Landesbeauftragte veröffentlicht Tätigkeitsbericht

Dienstag, 24 März 2020

https://www.datenschutz.de/landesbeauftragte-veroeffentlicht-taetigkeitsbericht/

Pressemitteilung der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg vom 24.03.2020.

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Dagmar Hartge, veröffentlicht heute ihren Tätigkeitsbericht zum Datenschutz für das Jahr 2019. Es ist der erste Bericht seit Einführung der Datenschutz-Grundverordnung, der ein vollständiges Kalenderjahr umfasst.

Im Jahr 2019 gingen bei der Landesbeauftragten 878 **Beschwerden** von natürlichen Personen ein, die der Ansicht waren, dass die Verarbeitung ihrer Daten gegen das Datenschutzrecht verstoßen hat. In über 400 Fällen leisteten wir eine schriftliche **Beratung** sowohl gegenüber Privatpersonen als auch gegenüber Verwaltungen und Unternehmen. In zwanzig Fällen machte die Landesbeauftragte von Befugnissen Gebrauch, die ihr unabhängig von den Bußgeldern zur Verfügung stehen (Warnung, Verwarnung, Anweisung/Anordnung). Wir erhielten 362 **Meldungen von Datenschutzverletzungen**. Mehr als die Hälfte davon betraf Fehler beim Versand von Unterlagen beziehungsweise E?Mails. In zehn Fällen waren von den Datenschutzverletzungen mehr als 1.000 Personen betroffen (A V, Seite 87). Dagmar Hartge:

> Zwar stellt die Bearbeitung der Meldungen von Datenschutzverletzungen bereits jetzt einen erheblichen Aufwand für meine Behörde dar. Trotz der hohen Anzahl der Meldungen gehe ich aber davon aus, dass es sich dabei nur um die Spitze des Eisbergs handelt. Verantwortliche, die Meldungen versäumen, unvollständig oder verspätet abgeben bzw. die betroffenen Personen trotz hohen Risikos nicht informieren, riskieren ein Bußgeld.

Auch im Jahr 2019 haben sich Bürgerinnen und Bürger in hohem Maße über die **Videoüberwachung** beschwert. In ihrem Bericht schildert die Landesbeauftragte den Fall eines Kultur- und Gewerbezentrums, dessen Hausverwaltung in großem Umfang Kameras eingesetzt hat (A I 5, Seite 22). Neben einer Fleischerei und einer Autowerkstatt befanden sich auch eine Diskothek und ein Theater in deren Erfassungsbereich – und mit ihnen die Besucherinnen und Besucher. Als Rechtfertigung gab die Hausverwaltung die Verhinderung von Diebstählen und Sachbeschädigungen an, vermochte dies aber nur im Falle von zwei Kameras mit einem berechtigten Interesse zu begründen. Wir untersagten den Betrieb der übrigen Kameras. Diese differenzierte Vorgehensweise stand im Einklang mit der höchstrichterlichen Rechtsprechung. Im Berichtszeitraum hatte das Bundesverwaltungsgericht nämlich eine Anordnung der Landesbeauftragten zur datenschutzgerechten Ausrichtung der **Kamera in einer Zahnarztpraxis** bestätigt (A I 4, Seite 19). Gerechtfertigt hatte die Zahnärztin ihre Kameras mit medizinischen Notfällen, der Verhinderung von Straftaten und Einsparungen von Personalkosten. Das Bundesverwaltungsgericht betonte hingegen die Notwendigkeit, zuerst mildere Mittel, die dieselben Zwecke erfüllen, in Erwägung

zu ziehen. Insbesondere stellte es fest, dass Kosteneinsparungen allein die Zulässigkeit einer Videoüberwachung keinesfalls begründen können.

Dass die Digitalisierung nahezu sämtliche Lebensbereiche betrifft, bestätigt sich auch in den brandenburgischen Schulen. Online-Lernplattformen, sogenannte **Schul-Clouds**, werden dort zunehmend eingesetzt (A II 2, Seite 36). Die zentrale Pilotierung eines entsprechenden Projekts hat das Hasso-Plattner-Institut übernommen. In Zusammenarbeit mit uns stellte es den teilnehmenden Schulen Muster für die erforderlichen datenschutzrechtlichen Unterlagen zur Nutzung der Schul-Cloud zur Verfügung. Im Rahmen dieser konstruktiven Zusammenarbeit konnte die Landesbeauftragte eine hohe Sensibilität für den Datenschutz erreichen. Gleichwohl haben wir empfohlen, externe Anbieterinnen und Anbieter von Lerninhalten nur einzubinden, wenn diese selbst die datenschutzrechtlichen Anforderungen erfüllen. Unsere Prüfungen auf Seiten einiger Schulen ergaben zudem noch einige Umsetzungsdefizite. Problematischer schien uns aber die derzeit noch notwendige, freiwillige Einwilligung der Schülerinnen und Schüler bzw. ihrer Eltern in die Datenverarbeitung. Wird diese widerrufen, dürfen die betroffenen Kinder und Jugendlichen die Schul-Cloud nicht mehr nutzen. Praktikabel ist dieses Ergebnis nicht. Gegenüber dem Gesetzgeber haben wir deshalb angeregt, eine Befugnisnorm für den Einsatz von Online-Lernplattformen im Brandenburgischen Schulgesetz zu verankern.

In einigen öffentlichen Wahlbekanntmachungen dürfen nicht mehr die **vollständige Anschrift der Wahlbewerberin oder des Wahlbewerbers**, sondern nur noch deren bzw. dessen Wohnort angegeben werden (A II 3, Seite 38). Dies ist nunmehr in zwei Verordnungen geregelt, welche die Landesregierung im Ergebnis unserer Anregung geändert hatte. Dennoch veröffentlichten zahlreiche Gemeinden vor allem im Rahmen der Kommunalwahlen weiterhin die vollständigen Anschriften der Kandidatinnen und Kandidaten. Wir haben aus diesem Anlass eine Umfrage unter den Gemeinden durchgeführt und diese gebeten, ihre Veröffentlichungspraxis zu überprüfen. Als Grund für die Weiterführung der bisherigen Praxis stellte sich schlicht die Unkenntnis der neuen Vorschriften heraus. Dagmar Hartge:

> Vor dem Hintergrund vielfältiger Bedrohungen von Kommunalpolitikerinnen und Kommunalpolitkern kommt dem gebotenen Verzicht auf die Veröffentlichung der vollständigen Anschriften von Wahlbewerberinnen und Wahlbewerbern eine aktuelle Bedeutung zu. Die Regelung zeigt, dass Datenschutz kein abstraktes Rechtsgut darstellt, sondern den Schutz von Personen gewährleistet. Er ist damit eine ganz konkrete Voraussetzung für gesellschaftliches Engagement.

Wer personenbezogene Daten verarbeitet, muss die Betroffenen zum Zeitpunkt der Datenerhebung über die Art und Weise der Verarbeitung sowie über deren Rechte informieren. Dies ist einerseits eine Kernregelung des neuen Datenschutzrechts, andererseits werden viele Patientinnen und Patienten bereits die Erfahrung gemacht haben, dass Ärztinnen und Ärzte ganz unterschiedlich mit diesen Informationspflichten umgehen. Bei einer **Überprüfung der Datenschutzinformationen in ausgewählten Arztpraxen** sahen wir diese Annahme bestätigt (A II 4, Seite 40). Teilweise sollten die Behandelten die Kenntnisnahme der Informationen per Unterschrift bestätigen – rechtlich vorgesehen ist dies nicht. Auch waren Informationen über die Datenverarbeitung häufig in unzulässiger Weise mit Einwilligungen vermischt worden. In den meisten Fällen besteht jedoch gar kein Bedarf, überhaupt eine

Einwilligungserklärung zu verlangen. Die Befugnis für die Datenverarbeitung zu Behandlungszwecken ergibt sich grundsätzlich bereits aus einem in der Regel bestehenden Vertragsverhältnis. Betroffene können einer medizinischen Dokumentation schließlich auch nicht widersprechen. Im Ergebnis konnte die Landesbeauftragte durch ihre Prüfung eine erfreuliche Sensibilisierung für Fragen des Datenschutzes in den Arztpraxen erreichen.

Zur Gewährleistung der Sicherheit in der Ausländerbehörde setzte ein Landkreis ein privates Wachschutzunternehmen ein. Wie sich bei einer unangekündigten Vor-Ort-Kontrolle herausstellte, führte das Unternehmen bereits am Eingang eine Art „Einlasskontrolle“ durch und ließ sich die Ausweise der Besucherinnen und Besucher zeigen. Der Wachschutz nahm mehrfach persönliche Unterlagen an sich, verschwand damit minutenlang, um sie zu kopieren, und übergab zuvor erhaltene Dokumente an die zuständigen Sachbearbeiterinnen und Sachbearbeiter. Es herrschte also eine durchaus intensive **Arbeitsteilung zwischen Behörde und Wachschutz** (A III 2, Seite 49). Lediglich den zuständigen Sachbearbeiterinnen und Sachbearbeitern stand es aber zu, personenbezogene Daten der Ausländerinnen und Ausländer zu verarbeiten. Dass diese Arbeitsteilung datenschutzrechtlich unzulässig war, liegt auf der Hand. Wir haben gegenüber dem Landkreis inzwischen eine Verwarnung ausgesprochen.

Im Rahmen der verpflichtenden Meldung einer Datenschutzverletzung teilte uns ein brandenburgisches Unternehmen mit, dass sein **Internetangebot durch eine Schadsoftware kompromittiert** war (A III 5, Seite 53). Besucherinnen und Besucher der Website riskierten, dass ihre Computer für komplizierte Berechnungen im Kontext digitaler Währungen missbraucht wurden. Ursache des Vorfalls war ein versäumtes Softwareupdate. Bereits zum Zeitpunkt der Meldung war die Software zur Bereitstellung und Pflege des Internetangebots fast zwei Jahre lang nicht aktualisiert worden. Der Vertrag mit einem externen IT-Dienstleister war seit einem Jahr ausgelaufen. In der Zwischenzeit hatte sich das Unternehmen nicht mehr um eine Aktualisierung der Software gekümmert. Erst auf unsere ausdrückliche Aufforderung hin schloss es einen Vertrag zur Auftragsverarbeitung mit dem neuen Dienstleister. Die Bußgeldstelle bei der Landesbeauftragten leitete wegen der fehlenden technisch-organisatorischen Maßnahmen sowie der mangelnden Sorgfalt bei der Gestaltung der Auftragsverarbeitung ein Ordnungswidrigkeitenverfahren ein. Dagmar Hartge:

> Regelmäßige Software-Updates sind als technische Maßnahme keine Kür, sondern unbedingte Pflicht. Dies gilt umso mehr, wenn die Rechner, auf denen solche Programme laufen, mit dem Internet verbunden und somit der Gefahr von Angriffen mit Schadsoftware ausgesetzt sind. Eine Aktualisierung von Betriebs- sowie Content-Management-Systemen schützt sowohl Unternehmen und Verwaltungen als auch Privatpersonen vor bösen Überraschungen.

Im zurückliegenden Jahr führte die Bußgeldstelle der Landesbeauftragten 47 **Ordnungswidrigkeitenverfahren** – doppelt so viele wie im Vorjahr (A I 8, Seite 27 sowie V 4.2, Seite 91). Etwa die Hälfte davon war nach der neuen Rechtslage zu bewerten. 24 Verfahren endeten mit der Verhängung eines Bußgeldes. Sie richteten sich noch überwiegend nach der alten Rechtslage, da die begangenen Ordnungswidrigkeiten zumeist vor Einführung der Datenschutz-Grundverordnung beendet worden waren. Insgesamt setzte die Bußgeldstelle im Jahr 2019 Bußgelder in Höhe von 69.150 Euro fest. Beispielsweise hatte der Betreiber eines Schwimmbads Gäste und Beschäftigte in unzulässiger Weise mit

einer Videokamera überwacht sowie gegen weitere datenschutzrechtliche Pflichten verstoßen. Ein anderes Unternehmen setzte einen Dienstleister ein, um Betroffenen Auskunft über die zu ihrer Person verarbeiteten Daten zu erteilen. Den für solche Fälle verpflichtenden Vertrag über die Auftragsverarbeitung versäumte es, schriftlich abzuschließen. Erschwerend kam u. a. hinzu, dass die Auskünfte unter dem Logo des Dienstleisters erteilt wurden und somit nicht zu erkennen war, in welcher Verbindung dieser zu dem Unternehmen stand. Ein weiteres Verfahren führte die Bußgeldstelle gegen einen Mediziner, der einen Bekannten mit der Sicherung der Patienten- und Mitarbeiterdaten aus seiner Arztpraxis beauftragte. Dieser speicherte die ihm anvertrauten Daten auf seinem Computer am Arbeitsplatz, wo der Arbeitgeber sie schließlich entdeckte. Verantwortlich für diesen Vorfall blieb der Mediziner, der es versäumt hatte, sich von der weisungsgemäßen Ausführung des Auftrags sowie von der Umsetzung der erforderlichen technischen und organisatorischen Schutzmaßnahmen seines Bekannten zu überzeugen.

Am 22. Juni 2019 trat das **Brandenburgische Polizei-, Justizvollzugs- und Maßregelvollzugsdatenschutzgesetz** in Kraft. Hinter dieser sperrigen Bezeichnung verbirgt sich die Umsetzung einer europäischen Richtlinie, die den Datenschutz für die Rechtsbereiche polizeiliches Handeln, Justizvollzug und Maßregelvollzug regelt. Die Datenschutz-Grundverordnung gilt hier nicht. Das genannte Gesetz enthält eine eigenständige, jährliche Berichtspflicht der Landesbeauftragten, der wir gleichzeitig mit dem Bericht zum allgemeinen Datenschutzrecht erstmals nachkommen (B 3, Seite 98).

Auf dem Gebiet der polizeilichen Arbeit stand die **automatische Kennzeichenerfassung (KESY)** im Fokus der Datenschutzaufsichtsbehörde (B 3, Seite 100). Stein des Anstoßes war das im Frühjahr 2019 eher zufällige Bekanntwerden der umfassenden und lange andauernden Erfassung von Kennzeichen auf brandenburgischen Autobahnen im Aufzeichnungsmodus. Im Ergebnis einer umfassenden Prüfung des von der Polizei Brandenburg betriebenen Verfahrens sprach die Landesbeauftragte gegenüber dem Polizeipräsidium zunächst eine Beanstandung wegen des Verstoßes gegen die Unterstützungspflicht aus. Es hatte sich geweigert, uns die für eine Prüfung erforderlichen Beschlüsse und Anordnungen vorzulegen. Im weiteren Verlauf beanstandeten wir auch die datenschutzrechtlichen Verstöße. Insbesondere stellt die von der Polizei herangezogene Regelung des § 100h Abs. 1 Satz 1 Nr. 2 Strafprozessordnung nach unserer Auffassung für den Einsatz der automatisierten Kennzeichenerfassung keine ausreichende Rechtsgrundlage dar. Darüber hinaus waren weitere, gravierende datenschutzrechtliche Mängel festzustellen. Eine von uns geforderte Löschung der nicht mehr benötigten Daten nahm die Polizei nicht vor. Vielmehr übertrug sie einen Teil der Datensätze lediglich von dem zentralen KESY-Server auf andere Datenträger, um diese jeweils den Staatsanwaltschaften zur Verfügung zu stellen. Das Verfahren betreibt sie aber in modifizierter Weise weiter.

KESY ist nur ein Beispiel für die große Zahl an Verfahren, mit denen die Polizei Brandenburg personenbezogene Daten verarbeitet. Mindestens ebenso wichtig sind das polizeiliche Vorgangsbearbeitungssystem ComVor, das Informations- und Auskunftsverfahren POLAS sowie das Einsatzleitsystem für Behörden und Organisationen mit Sicherheitsaufgaben ELBOS. Voraussetzung für einen gesetzeskonformen Umgang mit den personenbezogenen Daten ist ein fundiertes IT-Sicherheitskonzept, das aus einer Risikoanalyse abgeleitet wird. Ein solches Konzept beschreibt Mindestanforderungen an die IT Sicherheit, dient als Leitfaden zu ihrer Umsetzung und soll helfen, Bedrohungen frühzeitig zu erkennen. Die Polizei hatte durchaus vorgesehen, für die einzelnen Systeme und Komponenten ein systematisches **Rahmensicherheitskonzept** zu erstellen, konnte uns dieses trotz wiederholter Aufforderung allerdings über Jahre hinweg nicht komplett vorlegen (B 2, Seite 98). Termine

wurden nicht eingehalten und die Fertigstellung des Konzepts immer wieder verschoben. Diesen Missstand beanstandete die Landesbeauftragte im Jahr 2019. Die uns schließlich vorgelegten Unterlagen ergaben, dass trotz einiger Fortschritte noch erhebliche Defizite bei der Umsetzung der technisch-organisatorischen Maßnahmen bestehen.

Frau Hartge hat den Tätigkeitsbericht Datenschutz 2019 heute der Präsidentin des Landtages Brandenburg, Frau Prof. Dr. Ulrike Liedtke, übersandt. Auf eine persönliche Übergabe und die damit üblicherweise verbundene Pressekonferenz haben wir aus aktuellem Anlass zwar verzichtet. Für Fragen oder Interviews steht Frau Hartge aber telefonisch gerne zur Verfügung.

Der Tätigkeitsbericht der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg kann hier abgerufen werden.

Die Pressemitteilungen der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg können hier abgerufen werden.
