Datenschutz newsbox

Ausgabe 4 2019

DATAKONTEXT

Editorial

Am 10.04.2019 hat der Europäische Datenschutzausschuss seine „Leitlinien zur Verarbeitung personenbezogener Daten auf Grundlage des Art. 6 Abs. 1 b DS-GVO im Kontext von Online-Dienstleistungen“ ausformuliert.

Art. 6 Abs. 1 b DS-GVO legitimiert die Verarbeitung personenbezogener Daten, soweit sie zur Vertragserfüllung erforderlich ist. Die neu formulierten Leitlinien konkretisieren und schränken diesen Grundsatz insoweit ein, dass es zur Beurteilung dessen, ob eine Datenverarbeitung zur Vertragserfüllung erforderlich ist, nicht allein darauf ankommt, was im Vertrag vereinbart wurde. Unter Berücksichtigung der in Art. 5 DS-GVO niedergelegten Datenschutzgrundsätze wie Sparsamkeit, Fairness und Transparenz ist nach den Vorgaben des Europäischen Datenschutzausschusses eine Bewertung vorzunehmen, ob Unternehmen die Verarbeitung von Daten der Nutzerinnen und Nutzer auf die Rechtsgrundlage „Vertragserfüllung“ stützen können.

Beispielsweise kann eine Datenverarbeitung für Zwecke der personenbezogenen Onlinewerbung danach grundsätzlich nicht auf die Rechtsgrundlage „Vertragserfüllung“ gestützt werden. Interessierte Stellen werden die Möglichkeit erhalten, das Papier im Rahmen einer öffentlichen Konsultation kommentieren zu können.

Ob die Erforderlichkeit tatsächlich schon dann bejaht werden kann, wenn diese im Rahmen einer Klausel vereinbart wurde oder ob die Erforderlichkeit nicht erst dann angenommen werden kann, wenn die Verarbeitung für die Erfüllung eines Vertrages oder für die Vertragsanbahnung objektiv als erforderlich betrachtet werden muss, ist eine praxisrelevante Frage. Ob das Papier am Ende in dieser Hinsicht mehr Rechtssicherheit bringen wird, bleibt abzuwarten. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Ulrich Kelber*, begrüßt die Annahme der Leitlinien ausdrücklich.

Das Papier kann in den nächsten Wochen von interessierten Stellen im Rahmen einer öffentlichen Konsultation kommentiert werden.

Ihr Levent Ferik

DATAKONTEXT

Impressum

DATAKONTEXT GmbH
Augustinusstraße 9d
50226 Frechen

Tel.: 02234/98 94 9-30
Fax: 02234/98 94 9-32
fachverlag@datakontext.com
www.datakontext.com

Geschäftsführer:
Dr. Karl Ulrich/Hans-Günter Böse
Handelsregister
Amtsgericht Köln HRB 82299

Künstliche Intelligenz und Beschäftigtendatenschutz

Eine effektive Regelungsfähigkeit des Einsatzes der KI im Beschäftigungsverhältnis setzt deutlich erkennbare Anwendungsszenarien und damit einhergehende tatsächliche Veränderungen für die Arbeitswelt voraus, um hierfür regulierende Rahmenbedingen zu setzen.

I. Auswirkungen der KI auf Beschäftigungsverhältnisse

Da Anwendungen mit KI in alle Lebensbereiche eingreifen können und auch immer mehr menschliches Verhalten in immer breiteren Handlungsfeldern automatisieren und ersetzen sollen, wird sich auch die Arbeitswelt durch die KI verändern. KI-gesteuerte Systeme sind für ihr Funktionieren auf große Datenmengen angewiesen. „Die konkrete Funktionsweise ist zudem in besonderer Weise abhängig von der Auswahl und der Qualität der jeweils eingegebenen und/oder für die Entwicklung („Training") genutzten Daten."
Sowohl Quantität als auch Qualität der Daten sind in der Konsequenz der Motor und der Kraftstoff für KI-Anwendungen. Im Beschäftigungsverhältnis muss somit der Beschäftigte selbst zum Datenlieferenten werden, damit die Technologie einen effektiven Nutzen entfalten kann. Ohne eine entsprechende Datengrundlage funktionieren die KI-Anwendung zugrundliegenden Algorithmen nicht.
Mittels „trial and error" wird der Beschäftigte als betroffene Person zum Datensubjekt, bei dem so lange zulässige Lösungsmöglichkeiten versucht werden, bis die gewünschte Lösung gefunden wurde. Die dabei beim Beschäftigten erhobenen Daten können den Algorithmen etwa zum Targeting oder zur Erkennung von Mustern oder strukturellen Prozessen dienen.

II. Rechtlicher Rahmen

Unter den regulatorischen Rahmen des Datenschutzrechts fallen auch die für KI-Systeme erforderlichen Daten von Beschäftigten und ihre Verarbeitung.

III. Entwicklung von KI bzw. Algorithmen

Eine Software mit KI muss mit riesigen Datenmengen versehen werden und daraus Muster erkennen. Zu vernachlässigen ist aber nicht, wie die Muster zustande kommen. In einem zweiten Schritt werden dafür von der programmierenden Person Regeln hinzugefügt. Man kann zum Beispiel festlegen, dass mehrjährige Beschäftigungspausen in einem Bewerbungsprozess nachteilig gewertet werden. Anschließend sucht die Software aus Millionen oder Milliarden Kombinationsmöglichkeiten die beste Lösung für ein Problem heraus. Die KI vermag frühzeitig zu erkennen, welche theoretischen Optionen effektiv wirken können und verwirft alle übrigen Optionen unverzüglich. Es wird deswegen stets Zeit in Anspruch nehmen, bis das Zusammenspiel so funktioniert, dass KI-Systeme Aufgaben übernehmen und mithin eigenständige Entscheidungen treffen können. Experten und Data Scientists müssen die Daten vorsortieren und die Software beherrschen. Die den KI-Anwendungen zugrundeliegenden Algorithmen arbeiten zwar mit statistischen Methoden, fallen aber nur unter die Ausnahme für statistische Zwecke, wenn sie im öffentlichen Interesse durchgeführt werden. Für die Auswertung großer, aus einer Vielzahl unterschiedlicher Quellen stammender unstrukturierter Daten zum Zwecke der Erkennung von Gesetzmäßigkeiten, Korrelationen und Kausalitäten und der Generierung neuer Informationen (Kontextwissen) wird regelmäßig auf Art. 6 Abs. 4 DS-GVO als Rechtsgrundlage verwiesen. Bei der Auswertung vorhandener Daten bzw. unter Hinzuspeichern weiterer Daten zu einem bereits existierenden Datensatz werden neue, spezifischere Informationen zu einer bereits zuvor individualisierten natürlichen Person generiert, weswegen bei solchen Szenarien der zwingend erforderliche Einsatz von wirksamen Pseudonymisierungstechniken durch umfassende Transparenz und Betroffenenrechte, insbesondere durch ein Widerspruchsrecht, geboten ist. Unter dem Vorhandensein geeigneter Garantien erscheint die Entwicklung von KI bzw. von entsprechenden Algorithmen auf Grundlage des Art. 6 Abs. 4 DS-GVO denkbar. Eine Weiterverarbeitung i.S.d. Art. 6 Abs. 4 DS-GVO unter anderem für wissenschaftliche Forschungs- oder für statistische Zwecke gilt überdies nicht als unvereinbar mit den ursprünglichen Zwecken.

Mehr auf DataAgenda

Widerruf der Einwilligung für Werbevideos

Frage des GDD-Erfa-Kreises Coburg

Unternehmen A möchte ein aufwendig produziertes (Werbe)-Video über sein Unternehmen drehen. Dabei sollen auch ausgesuchte Mitarbeiter auftreten. Nach DS-GVO müssen von den Mitarbeitern daher Einwilligungen eingeholt werden, die jederzeit widerrufen werden können. Was wäre die Rechtsfolgen, falls dies nach Fertigstellung des Videos passiert? Müssen die einzelnen Mitarbeiter dann entfernt / geschwärzt werden oder greift die frühere Rechtsfolge, dass in solchen Fällen Widerrufe nur ganz ausnahmsweise zulässig sind? Wäre es eine Alternative, in solchen Konstellationen anstatt Einwilligungen sog. Model-Release-Verträge abzuschließen? Regelmäßig erhalten die Mitarbeiter keine Gegenleistung, im Video aufzutreten, sie sind stolz darauf und eine Gegenleistung würde die nichtteilnehmenden Mitarbeiter benachteiligen.

Antwort des BayLDA:

Wenn man von den Mitarbeitern, die gefilmt werden, Einwilligungen einholt, muss diese Einwilligung grundsätzlich widerruflich sein. Widerruft ein Mitarbeiter die Einwilligung, muss er künftig auf dem Film unkenntlich gemacht bzw. entfernt werden.
Diese Schwierigkeit wird vermieden, wenn mit dem Beschäftigten tatsächlich ein Vertrag geschlossen wird, in dem geregelt wird, wo und wie der Film veröffentlicht wird. Dort können auch weitere Modalitäten geregelt werden, etwa auch, dass ein späteres Schwärzen/Entfernen des Mitarbeiters im bzw. aus dem Film grundsätzlich nicht in Betracht kommt.

Zugangssicherung von Online-Diensten

Der Arbeitskreis Technische und organisatorische Datenschutzfragen der Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder (DSK) hat eine Orientierungshilfe zu den Anforderungen erarbeitet, denen Anbieter von Online-Diensten zur Zugangssicherung nachkommen müssen. In der Regel verarbeiten Anbieter von Online-Diensten personenbezogene Daten von Nutzerinnen und Nutzern, sodass der Anwendungsbereich der DS-GVO für diese eröffnet ist.
Maßnahmen zur Sicherung des Zugangs zu den Diensten ergeben sich dabei bereits aus den Anforderungen des Art. 32 DS-GVO (Sicherheit der Verarbeitung). Die neu veröffentlichte Orientierungshilfe beschreibt Maßnahmen, die nach Ansicht der Datenschutzaufsichtsbehörden dem Stand der Technik entsprechen und einen effektiven Schutz gewährleisten können.
Die DSK empfiehlt Anbietern von Online-Diensten, sich bei der Auswahl der Maßnahmen an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik innerhalb des IT-Grundschutz-Kompendium an dem Abschnitt „Identitäts- und Berechtigungsmanagement“ zu orientieren (u. a. Basisanforderung ORP.4.A8 „Regelung des Passwortgebrauchs“ oder ORP.4.A11 „Zurücksetzen von Passwörtern“).

Quelle: Konferenz der unabhängigen Datenschutz-Aufsichtsbehörden des Bundes und der Länder

DSK fordert weitere Nachbesserung für Facebook-Fanpages

Mit Urteil vom 5. Juni 2018 hat der Gerichtshof der Europäischen Union (EuGH), Aktenzeichen C-201/16, entschieden, dass bei Facebook-Fanpages eine gemeinsame Verantwortlichkeit von Facebook-Fanpage-Betreiberinnen und Betreibern und Facebook besteht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in ihrer Entschließung vom 6. Juni 2018 deutlich gemacht, welche Konsequenzen sich aus dem Urteil für die gemeinsam Verantwortlichen – insbesondere für die Betreiberinnen und Betreiber einer Fanpage – ergeben. Bei einer gemeinsamen Verantwortlichkeit fordert die Datenschutz-Grundverordnung (DSGVO) unter anderem eine Vereinbarung zwischen den Beteiligten, die klarstellt, wie die Pflichten aus der DSGVO erfüllt werden.

Fanpage-Betreiberinnen und Betreiber müssen sich ihrer datenschutzrechtlichen Verantwortung stellen

Die DSK stellte fest, dass eine von Facebook noch im Juni 2018 angekündigte Vereinbarung nach Art. 26 DSGVO (Gemeinsam für die Verarbeitung Verantwortliche) bislang nicht zur Verfügung gestellt worden sei. Auch Fanpage-Betreiberinnen und Betreiber müssten sich ihrer datenschutzrechtlichen Verantwortung stellen. Ohne Vereinbarung nach Art. 26 DSGVO sei der Betrieb einer Fanpage, wie sie derzeit von Facebook angeboten werde, rechtswidrig.

Betroffene können ihre Rechte aus der DSGVO gegenüber jedem Verantwortlichen geltend machen

Daher forderte die DSK, dass nun die Anforderungen des Datenschutzrechts beim Betrieb von Facebook-Fanpages erfüllt werden. Dazu gehöre insbesondere, dass die gemeinsam Verantwortlichen Klarheit über die derzeitige Sachlage schaffen und die erforderlichen Informationen den betroffenen Personen (= Besucherinnen und Besucher der Fanpage) bereitstellten. Eine gemeinsame Verantwortlichkeit bedeute allerdings auch, dass Fanpage-Betreiberinnen und Betreiber (unabhängig davon, ob es sich um öffentliche oder nicht-öffentliche Verantwortliche handelt) die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und dies nachweisen können. Zudem könnten Betroffene ihre Rechte aus der DSGVO bei und gegenüber jedem Verantwortlichen geltend machen (Art. 26 Abs. 3 DS-GVO).

Kurz nach dem die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ihren Beschluss zu den sog. Facebook-Fanpages veröffentlicht hat, kam Facebook den dort postulierten Anforderungen teilweise nach.

Facebook reagiert

Nach der Veröffentlichung dieses Beschlusses hat Facebook ein Dokument mit dem den Titel „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ online gestellt. Obwohl Facebook nicht explizit darauf eingeht, ob diese Veröffentlichung als eine direkte Reaktion auf den Beschluss der DSK zu betrachten ist, ist nicht zu verkennen, dass Facebook mit diesem Dokument den Forderungen hinsichtlich einer Vereinbarung zur gemeinsamen Verantwortlichkeit nach der Art. 26 DSGVO entgegen kommt.
In seinem neuesten Positionspapier vom 01.04. 2019 fordert die DSK sowohl Facebook als auch die Fanpage-Betreiber auf ihrer Rechenschaftspflicht nachzukommen. Die Datenschutzkonferenz erwartet, dass Facebook entsprechend nachbessert und die Fanpage-Betreiber ihrer Verantwortlichkeit entsprechend gerecht werden. Solange diesen Pflichten nicht nachgekommen sei, ist ein
datenschutzkonformer Betrieb einer Fanpage nicht möglich.

Anforderungen werden bislang nicht erfüllt

Diese von Facebook veröffentliche „Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“ erfüllt nach Ansicht der DSK nicht die Anforderungen an eine Vereinbarung nach Art. 26 DS-GVO. Insbesondere stehe es im Widerspruch zur gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO, dass sich Facebook die alleinige Entscheidungsmacht „hinsichtlich der Verarbeitung von Insights-Daten“ einräumen lassen wolle. Die von Facebook veröffentlichten Informationen stellen zudem die Verarbeitungstätigkeiten, die im Zusammenhang mit Fanpages und insbesondere
Seiten-Insights durchgeführt werden und der gemeinsamen Verantwortlichkeit unterfallen, nicht hinreichend transparent und konkret dar, so die Aufsichtsbehörden. Sie seien nicht ausreichend, um den Fanpage-Betreibern die Prüfung der Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten der Besucherinnen und Besucher ihrer Fanpage zu ermöglichen.

Quelle: Datenschutz-Konferenz

Umsetzung der DS-GVO in Arztpraxen

Im Hinblick auf die Erfüllung der Informationspflichten in Arztpraxen hatte sich das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) bereits früh nach Geltung der DS-GVO geäußert. Darin beschreibt das ULD die Anforderungen, die die DS-GVO an die Betreiber oder die Betreiberin der Praxis, Apotheke etc. als den Verantwortlichen im Sinne des Gesetzes, stellt. Der Beitrag geht insbesondere auf folgende Themen ein:

- Rechtsgrundlagen für die Verarbeitung personenbezogener Daten der Patienten
- Informationspflichten: Die Betroffenen müssen über bestimmte Umstände bei der Verarbeitung ihrer Daten informiert werden (Art. 13 DS-GVO)
- Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Muss ein betrieblicher Datenschutzbeauftragter benannt werden?
- Muss eine Datenschutz-Folgenabschätzung durchgeführt werden?
- Weitere Pflichten

Auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit berichtet, dass die Zahl der Beratungsanfragen von Ärzten und Patienten erhebliche Unsicherheiten bei der Umsetzung der DS-GVO im Hinblick auf die Komplexität der maßgeblichen Regelungen zeigt. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat daher die fünf meist gestellten Fragen zum Datenschutz in Arztpraxen und Zahnarztpraxen ermittelt und eine Handreichung dazu veröffentlicht.
Diese folgenden fünf Fragen belegen die Spitzenplätze der von der Aufsichtsbehörde ermittelten FAQs:

1. Wie sind die Informationspflichten nach Art. 13 und 14 DS-GVO in der Arztpraxis umzusetzen?
2. Wann muss im Rahmen der ärztlichen Behandlung von Patienten eine Einwilligungserklärung eingeholt werden?
3. Darf die ärztliche Behandlung verweigert werden, wenn der Patient den Erhalt der Datenschutzinformationen nicht quittiert und/oder nicht in die Verarbeitung personenbezogener Daten einwilligt?
4. Ist die Übermittlung von Patientendaten (Befunden, Arztbriefen u. ä.) per E-Mail oder per Fax zulässig?
5. Wann muss eine Arztpraxis einen Datenschutzbeauftragten benennen?

Verpflichtende Benennung Datenschutzbeauftragter abseits der DS-GVO

Die GDD stellt einen Überblick zur Verfügung, welche Mitgliedstaaten in ihrem nationalen Umsetzungsgesetz eine verpflichtende Benennung Datenschutzbeauftragter abseits der Grundverordnung vorgesehen haben.

BELGIEN

Art. 21 Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel: Jede nicht-öffentliche Stelle, die eine Verarbeitung personenbezogener Daten zugunsten einer Bundesbehörde durchführt bzw. an diese von einer Bundesbehörde personenbezogene Daten übertragen wurden, muss einen Datenschutzbeauftragten bennen, falls die Verarbeitung der Daten wahrscheinlich zu einem hohen Risiko für Betroffene gem. Art. 35 DS-GVO führt.

Link zum Gesetz (EN)

DEUTSCHLAND

§ 38 Abs. 1 BDSG: In Fortführung von § 4f BDSG a.F. ist der Datenschutzbeauftragte bei nicht-öffentlichen Stellen verpflichtend zu benennen, wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Unabhängig von der Anzahl der mit der automatisierten Verarbeitung betrauten Personen ist die Benennung eines DSB auch dann zwingend erforderlich, wenn:

- Verarbeitungen vorgenommen werden, die einer Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO unterliegen, oder
- personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder der anonymen Übermittlung, oder
- für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Link zum Gesetz (DE)

SPANIEN

Art. 34 Ley Orgánica 3/2018: Verantwortliche oder Auftragsverarbeiter müssen in jedem Fall einen Datenschutzbeauftragten, wenn es sich um folgende Organisationen handelt:

- Kammern und Körperschaften einschließlich ihrer Generalräte
- Bildungseinrichtungen, die Bildung im Sinne aller in den Bildungsgesetzen angebotenen Niveaus anbieten, einschließlich der privaten und öffentlichen Universitäten
- Organisationen, die Netze betreiben und elektronische Kommunikationsdienste im Sinne der anwendbaren Gesetze anbieten, falls sie gelegentlich und systematisch personenbezogene Daten in großem Umfang verarbeiten
- Anbieter sozialer Netzwerke, falls sie in großem Umfang Profile der Nutzer anfertigen
- Finanzinstitute gem. Art. 1 des Gesetzes 10/2014 vom 26. Juni
- Kreditinstitute
- Versicherungsunternehmen und Rückversicherungsunternehmen
- Investmentdienste, die durch die Börsengesetze reguliert werden
- Energieversorger und Vermarkter von elektrischer Energie sowie Versorger und Vermarkter von Gas
- Organisationen, die gemeinsame Dateien zur Bewertung einer Kreditfähigkeit oder dem Betrugsmanagement bzw. der Prävention verantworten, einschließlich der Verantwortlichen für Dateien, die durch die Gesetze zur Verhütung und Bekämpfung der Geldwäsche und der Finanzierung des Terrorismus reguliert werden
- Organisationen, die Werbekampagnen durchführen oder Handelsforschung betreiben, einschließlich der Marktanalyse und Marktforschung, falls sie Verarbeitungen auf Basis von Vorlieben der Betroffenen durchführen oder Profile derselbigen erstellen
- Gesundheitseinrichtungen, die gesetzlich zur Aufbewahrung von Patientendaten verpflichtet sind. Ausgenommen hiervon sind Gesundheitsberufe, die ihre Tätigkeit als Einzelperson ausüben, selbst wenn sie zur Abewahrung der Patientendaten verpflichtet sind
- Organisationen, die mit der Veröffentlichung von Unternehmensberichten befasst sind, vorausgesetzt die Berichte beziehen sich auf eine natürliche Person
- (Glücks-)Spielanbieter, die ihre Aktivität über elektronische, telematische oder interaktive Kanäle entwickeln und durch die Gesetze für (Glücks-)Spieleanbieter reguliert werden
- Private Sicherheitsunternehmen
- Sportverbände, wenn sie Daten von Minderjährigen verarbeiten

Link zum Gesetz (ES)

ZYPERN

Teil IV 14. Gesetz 125(I)/2018: Die zypriotische Aufsichtsbehörde hat die gesetzliche Befugnis, eine Liste von Verarbeitungstätigkeiten zu veröffentlichen, die eine Benennungspflicht gem. Art. 37 Abs. 1 DS-GVO auslösen soll. Eine entsprechende Veröffentlichung ist bisher nicht erfolgt.

Link zum Gesetz (EN)

IT-Grundschutzprofil für Handwerksbetriebe

Im Rahmen ihrer 2017 geschlossenen Kooperation haben der ZDH (Zentralverband des Deutschen Handwerks) und das BSI (Bundesamt für Sicherheit in der Informationstechnik) mit dessen Initiative – der Allianz für Cyber-Sicherheit – den Prozess zur Erstellung eines IT-Grundschutz-Profils für Handwerksbetriebe initiiert. Die Basis hierfür bildet das vom BSI entwickelte IT-Grundschutz-Kompendium. Dieses enthält Methoden und Vorgehensweisen zu den unterschiedlichsten Themen aus dem Bereich der Informationssicherheit. Außerdem hilft es dabei, notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Experten aus Handwerksorganisationen haben in einer begleitenden Workshop-Reihe, ausgehend von den typischen Geschäftsprozessen Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung, ein Muster-Sicherheitskonzept entwickelt. Dieses dient als Schablone für Handwerksbetriebe mit vergleichbaren Rahmenbedingungen.

Individuelle Sicherheitsprozesse bedarfsgerecht gestalten

Der durch die Allianz für Cybersicherheit gemeinsam mit dem Kompetenzzentrum Digitales Handwerk entwickelte Routenplaner zeigt Wege auf, wie kleine und mittelständische Unternehmen das Thema Informationssicherheit zielgerichtet angehen und umsetzen können. Handwerksbetriebe können anhand von drei Routen ihren individuellen Sicherheitsprozess gemäß IT-Grundschutz des BSI bedarfsgerecht gestalten. Anschauliche Routenpläne und zielgruppengerechte Arbeitshilfen führen auf die für Handwerksbetriebe maßgeblichen IT-Grundschutz-Bausteine und dazu passenden Umsetzungshinweise des BSI in der aktuellen Edition 2019.
Das IT-Grundschutz-Profil für Handwerksbetriebe ermöglicht durch eine breite und grundlegende Erst-Absicherung den Einstieg in die Informationssicherheit für die in Handwerksbetrieben typischen Geschäftsprozesse Auftragsgewinnung, Angebotserstellung, Auftragsdurchführung und Abrechnung.

Quelle: Zentralverband des Deutschen Handwerks
Bundesamt für Sicherheit in der Informationstechnik (BSI)

BayLDA veröffentlicht Tätigkeitsbericht für die Jahre 2017/2018

Gemäß § 38 Abs. 1 Satz 7 des Bundesdatenschutzgesetzes (BDSG) hat das BayLDA als Aufsichtsbehörde regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen. In ihren Tätigkeitsberichten informieren die Aufsichtsbehörden die Öffentlichkeit über die Schwerpunkte ihrer Arbeit.
Seinen 8. Tätigkeitsbericht hat das BayLDA am 22.03.2019 veröffentlicht. In den 150 Seiten ihres Tätigkeitsberichts sind konkrete Fälle aus dem Zeitraum vor Anwendbarkeit der Datenschutz-Grundverordnung (DS-GVO), d.h. vor dem 25. Mai 2018 nur dann aufgenommen worden, wenn sie auch noch für den neuen Rechtsrahmen Bedeutung hatten. Nach eigenen Angaben konnte die Behörde die größten Unsicherheiten und häufigsten Anfragen im Bereich der Informationspflichten beobachten. Mit anderen Worten bezog sich eine Fülle der Fragen darauf, in welcher Art und Weise und in welchem Umfang Betroffene Personen darüber informiert werden müssen, wie mit ihren Daten umgegangen wird. Etwa ebenso häufig waren Fragen nach den Rechtsvoraussetzungen für die Veröffentlichung von Bildern von Vereinsfesten, Mitarbeiterzeitungen, Berichte über Veranstaltungen, Erstellen von Chroniken usw. festzustellen.
In 19 von 24 Kapiteln des Tätigkeitsberichts stellt das BayLDA auf übersichtliche,
und prägnante Art und Weise Einzelfälle aus den verschiedensten Bereichen vor und macht seine eigene Bewertung transparent. Diese erstrecken sich von Datenschutz im Internet, über Werbung, Versicherungswirtschaft, Gesundheit, Videoüberwachung bis zum technischen Datenschutz und der Informationssicherheit.
Künftig wird das BayLDA nicht mehr wie bisher im Zyklus von zwei Jahren sondern, gemäß DS-GVO, jährlich einen Bericht über ihre Tätigkeit erstellen. Somit ist dies der letzte Tätigkeitsbericht, der relativ umfangreich ausgewählte Sachverhalte aus den vergangenen zwei Jahren darstellt.
Der Tätigkeitsbericht für die Jahre 2017 und 2018 ist unter folgendem Link erreichbar:

Quelle: https://www.lda.bayern.de/de/taetigkeitsberichte.html

Videoüberwachung in der Zahnarztpraxis scheitert regelmäßig an Erforderlichkeit

Eine Videoüberwachung in einer Zahnarztpraxis, die ungehindert betreten werden kann, unterliegt strengen Anforderungen an die datenschutzrechtliche Erforderlichkeit. Dies hat das Bundesverwaltungsgericht in Leipzig heute entschieden.
Die Klägerin ist Zahnärztin. Ihre Praxis kann durch Öffnen der Eingangstür ungehindert betreten werden; der Empfangstresen ist nicht besetzt. Die Klägerin hat oberhalb dieses Tresens eine Videokamera angebracht. Die aufgenommenen Bilder können in Echtzeit auf Monitoren angesehen werden, die die Klägerin in Behandlungszimmern aufgestellt hat (sog. Kamera-Monitor-System). Die beklagte Landesdatenschutzbeauftragte gab der Klägerin u.a. auf, die Videokamera so auszurichten, dass der Patienten und sonstigen Besuchern zugängliche Bereich vor dem Empfangstresen, der Flur zwischen Tresen und Eingangstür und das Wartezimmer, nicht mehr erfasst werden. Insoweit ist die nach erfolglosem Widerspruch erhobene Klage in den Vorinstanzen erfolglos geblieben.

Das Bundesverwaltungsgericht hat die Revision der Klägerin bezüglich ihrer Zahnarztpraxis aus im Wesentlichen folgenden Gründen zurückgewiesen: Die seit 25. Mai 2018 in allen Mitgliedstaaten der Europäischen Union unmittelbar geltende Datenschutz-Grundverordnung findet keine Anwendung auf datenschutzrechtliche Anordnungen, die – wie im vorliegenden Fall – vor diesem Zeitpunkt erlassen worden sind. Entscheidungen, die vor diesem Stichtag getroffen wurden, werden nicht nachträglich an diesem neuen unionsrechtlichen Regelungswerk gemessen. Der Bundesgesetzgeber hatte die Zulässigkeit der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) vor dem 25. Mai 2018 durch § 6b des Bundesdatenschutzgesetzes a. F. auch für private Betreiber abschließend geregelt.
Nach Absatz 1 dieser Vorschrift setzte die Beobachtung durch ein Kamera-Monitor-System auch ohne Speicherung der Bilder voraus, dass diese zur Wahrnehmung berechtigter Interessen des Privaten erforderlich ist und schutzwürdige Interessen der Betroffenen nicht überwiegen. Nach den bindenden Tatsachenfeststellungen des Oberverwaltungsgerichts hat die Klägerin bereits nicht dargelegt, dass sie für den Betrieb ihrer Zahnarztpraxis auf die Videoüberwachung angewiesen ist. Es bestehen keine tatsächlichen Anhaltspunkte, die ihre Befürchtung, Personen könnten ihre Praxis betreten, um dort Straftaten zu begehen, berechtigt erscheinen lassen. Die Videoüberwachung ist nicht notwendig, um Patienten, die nach der Behandlung aus medizinischen Gründen noch einige Zeit im Wartezimmer sitzen, in Notfällen betreuen zu können. Schließlich sind die Angaben der Klägerin, ihr entstünden ohne die Videoüberwachung erheblich höhere Kosten, völlig pauschal geblieben.

Quelle: Bundesverwaltungsgericht
Urteil vom 27. März 2019 – BVerwG 6 C 2.18 –

Einwilligung für Fotos

Frage des GDD-Erfa-Kreises Coburg zum Thema Einwilligung für Fotos:
Auf einer Veranstaltung werden Fotos durch den Veranstalter gemacht. Bei Portraitfotos ist eine Einwilligung notwendig. Wie verhält es sich bei der Aufnahme von mehreren Personen, die „einfach im Raum stehen", aber trotzdem gut zu erkennen und identifizieren sind, z.B. bei Veranstaltungen von kleinen Vereinen mit überschaubarer Anwesenheitszahl? Diese Bilder sollen danach zum Beispiel an die Presse gegeben werden. Benötigt man für jedes Foto eine Einwilligung aller darauf zu Erkennenden, auch wenn diese nur von der Seite oder von hinten aufgenommen wurden?

Antwort des BayLDA:
Wenn Vereine eigene Veranstaltungen machen und dort fotografiert wird (also z.B. durch Mitglieder im Auftrag des Vereins) und diese Bilder veröffentlichen wollen, kann dies im Rahmen der sog. Interessensabwägung nach Art. 6 Abs. 1 Buchstabe f DS-GVO zulässig sein, ohne dass man eine ausdrückliche Einwilligung der betroffenen Personen einholen muss. Dies gilt auch, wenn einzelne Personen gut identifizierbar sind – solange eben die Veranstaltung als solche, Anlass und Vordergrund der Berichterstattung ist und nicht die einzelne Person als solche.
Anders ist es aber, wenn Kinder davon betroffen sind. Hier ist eine Einwilligung der Erziehungsberechtigten einzuholen.
Unabhängig davon sind die betroffenen Personen auf geeignete Art und Weise (z.B. Aushänge) insbesondere darauf hinzuweisen, dass und zu welchen Zwecken Bilder gemacht und wo sie veröffentlicht werden sollen. Personen, die sich nicht fotografieren lassen möchten, können sich dann darauf einstellen und sich entsprechend verhalten.

Datenschutz bei der Nutzung von Multifunktionsgeräten

Im Rahmen seines IT-Grundschutz-Katalogs gibt das Bundesamt für Sicherheit in der Informationstechnik umfangreiche Maßnahmen für die Sicherheit von vernetzten Druckern, Druckservern, Dokumentenscannern, Kopierern und Multifunktionsgeräten vor. Als Multifunktionsgeräte werden dabei Geräte bezeichnet, die mehrere verschiedene papierverarbeitende Funktionen bieten, etwa Drucken, Kopieren und Scannen oder auch Fax-Dienste. Wie jedes IT-System sind auch Drucker, digitale Kopierer, netzfähige Scanner und Multifunktionsgeräte vielfältigen Gefahren ausgesetzt. Für den IT-Grundschutz dieser Systeme werden die folgenden typischen Gefährdungen angenommen.
Die empfohlenen Maßnahmen des BSI behandeln die Planung, Konzeption, Beschaffung, Umsetzung, Betrieb, Aussonderung, Notfallvorsorge. Die Landesbeauftragte für Datenschutz und Informationsfreiheit, Freie Hansestadt Bremen hat dieses Thema ebenfalls unter der Orientierungs- und Handlungshilfe „Fotokopierer: Die angreifbare Datenstation" aufgegriffen. Darin werden die Eckpunkte eines datenschutzgerechten Einsatzes digitaler Kopiersysteme behandelt.

Auskunftsrecht nach Art. 15 DS-GVO: Kopie der personenbezogenen Daten

Frage des GDD-Erfa-Kreises Würzburg zur Kopie der personenbezogenen Daten:
Die Auskunft nach Art. 15 Abs. 3 DS-GVO regelt, dass der Verantwortliche eine Kopie der zu verarbeitenden Daten zur Verfügung stellt. Muss diese zwingend bei einer Auskunft als Anlage mitgeschickt werden oder reicht es, die betreffenden Daten (mit den weiteren Angaben nach Art. 15 Abs. 1 DS-GVO) in dem Antwortschreiben mitzuteilen? Eine Kopie würde nur dann mitgeschickt werden, wenn die betroffene Person explizit danach fragt

Antwort BayLDA:
Eine zusätzliche Kopie der Daten muss nicht mitgeschickt werden. Art. 15 Abs. 3 DS-GVO regelt nach unserer Ansicht die bevorzugte Form der Auskunftserteilung und bewirkt keinen zusätzlichen Inhalt für eine Auskunft nach Art. 15 DS-GVO. Es genügt also auch, in einem Antwortschreiben die personenbezogenen Daten der betroffenen Person aufzulisten.

Erste Abmahnungen wegen fehlender Verschlüsselung

Was viele durch die DS-GVO befürchteten, ist lange ausgeblieben. Nun aber gibt es sie doch: Die erste kleine Abmahnwelle ist angelaufen. Wegen angeblicher Verstöße gegen die Datenschutz-Grundverordnung (DS-GVO) versendet nach übereinstimmenden Medienberichten ein selbst ernannter Verbraucherschutzverband Abmahnungen. Empfänger sind vor allem Unternehmen, die ein Kontaktformular ohne SSL-Verschlüsselung auf ihrer Homepage haben.

Woher kommen die Abmahnungen?

Hinter den versendeten Abmahnungen steckt die IGD Interessengemeinschaft Datenschutz e.V. Auf ihrer Internetseite bezeichnet sich der Verein IGD als Bürgerrechtsorganisation: „Die Interessengemeinschaft Datenschutz ist eine als eingetragener Verein geführte Bürgerrechtsorganisation, die sich für die Datenschutzinteressen von Verbrauchern in Deutschland einsetzt. […] Unsere zentrale Aufgabe ist es, die individuellen Rechte der Bürger, wie Sie einst im Bundesdatenschutzgesetz und nun auch in der EU-Weit harmonisierten Datenschutzgrundverordnung erfasst sind, gegenüber Unternehmern und Unternehmen zu vertreten.“ Der Verein sitzt im brandenburgischen Ludwigsfelde bei Berlin.

Fehlende Verschlüsselung beim Versand des Kontaktformulars

Der Art. 32 DS-GVO regelt die Sicherheit der Verarbeitung und verlangt tatsächlich, dass personenbezogene Daten wie E-Mails durch technische Maßnahmen geschützt werden. Dazu dürfte nach allgemeiner Auffassung auch eine adäquate Verschlüsselung gehören. Die angeschriebenen Webseiten-Betreiber haben also mit großer Wahrscheinlichkeit gegen diese Regelung der DS-GVO verstoßen.

IGD fordert Zahlung und Unterlassungserklärung

Der Verein IGD bedient sich nun dem Instrument der Abmahnungen. Ob dieses für Verstöße gegen die DS-GVO wirklich anwendbar ist, wird gegenwärtig sehr kontrovers diskutiert. Auch die deutsche Gerichtsbarkeit hat hierzu bislang keine eindeutige Rechtsauffassung vertreten. Trotzdem fordert der Verein nun von den angeschriebenen Unternehmen eine sofortige Zahlung von rund 280,- Euro und die Abgabe einer Unterlassungserklärung. Wer die unterzeichnet, kann bei nochmaligen Verstößen eine Vertragsstrafe von 4000,- Euro auferlegt bekommen.

Speicherbegrenzung bei Aufnahmen aus Videoüberwachung

Frage des GDD-Erfa-Kreises Coburg zur Videoüberwachung:
Ein Motorradhändler vertreibt hochwertige neue Motoräder sowie Ersatzteile und repariert in einer eigenen Werkstatt auch Maschinen. Ersatzteile werden von Lieferanten an einer Laderampe in ein Teilelager gestellt. Hier ist aufgrund der hohen Umschlagfrequenz nicht über den gesamten Entladevorgang hinweg ein Mitarbeiter des Motorradverkäufers anwesend. Die Laderampe und das Teilelager sind mit Videokameras überwacht, die Aufnahmen werden aufgezeichnet. In der Vergangenheit kam es bei der Lieferung von Neuteilen oft zu Mängeln durch Beschädigungen. Für den Nachweis, dass es sich um einen Liefermangel handelt, verlangt der Zulieferer die Aufzeichnungen der Kamera. Die Kameraüberwachung dient also dem Zweck ein Fehlverhalten des Lieferanten (…). Einen anderen Nachweis für eine unsachgemäße Handhabung der Ware durch den Lieferanten (…) akzeptiert der Zulieferer, welcher die Ware über Werksfahrer ausliefern lässt, nicht. Der zweite Grund der Videoüberwachung und der Speicherung liegt darin, dass es in der Vergangenheit öfters zu Diebstählen durch Mitarbeiter kam, welche hochwertige Ersatzteile aus dem Lager entwendeten. Aufgrund der oben beschriebenen Unübersichtlichkeit fallen die Diebstähle meist erst viel später auf, nämlich wenn das entwendete Teil verbaut werden soll.
Da die Mängel, bzw. die Diebstähle aufgrund der individuellen Arbeitsabläufe und Gegebenheiten in diesem speziellen Fall erst mehrere Tage nach der Lieferung, bzw. der Tat bemerkt werden können, müssten die Aufnahmen – um einen Nachweis für fahrlässiges oder vorsätzliches Handeln zu bieten – über einen längeren Zeitraum gespeichert werden. Eine tägliche Grobsichtung, um fahrlässiges Verhalten festzustellen, ist aufgrund der hohen Umschlagfrequenz bei den Anlieferungen nicht immer zielführend. Dort würden nur die offensichtlichen Fehler (Herunterfallen von Teilen o.ä.) auffallen. Details, wie zum Beispiel das Ansetzen der Sackkarre an der falschen Seite eines Kartons, das Belasten einer sensiblen Kante der Schutzverpackung, welche ursächlich für viele Mängel sind, sind bei einer täglichen Sichtung der Aufnahmen kaum zu erkennen. Ebenso sieht es bei dem Zweck der Diebstahlsaufklärung auf. Bei einer täglichen Sichtung kann nicht festgestellt werden, ob der Mitarbeiter ein Teil im Rahmen seiner Tätigkeit in der Werkstatt aus dem Lager entnimmt, um es zu verbauen oder ob er es zum Zwecke des Diebstahls entnimmt.
Bei wie vielen Tagen wäre in diesem Fall die Höchstgrenze für eine Speicherung der Aufzeichnungen erreicht?

Antwort des BayLDA:
Die Daten der Videoüberwachung müssen gemäß der DS-GVO gelöscht werden, wenn sie zur Erreichung der Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Absatz 1 lit. a DS-GVO) oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Ob eine Sicherung des Materials notwendig ist, dürfte bei Videoüberwachungs- „Standardfällen“ innerhalb von ein bis zwei Tagen geklärt werden können. Unter Berücksichtigung von Art. 5 Absatz 1 lit. c DS-GVO – „Datenminimierung“ – und Absatz 1 lit. e DS-GVO – „Speicherbegrenzung“ sollte grundsätzlich nach 48 Stunden eine Löschung erfolgen.
Die Zwecke der Verarbeitung der Kameraaufnahmen müssen ausreichend deutlich definiert werden. Sofern ein solcher Zweck eine längere Speicherdauer erforderlich macht, ist dies grundsätzlich zulässig, nach Abwägung der Interessenlagen und ggf. Ausschluss von milderen Mitteln (z.B. mehr Personalkontrollen etc.) mit Begründung. Eine pauschale Höchstspeicherdauer ist in der DS-GVO nicht fixiert, da es auf den Einzelfall ankommt, allerdings waren aus unserer Praxis bislang max. 14 Tage in der Regel die Höchstgrenze für die jeweiligen zulässigen Zwecke der Videoüberwachung, so dass pauschal 30 Tage für alle Aufnahmebereiche aus unserer Sicht zu lang wären. Ggf. sollte sich das Unternehmen direkt an uns wenden und konkrete Angaben zum Aufnahmeort, des Zwecks und der – längeren – Speicherdauer machen, damit wir den Fall präziser beurteilen können.