Landesbeauftragte veröffentlicht Tätigkeitsbericht Datenschutz 2020

Montag, 03 Mai 2021

https://www.datenschutz.de/landesbeauftragte-veroeffentlicht-taetigkeitsbericht-datenschutz-2020/

Presseinformation der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht vom 03.05.2021

Heute legt die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Dagmar Hartge, ihren Tätigkeitsbericht zum Datenschutz für das Jahr 2020 vor.

Das vergangene Jahr war auch und gerade auf dem Gebiet des Datenschutzes von den Herausforderungen der Corona-Pandemie geprägt. Nicht zuletzt der plötzliche Aufwind für die Digitalisierung in ganz unterschiedlichen Lebensbereichen spiegelt sich auch im Tätigkeitsbericht wider. Dagmar Hartge:

Es steht außer Frage, dass während einer Pandemie pragmatische Lösungen gefragt sind, um Gesellschaft, Wirtschaft und Staat weiterhin am Laufen zu halten. Gleichzeitig erwarten Bürgerinnen und Bürger, dass ihr Grundrecht auf Datenschutz gewahrt bleibt. Die Ergebnisse zahlreicher Beschwerden und Beratungen aus dem vergangenen Jahr zeigen mir, dass sich dieser Spagat lohnt. Den Datenschutz von vornherein in die Lösungen einzubeziehen, verhindert zudem aufwendige Nachbesserungen.

Während derzeit vor allem die digitalen Instrumente zur Nachverfolgung von Kontakten diskutiert werden, stand im vergangenen Frühjahr und Sommer die analoge Erhebung von Kontaktdaten im Vordergrund. Zahlreiche Besucherinnen und Besucher beschwerten sich über offen ausliegende **Corona-Gästelisten**. Die Ergebnisse einer Kontrolle in über 50 brandenburgischen Gaststättenbetrieben waren ernüchternd: In 30 Fällen wurden mehr Daten erhoben, als dies vorgeschrieben war und in 36 Fällen haben Cafés und Restaurants die Löschfrist nicht oder nicht rechtzeitig umgesetzt. In Einzelfällen nutzten Betriebe die erhobenen Kontaktdaten vorschriftswidrig für eigene Werbezwecke (A I 2, Seite 16). Unverhältnismäßig war die Verwendung von Gästelisten zur Verfolgung von Ordnungswidrigkeiten, die mit der Eindämmung der Pandemie nichts zu tun hatten. Konkret ging es um die Nutzung der Kontaktdaten für die Verhängung eines Verwarngeldes auf der Grundlage des Waldgesetzes des Landes Brandenburg. Anlass war eine Geburtstagsfeier mit 50 Gästen im Wald (A I 3, Seite 18).

Grundlage für die Erfassung der Kontaktdaten von Gästen waren die verschiedenen **Corona-Verordnungen der Landesregierung**. Die Landesbeauftragte hat sich frühzeitig dafür eingesetzt, dass diese dem Grundsatz der Datensparsamkeit Rechnung trugen. So hat sie beispielsweise empfohlen, auf den Begriff der „Anwesenheitsliste“ zu Gunsten des „Anwesenheitsnachweises“ zu verzichten, um klarzustellen, dass die Datenerfassung auf einzelnen Blättern erfolgte. Dadurch konnte der Einblick Unbefugter leichter verhindert und die Löschfristen für die erfassten Daten überhaupt erst umgesetzt werden. Das Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz hat diesen Rat umgesetzt und in der Verordnung zudem klargestellt, dass die Anwesenheitsnachweise ausschließlich zum Zweck der Auskunftserteilung gegenüber dem Gesundheitsamt zu nutzen sind (A I 1, Seite 14).

Die Herausforderung, **schulischen Distanzunterricht** von heute auf morgen umzusetzen, traf die meisten Schulen völlig unvorbereitet. Schulträger und Lehrkräfte mussten improvisieren und die Schülerinnen und Schüler sowie deren Eltern waren fast täglich mit neuen Herausforderungen konfrontiert. Manche Schulen nutzten Cloud-Lösungen von Microsoft, um den Unterricht unter Pandemiebedingungen aufrechtzuerhalten. Daran hielten sie teilweise auch dann noch fest, nachdem es in einigen Fällen zu einer gravierenden Datenschutzverletzung gekommen war. Im Ergebnis hielt die Landesbeauftragte dies nicht für zulässig. Weder war es Schülerinnen und Schülern bzw. Lehrkräften möglich, der Verarbeitung ihrer personenbezogenen Daten zuzustimmen – einer Einwilligung hätte es an der Freiwilligkeit und Informiertheit gemangelt. Noch konnten die verantwortlichen Stellen den erforderlichen datenschutzkonformen Vertrag mit dem Dienstleiser zur Auftragsverarbeitung nachweisen. Völlig unklar war zudem, welche Daten an den Hersteller übermittelt wurden und was Microsoft mit ihnen vorhatte (A IV 5, Seite 72). Dagmar Hartge:

Aus meiner Sicht gibt es keinen Grund, auf kommerzielle Lernplattformen zu setzen, die nicht in zulässiger Weise eingesetzt werden können. Mit der Schul-Cloud Brandenburg besteht schließlich eine flächendeckende und datenschutzgerechte Alternative. Ich kann an alle Schulen, die daran noch nicht teilnehmen, nur appellieren, dieses Angebot zu nutzen.

Die Notwendigkeit, persönliche Kontakte zu reduzieren, führte im Berichtszeitraum zu einer ungeahnten Konjunktur von **Videokonferenzen**. Neben Beschwerden über den Einsatz bestimmter Produkte erreichten uns auch zahlreiche Beratungsersuchen. Viele erwarteten von der Landesbeauftragten konkrete Produktempfehlungen, die gar nicht zu unseren Aufgaben gehören. Die Landesbeauftragte hat sich jedoch an der Erarbeitung einer Orientierungshilfe der Datenschutzkonferenz zur Nutzung von Videokonferenzsystemen beteiligt. Im Ergebnis sind solche Lösungen zu empfehlen, die auf der eigenen, bereits vorhandenen IT-Infrastruktur basieren. Die Beauftragung eines Dienstleisters ist zwar auch möglich, hier sollten aber nur Anbieter mit Sitz in Europa ausgewählt werden. Die Vorschriften zur Auftragsdatenverarbeitung sind dabei zu beachten. Einfach im Internet zugängliche Videokonferenzdienste sind aus datenschutzrechtlicher Sicht zumeist kritisch zu bewerten. In jedem Fall bleibt die jeweilige Stelle für die Einhaltung des Datenschutzes verantwortlich und muss diese vor dem Einsatz der Programme sicherstellen und dokumentieren. (A I 6, Seite 26). In diesem Sinne hat die Landesbeauftragte auch die staatlichen **Universitäten und Fachhochschulen** des Landes Brandenburg beraten, nachdem sie sich dort im Rahmen einer Umfrage einen Überblick über die eingesetzten Programme für die Online-Lehre verschafft hatte. Wir werden in diesem Jahr überprüfen, inwieweit die Hochschulen unserem Rat gefolgt sind (A I 7, Seite 28).

Der Europäische Gerichtshof hat erneut die Weichen für eine stärkere Berücksichtigung des europäischen Datenschutzes im Rahmen der internationalen Datenverarbeitung gestellt. Mit dem **„Schrems-II-Urteil“** erklärte er eine entscheidende Grundlage für die Datenübermittlung in die USA – das EU-US-Privacy-Shield – für ungültig. Wenn der nach dem Unionsrecht erforderliche Schutz der Daten nicht gewährleistet werden kann, muss ihre Übermittlung beendet werden. Anderenfalls sind wir als Aufsichtsbehörde nach dem Urteil des Europäischen Gerichtshofs verpflichtet, die Übermittlung zu untersagen. Unternehmen und Vereine stehen dadurch vor großen Herausforderungen. Die Landesbeauftragte hat im Berichtszeitraum viele von ihnen beraten (A V 2, Seite 106). Die Auswirkungen des Urteils waren auch Gegenstand ihrer Beratungen der Schulen und Hochschulen im Zusammenhang mit dem Einsatz von Lernplattformen und Videokonferenzsystemen.

Befasst war die Landesbeauftragte noch mit vielen weiteren pandemiebezogenen Sachverhalten. Beispielsweise haben wir ein gemeinnütziges Unternehmen bei der **Entwicklung cloudbasierter Gesundheitsanwendungen** beraten. Dabei ging es um die Erfassung von Anamnesedaten bei der Patientenaufnahme im Zusammenhang mit Corona sowie um die Entwicklung eines Symptomtagebuchs (A I 4, Seite 20). Um Unternehmen und Behörden bei der datenschutzgerechten Umsetzung von **Heimarbeit** zu unterstützen, haben wir die wichtigsten Anforderungen sowie die daraus resultierenden technischen und organisatorischen Maßnahmen zur Verarbeitung personenbezogener Daten im Rahmen der Heimarbeit in einer Handreichung zusammengefasst und veröffentlicht (A I 5, Seite 22). Gegenüber der Investitionsbank sprach die Landesbeauftragte eine Verwarnung aus, weil diese bei der Umsetzung des Verfahrens zur **Antragstellung für Corona-Soforthilfen** keine ausreichende Verschlüsselung der E-Mail-Kommunikation eingesetzt, teilweise nicht erforderliche Daten erhoben und zudem nur mangelhaft über die Datenverarbeitung informiert hatte (A II 3, Seite 40).

Wie in allen Jahren zuvor war auch im Berichtszeitraum die **Videoüberwachung** wieder ein Dauerbrenner des Datenschutzes. Die Zahl der schriftlichen Anfragen und Beschwerden hierüber stieg von 42 im Jahr 2014 auf 190 im Jahr 2020. Auch die Anzahl der von uns überprüften Kameras nahm erneut zu (A VI 2, Seite 113). Eine besondere Aufmerksamkeit verschaffte dem Thema die Staatskanzlei des Landes Brandenburg. Im Rahmen der vierwöchigen **EinheitsEXPO** anlässlich des 30. Jahrestages der Deutschen Einheit ließ sie mehrere Exponate in der Potsdamer Innenstadt zum Schutz gegen Zerstörung und zur Durchsetzung des pandemiebedingten Abstandsgebots durch Videokameras überwachen. Während ein Nachtbetrieb der Kameras durchaus zulässig gewesen wäre, hat die Staatskanzlei die Kameras vorwiegend ganztägig und unter Beobachtung weiträumiger Flächen eingesetzt. Eine ausreichende Beschilderung, die darauf hingewiesen hätte, gab es zunächst nicht. Auch fehlte eine Dokumentation, aus der die Begründung für die Videoüberwachung ebenso wie die technischen Maßnahmen zur datenschutzrechtlichen Absicherung des Kameraeinsatzes hätte hervorgehen müssen. Maßgaben der Datenschutzaufsichtsbehörde ignorierte die Staatskanzlei oder setzte sie nur halbherzig um. Im Ergebnis sprach die Landesbeauftragte eine Verwarnung aus. Anstatt der Videoüberwachung hätte es weniger eingriffsintensive Mittel gegeben. Den schutzwürdigen Interessen der von den Kameras erfassten Bürgerinnen und Bürger kam ein höheres Gewicht zu (A II 2, Seite 37).

Dass Kameras nicht nur als fest installierte Technik in Erscheinung treten, zeigte der Fall eines **Drohneneinsatzes durch ein Immobilienunternehmen**. Zur besseren Vermarktung eines Grundstückes ließ es Drohnen über die Nachbarschaft fliegen und Luftaufnahmen fertigen. Auf den Bildern, die das Unternehmen in seinem Internetangebot veröffentlichte, waren auch die angrenzenden Grundstücke zu sehen – private Gärten und Sonnenterassen der Nachbarn inklusive. Bereits luftverkehrsrechtlich war ein solcher Drohneneinsatz mit Kameras unzulässig. Auch datenschutzrechtlich war er nicht erforderlich und griff in unzulässiger Weise in die Rechte der Nachbarn ein. Das Unternehmen löschte die Aufnahmen freiwillig von seiner Webseite. Die Landesbeauftragte erteilte daher lediglich einen förmlichen rechtlichen Hinweis, um die Rechtslage zu verdeutlichen (A IV 3, Seite 67).

Im Rahmen der Umsetzung des im Berichtszeitraum in Kraft getretenen Masernschutzgesetzes kam es zu zahlreichen Beschwerden. Das Gesetz sieht unter anderem vor, dass Schülerinnen und Schüler den Nachweis über einen ausreichenden **Impfschutz gegen Masern** erbringen müssen. In der Praxis wurden zu diesem Zweck teilweise Kopien der Impfausweise einfach zur Schülerakte genommen. Eine solche Datenspeicherung ist unzulässig, der Datenumfang der Nachweise geht in der Regel über das erforderliche Maß hinaus. Vor dem Hintergrund vieler Beschwerden und Anfragen haben wir die

staatlichen Schulämter bei der Erarbeitung entsprechender Hinweise für die Schulen unterstützt (A IV 1, Seite 64).

Eines der wichtigsten Betroffenenrechte, das die Datenschutz-Grundverordnung enthält, ist das **Recht auf Auskunft** über die Verarbeitung von Daten zur eigenen Person. Es ist unverzichtbare Voraussetzung für die Ausübung weiterer Ansprüche wie beispielsweise des Rechts auf Berichtigung, Löschung oder Widerspruch. Ein Beschwerdeführer hatte sich zunächst erfolglos gegenüber einem Inkassodienstleister um eine Auskunft zu den über ihn gespeicherten Daten bemüht. Nach unserer Intervention stellte sich heraus, dass das Unternehmen davon ausgegangen war, es hätte sich um den Wunsch nach einer Bonitätsauskunft gehandelt, die mangels Bonitätsbeurteilung des Betroffenen nicht erteilt werden konnte. Erst als man in einem ganz anderen Unternehmensbereich suchte, fanden sich doch noch Daten des Antragstellers, nämlich solche aus einem Inkassoverfahren. Die Auskunft wurde schließlich erteilt und das Unternehmen sagte zu, alle Beschäftigten zu dieser Thematik zu schulen (A II 6, Seite 45). In einem anderen Fall hat die Landesbeauftragte hingegen eine Warnung gegenüber einem Autovermieter ausgesprochen. Dieser verweigerte einem Autofahrer, dem es als Ersatz für einen Unfallwagen von sich aus ein Mietfahrzeug angeboten hatte, die Auskunft über die Herkunft seiner Daten. Es begründete dies ohne weitere Rückfrage mit der nicht nachgewiesenen Bevollmächtigung des in der Sache tätigen Rechtsanwalts des Autofahrers (A II 7, Seite 47).

Dass es nicht genügt, die internen Rechnersysteme zu schützen, zeigte der Fall einer überregional tätigen Hilfs- und Wohlfahrtsorganisation, deren Website sich als Einfallstor in deren Datenbanken herausstellte. Der Grund lag in einer **Sicherheitslücke im Content-Management-System**, die den unbefugten Angriff ermöglichte. Die Datenbank beinhaltete personenbezogene Daten, die über ein Anmeldeformular des Internetangebots erfasst worden waren. Die Zahl der von dem unerlaubten Zugriff betroffenen personenbezogenen Daten ging in die Hunderttausende, teilweise enthielten sie auch Angaben zum Gesundheitszustand. Die komplizierte Organisationsstruktur der Einrichtung sowie die Beauftragung externer Dienstleister erschwerte die Aufklärung der Angelegenheit erheblich. Die Landesbeauftragte prüft derzeit die Einleitung eines Ordnungswidrigkeitenverfahrens (A IV 6, Seite 76).

Ähnlich intensiv wie mit Auskunftserteilungen hat sich die Landesbeauftragte im Berichtszeitraum mit der datenschutzgerechten Nutzung der E-Mail-Kommunikation befasst. In ihrem Tätigkeitsbericht schildert sie exemplarisch drei Fälle, in denen die IT-Systeme von Unternehmen durch **Schad- und Erpessersoftware** befallen wurden. Jedes Mal waren nicht ausreichende technische und organisatorische Schutzmaßnahmen Ursache der Infektionen und damit der Verletzungen des Datenschutzes. Wichtig ist auch die Sensibilisierung der Beschäftigten, kritisch mit E-Mail-Anhängen oder in E-Mails versandten Internetlinks umzugehen (A IV 9.1, Seite 82). Auch der **Versand unverschlüsselter E?Mails** wird uns häufig als Meldung einer Datenschutzverletzung angezeigt – vor allem dann, wenn die Nachricht an die falsche Adresse versandt wurde und sensitive Informationen enthielt. Im Berichtszeitraum hat die Landesbeauftragte die brandenburgischen Jugendämter anlässlich entsprechender Hinweise aufgefordert, für die Übermittlung besonders schutzbedürftiger Sozialdaten eine Ende-zu-Ende-Verschlüsselung zu nutzen. In unserem Rundschreiben haben wir konkrete Hilfestellungen erläutert und empfohlen, Schulungen zur Sensibilisierung der Beschäftigten durchzuführen (A IV 9.3, Seite 86). Ebenso häufig wie der Fehlversand von E-Mails kommt der **Versand mit offenen Verteilern** vor. Die Gefahr besteht hier nicht so sehr in den besonders sensitiven Daten, sondern vielmehr in der unter Umständen sehr hohen Zahl betroffener Personen. Wir raten dazu, die unüberlegte Nutzung der CC-Funktion bereits im Vorfeld zu erschweren, beispielsweise durch eine in das E?Mail-Programm implementierte Warnmeldung oder

durch die Gewährleistung eines Vier-Augen-Prinzips in Abhängigkeit von der Größe des Empfängerkreises (A IV 9.2, Seite 84).

Erfreuliches gibt es zum **Verfahren der automatisierten Kennzeichenerfassung KESY** auf brandenburgischen Autobahnen zu berichten. Die im Zusammenhang mit Ermittlungsverfahren bis Juni 2019 (Altdaten) gespeicherten Kennzeichen sind letztendlich gelöscht worden. Darüber hinaus hat das Polizeipräsidium eine Reihe von Maßnahmen getroffen, um eine Akkumulation von Kennzeichendaten und deren Nutzung künftig einzuschränken (B 2.2, Seite 128). Die Weiterentwicklung des Verfahrens ist mit einer umfassenden Neukonzeption verbunden. Es berücksichtigt wesentliche Forderungen der Landesbeauftragten hinsichtlich der Datentrennung und Datenlöschung sowie differenzierter Zugriffsrechte. Gleichwohl stand die Vorlage des Sicherheitskonzepts sowie einer überarbeiteten Fassung der von uns im ersten Entwurf bemängelten Datenschutz-Folgenabschätzung zum Jahresende noch aus (B 2.3, Seite 131). Ungeachtet dessen fehlt unseres Erachtens jedoch von Anfang an eine Rechtsgrundlage für die automatisierte Kennzeichenerfassung im Aufzeichnungsmodus.

Vor diesem Hintergrund hat die Bundesregierung eine gesetzliche Regelung für die Kennzeichenfahndung für das Strafverfahren vorgeschlagen. Sie wollte damit das Verfahren in verhältnismäßiger Weise auf den Fahndungsmodus (Speicherung nur der Treffer) beschränken. Der Gesetzentwurf wird im Bundestag und Bundesrat diskutiert. In der Länderkammer setzte sich die Landesregierung jedoch noch einmal für eine Vorschrift ein, welche die weitere Aufzeichnung aller vorbeifahrenden Fahrzeuge erlaubt. Dagmar Hartge:

Ich bin weiterhin der Auffassung, dass ein dauerhafter Betrieb der automatisierten Kennzeichenfahndung im Aufzeichnungsmodus einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt. Ob das Gesetzgebungsverfahren auf Bundesebene zu demselben Ergebnis kommt, wird sich zeigen. In jedem Fall braucht es endlich Rechtssicherheit.

Seit dem 1. Januar 2021 sind die gesetzlichen Krankenkassen verpflichtet, den Versicherten eine **elektronische Patientenakte** anzubieten. Das Patientendaten-Schutz-Gesetz regelt die Umsetzung dieses Vorhabens und wurde im Berichtszeitraum vom Deutschen Bundestag verabschiedet, ohne die Kritik der Datenschützer und auch des Bundesrates zu berücksichtigen. Im Kern geht es u. a. darum, dass die Patientinnen und Patienten in der ersten Umsetzungsphase vor die Entscheidung gestellt werden, entweder allen Behandelnden alle elektronischen Dokumente zur Kenntnis zu geben oder gar keine. Hier bedarf es einer Möglichkeit, differenzierte Zugriffsrechte zu vergeben. Die Landesbeauftragte hat gegenüber beiden ihrer Aufsicht unterstehenden Krankenkassen noch vor Jahresfrist eine Warnung bezüglich des Berechtigungsmanagements ausgesprochen (A II 1, Seite 34).

Ein weiteres Vorhaben, das auf Bundesebene entschieden wurde, aber erhebliche Auswirkungen auch im Land Brandenburg haben wird, ist das **Registermodernisierungsgesetz**. Mit diesem Gesetz wird die Steuer-Identifikationsnummer als ein übergreifendes Ordnungsmerkmal für besonders relevante Register eingeführt, um digitale Verwaltungsdienstleistungen bürgerfreundlich anbieten zu können. Angesichts ihres breiten Einsatzbereichs ist die Identifikationsnummer nichts anderes als eine Personenkennziffer, deren Unzulässigkeit das Bundesverfassungsgericht bereits in seinem Volkszählungsurteil festgestellt hatte. Auch der Bundesfinanzhof hat in einer späteren Entscheidung die Zweckbindung der Steuer-Identifikationsnummer für ausschließlich steuerliche Zwecke betont. Verbesserungs- und Alternativvorschläge der Datenschutzkonferenz drangen im Ergebnis nicht durch. Der Deutsche

Bundestag hat das Gesetz im Berichtszeitraum verabschiedet. Wir haben uns auf Arbeitsebene bis zum Schluss für eine datenschutzkonforme Registermodernisierung eingesetzt (A V 1.1, Seite 92).

Insgesamt haben die Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten im zurückliegenden Jahr 1.322 **Beschwerden** natürlicher Personen bearbeitet – im Vorjahr waren es noch 878 (A VI 1, Seite 112). Auch die Zahl der **Beratungen** von Privatpersonen, Verwaltungen und Unternehmen ist im Jahresvergleich um mehr als 50 % gestiegen (A VI 3, Seite 115). Während wir im Jahr 2019 noch 362 **Meldungen von Datenschutzverletzungen** zu bearbeiten hatten, erhielten wir im Berichtszeitraum bereits 409 solcher Meldungen (A VI 4, Seite 115). Mehr als die Hälfte davon betraf den Fehlversand von Unterlagen. Der relativ hohe Anteil technischer Mängel, die Grund für eine Meldung waren, zeigt, dass Unternehmen und Verwaltungen weiterhin gefordert sind, technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen und aktuell zu halten, um beispielsweise digitale Angriffe abzuwehren. In 37 Fällen machte die Landesbeauftragte von Befugnissen wie Warnungen, Verwarnungen oder Anordnungen Gebrauch (A VI 5.1, Seite 118). Dagmar Hartge:

Der erneut gestiegene Umfang von Beschwerden und Beratungen verdeutlicht, dass die Bürgerinnen und Bürgern ihr Grundrecht auf Datenschutz in Pandemiezeiten sehr bewusst einfordern. Gleichzeitig führt der damit verbundene Arbeitsaufwand vor Augen, dass meine Behörde im zurückliegenden Jahr an den Rand der Leistungsfähigkeit gelangt ist. Die Priorisierung der Fälle hat dazu geführt, dass immer mehr Beschwerdeführerinnen und Beschwerdeführer deutlich länger auf eine Antwort warten müssen. Dass wir die Arbeit trotz der organisatorischen Herausforderungen durch die coronabedingten Einschränkungen stemmen konnten, ist das Ergebnis des Engagements meiner Mitarbeiterinnen und Mitarbeiter. Sie haben in vielen Arbeitsbereichen inzwischen ihre Belastungsgrenze erreicht. Ihnen möchte ich an dieser Stelle ausdrücklich danken.

Die Zahl der **Ordnungswidrigkeitenverfahren** stieg im Berichtszeitraum von 47 auf 70 (A VI 5.2, Seite 119, sowie A II 8, Seite 49). Der größte Anteil wurde von den zuständigen Polizeibehörden oder Staatsanwaltschaften an die Bußgeldstelle der Landesbeauftragten weitergeleitet. In 16 Fällen verhängte die Landesbeauftragte ein Bußgeld; die Gesamtsumme der festgesetzten Bußgelder betrug 331.200 Euro. Beispielsweise hatte die Betreiberin einer Ballettschule Bilder minderjähriger Tanzschülerinnen ohne eine vorherige schriftliche Einwilligung im Internet veröffentlicht. In einem anderen Fall nutzte eine Arzthelferin die in der Praxis hinterlegte Telefonnummer eines Patienten zum Zweck einer privaten Kontaktaufnahme – eine Vorgehensweise, die nicht nur der Ehefrau des Betroffenen missfiel. Private Neugier motivierte schließlich einen Polizeibediensteten, sich über dienstliche Informationssysteme nach den Daten eines prominenten Potsdamers zu erkundigen.

Die Landesbeauftragte, Dagmar Hartge, hat ihren Tätigkeitsbericht heute der Präsidentin des Landtages Brandenburg, Prof. Dr. Ulrike Liedtke, überreicht.

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