist also nicht der subjektive Bedarf, sondern die objektive Unerlässlichkeit. Auch darf im Zuge der Normalisierung nicht vergessen werden, nicht mehr für Pandemiemaßnahmen notwendige Daten wie geboten sicher zu löschen.

Nach dem Vorgenannten bestanden keine Bedenken, andere Personen wie Gesprächspartner oder Gäste zu fragen, ob bei Ihnen eine Infektion mit COVID-19 festgestellt wurde oder ob sie mit einer solchen Person Kontakt hatten. Dies gilt auch für die Frage, ob die Person kürzlich aus einem vom Robert-Koch-Institut als Risikogebiet eingestuften Gebiet zurückgekehrt ist.

Fragwürdig erschien dagegen die Zulässigkeit rein vorsorglicher Erhebung von Daten, wie beispielsweise die Sammlung von Kontaktdaten. Hierzu wäre die Einwilligung der Betroffenen geboten. Besondere Zurückhaltung ist bei der Offenlegung von nachgewiesenen Infektionen oder eines konkreten Infektionsverdachts geboten. Dies kann nur auf konkreter Grundlage zum nicht anders erreichbaren Schutz von Dritten erforderlich werden, der die Schutzinteressen des betroffenen Infizierten überwiegt.

Weiterführende Hinweise:

Die Berücksichtigung der Grundsätze der Datenschutz-Grundverordnung wie u. a. Verhältnismäßigkeit und Transparenz bei der Umsetzung von Maßnahmen nach den gesetzlichen Regelungen der Mitgliedstaaten betont die „Erklärung zur Verarbeitung personenbezogener Daten im Zusammenhang mit COVID-19“ des Europäischen Datenschutzausschusses (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_art_23gdpr_20200602_de_1.pdf).

Die Datenschutzaufsichtsbehörden des Bundes und der Länder hatten in unterschiedlichem Umfang Informationen zur Thematik der Corona-Pandemie auf den Homepages veröffentlicht. Eine frühe umfassende Darstellung mit häufigen Fragestellungen aus verschiedenen Bereichen fand sich u. a. beim Hamburger Beauftragten für Datenschutz und Informationsfreiheit (https://datenschutz-hamburg.de/assets/pdf/Corona-FAQ.pdf).

Corona im Beschäftigungsverhältnis

Die öffentlichen Arbeitgeber in Sachsen-Anhalt können auf der Grundlage von Art. 6 Abs. 1 lit. e), Art. 88 DS-GVO, § 50 BeamtStG und § 84ff LBG LSA, § 26 DSAG LSA die erforderlichen Daten verarbeiten. Nicht-öffentlichen Arbeitgeber stehen die Rechtsgrundlagen des § 26 BDSG und des Art. 6 Abs. 1 lit. f) DS-GVO zur Verfügung. Dies schließt Fragen ein, die im Rahmen der Fürsorgepflicht gegenüber anderen Beschäftigten geboten sind, soweit sie verhältnismäßig sind (z. B. bezüglich festgestellter Infektionen oder Infektionsverdacht). Infolge der Nebenpflichten der Beschäftigten aus dem Dienst- bzw. Arbeitsverhältnis, den Dienstherrn bzw. Arbeitgeber über eine eigene Erkrankung oder den Kontakt mit einem Erkrankten zu informieren, erscheinen weitergehende Maßnahmen wie Fiebermessen eher unverhältnismäßig. Bei konkretem Verdacht besteht jedoch ggf. die Möglichkeit, amtsärztliche Untersuchungen zu veranlassen. Erfährt der Arbeitgeber, dass ein Mitarbeiter erkrankt ist, müssen die Reaktionen wiederum verhältnismäßig sein. Eine Offenbarung an andere Beschäftigte sollte soweit möglich ohne Personenbezug erfolgen (Hinweis auf die Tatsache des Kontakts mit einem Infizierten).

Weitergehende Informationen zur Verarbeitung im Beschäftigtenbereich finden sich u. a. Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (FAQ-Corona https://www.baden-wuerttemberg.datenschutz.de/faq-corona/).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat zu den vielfältigen Fragestellungen, die die Corona-Pandemie und die Bekämpfungsmaßnahmen nach der jeweils aktuellen Rechtslage in Beschäftigungsverhältnissen aufwarfen, im Dezember 2021 eine umfängliche Anwendungshilfe für die Praxis erstellt („Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie“, https://datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf).

Heimarbeit

Öffentliche Stellen und Unternehmen gestatteten ihren Beschäftigten im Zusammenhang mit der Corona-Pandemie kurzfristig, ihre Aufgaben weitreichend in Heimarbeit durchzuführen. Datenschutzrechtlichen Anforderungen muss auch bei Heimarbeit Rechnung getragen werden. Insbesondere müssen die Vertraulichkeit und die Verfügbarkeit der Daten gewährleistet sein.

Es ist grundsätzlich nicht empfehlenswert, die Verarbeitung personenbezogener Daten auf privaten Geräten bei der Arbeit im Homeoffice zu erlauben. Dienstliche bzw. betriebliche Geräte sind vorteilhafter, da sie entsprechend konfiguriert werden können. Die Geräte müssen sicher mit dem Netzwerk des Unternehmens oder der öffentlichen Stelle verbunden sein. Auch zu Hause sind diverse Sicherheitsmaßnahmen notwendig (z. B. Bildschirmschoner, Verschluss von Geräten und Unterlagen).

Die Empfehlungen des Landesbeauftragten für kleine und mittlere Unternehmen zur Verarbeitung personenbezogener Daten in Heimarbeit enthalten Erläuterungen insbesondere zu technischen und organisatorischen Vorgaben (https://lsaurl.de/kmuheimarbeit). Im Juli 2021 hat der Landesbeauftrage umfängliche „Hinweise zum Homeoffice in Behörden und Betrieben“ veröffentlicht. Vielfältige datenschutzrechtliche Fragestellungen in Bezug auf die Vorbereitung, die notwendigen Vorgaben, die technische Einrichtung und Ausgestaltung sowie die Sicherheit beim Transport und im häuslichen Bereich werden aufgegriffen. Dies findet sich nebst einer Checkliste im Infopaket Homeoffice (https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-homeoffice).

Schulen

Infolge des Unterrichtsausfalls erhöhten sich die Anfragen beim Landesbeauftragten nach der Nutzung digitaler Methoden zur Unterrichtung und zur Kommunikation (u. a. zu Lernplattformen, Cloud-Produkten, Messenger-Diensten, Videodiensten). Wird Technik eingesetzt, ist stets zu beachten, dass sie den Sicherheitsanforderungen des Art. 32 DS-GVO entsprechen muss. In diesem Rahmen ist insbesondere auf die Ende-zu-Ende-Verschlüsselung zu achten.

Aus datenschutzrechtlicher Sicht werden für die Kommunikation dienstliche E-Mail-Adressen bevorzugt. Soweit Cloud-Dienste nötig sind, sollten die Angebote von öffentlichen Stellen bevorzugt werden.

Hierzu ist insbesondere auf das Angebot des Bildungsservers Sachsen-Anhalt des Landesinstituts für Schulqualität und Lehrerbildung Sachsen-Anhalt hinzuweisen (https://www.bildung-lsa.de/). Das Verteilen und Einsammeln von Hausaufgaben ist beispielsweise mit der emuCLOUD (Schulcloud für Sachsen-Anhalt) möglich. Über die Lernplattform Moodle können verschiedene Unterrichtsangebote gemacht werden. Auch ist die Einrichtung einer dienstlichen E-Mail-Adresse möglich.

Zu datenschutzrechtlichen Fragestellungen im Zusammenhang mit Lernplattformen ergeben sich umfängliche Hinweise aus der Orientierungshilfe zu Online-Lernplattformen im Schulunterricht (https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/orientierungshilfen/Orientierungshilfe_fuer_Online-Lernplattformen_im_Schulunterricht.pdf).

Soweit Angebote aus dem nicht-öffentlichen Bereich genutzt werden, ist eine entsprechende vertragliche Ausgestaltung notwendig (Auftragsverarbeitung nach Art. 28 DS-GVO, eine Formulierungshilfe finden Sie hier: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Hinweise/auftrags_dv/Muster_fuer_Auftragsverarbeitungsvertrag_nach_DS-GVO.pdf).

Insbesondere sollte darauf geachtet werden, dass personenbezogene Daten von Schülerinnen und Schülern nur dort gespeichert werden, wo ein von der Datenschutz-Grundverordnung gebotenes Datenschutzniveau gegeben ist. Dies ist bei Anbietern außerhalb der Europäischen Union bzw. dem europäischen Wirtschaftsraum häufig nicht gegeben.

Auch in Bezug auf Videokonferenzen sind die Datenschutzgrundsätze und die technischen und organisatorischen Anforderungen des Art. 32 DS-GVO zu beachten (Zweckbindung, Verschlüsselung). Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat hierzu die „Orientierungshilfe Videokonferenzsysteme“ veröffentlicht. Sie findet sich neben weiteren Hinweisen und einer Checkliste im Infopaket Videokonferenzen auf der Homepage (https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-videokonferenzen).

Die Nutzung von Messenger-Diensten begegnet ebenfalls datenschutzrechtlichen Bedenken. Eine mit der Nutzung derartiger Dienste ggf. verbundene Offenbarung von personenbezogenen schulrelevanten Daten an Unbefugte ist grundsätzlich unzulässig. Die Anforderungen an die datenschutzkonforme Ausgestaltung sind sehr hoch (vgl. dazu das Whitepaper der Datenschutzkonferenz „Technische

Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“,
https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf).
Die Umsetzung dürfte mit den an Schulen vorhandenen Mitteln nur schwer möglich sein.

Weiter muss bei dem Einsatz von digitalen Methoden an den oftmals gegebenen Bedarf des Einsatzes privater Geräte gedacht werden. Die Einbeziehung von privaten Geräten der Schülerinnen und Schüler begegnet schon deshalb Bedenken, da die Schulleitung keinen Einfluss auf die Absicherung der Geräte hat. Zudem dürfte die Inanspruchnahme der Geräte nur auf Basis der Einwilligung möglich sein. Die gebotene Freiwilligkeit kann aber fraglich sein, wenn eine Teilnahme am Unterrichtsgeschehen anders nicht mehr möglich ist. Die Nutzung privater Geräte der Lehrerschaft ist ohnehin nur sehr eingeschränkt möglich (siehe § 84a Abs. 7 SchulG LSA). Weitere Hinweise finden sich in der Handreichung „Datenschutz an Schulen“ des Ministeriums für Bildung, die den Schulleitungen über den Bildungsserver zur Verfügung steht.

Auch wenn ausnahmsweise ein coronabedingter Einsatz von privaten Geräten und Messenger- bzw. Videodiensten für vertretbar gehalten wird, ist insgesamt Zurückhaltung geboten. Insbesondere sind die Daten nach einer Normalisierung in herkömmliche Systeme zu überführen und der technische Notbetrieb einzustellen.

Impressum
Herausgeber:
Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Leiterstr. 9
39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
https://datenschutz.sachsen-anhalt.de

Stand: April 2020, zul. geänd. Januar 2023