www.datenschutzzentrum.de

Landesbeauftragte für Datenschutz Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Frau Hansen
Durchwahl: 988-200

Kiel, 24. Mai 2019

# PRESSEMITTEILUNG

**Datenschutz und Informationsfreiheit in Schleswig-Holstein: hart am Wind**
**– Landesbeauftragte für Datenschutz stellt Tätigkeitsbericht 2019 vor –**

Einen Tag vor dem ersten Geburtstag der Datenschutz-Grundverordnung legt die **Landesbeauftragte für Datenschutz Schleswig-Holstein Marit Hansen** ihren Tätigkeitsbericht für die Jahre 2017 und 2018 vor. Der Berichtszeitraum war geprägt von der europäischen **Datenschutzreform**, die zu Veränderungen der gesetzlichen Regelungen und damit verbunden zu Rekordzahlen an Beschwerden und Nachfragen führte. Ebenfalls zunehmend nachgefragt wurden Hilfen im Bereich **Informationsfreiheit**, wenn Bürgerinnen und Bürger ihr Recht wahrnehmen wollen, Zugang zu Daten der Verwaltung zu erlangen, und dabei öffentliche und private Interessen abgewogen werden müssen.

Hansen, die das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) leitet, zieht ihr Resümee über die Arbeit der letzten zwei Jahre: „Datenschutz und Informationsfreiheit voranzubringen, bedeutet, **hart am Wind zu segeln und den Widrigkeiten zu trotzen**, die es uns schwer machen, unseren gesetzlichen Auftrag vorbildlich zu erfüllen. Mit der Einführung der Datenschutz-Grundverordnung haben sich die Pflichten der Verarbeiter zwar vergleichsweise wenig geändert, das Thema ist nun aber verstärkt ins Bewusstsein von Datenverarbeitern und den Menschen gerückt, um deren Daten es geht. Wir hatten alle Hände voll zu tun, um Irrtümer richtigzustellen, Mythen zu entzaubern und vor allem Hinweise zu geben, wie sich die **Datenschutzanforderungen praktisch umsetzen** lassen. All dies natürlich, ohne das Tagesgeschäft zu vernachlässigen. Jeden Tag kommen Beschwerden an, denen wir nachgehen müssen, und fast täglich melden uns Behörden und Unternehmen Datenpannen."

Drei Problembereiche macht Hansen aus, die zu den Widrigkeiten beitragen:

1. Viele der Datenschutzanforderungen bedürfen einer Konkretisierung. **Gerichtliche Prozesse** zu Datenschutzfragen, die grundlegend für ganz Europa sind, können allerdings Jahre oder **Jahrzehnte dauern**. Zum einen sollten in solchen Fällen die wichtigen Fragen schneller dem Europäischen Gerichtshof als höchste Instanz vorgelegt werden, um eine verbindliche Klärung herbeizuführen. Zum anderen sollten **Standardisierungsinitiativen** die Anforderung des eingebauten Datenschutzes in ihren Best Practices und Standards im Bereich der Informationstechnik einfließen lassen.

   Fanpage-Entscheidung, Textziffer 7.1, S. 139

2. Insbesondere große internationale Anbieter von Produkten oder Diensten behaupten oft nur, dass sie Datenschutzanforderungen umsetzen, doch die Realität sieht anders aus. Die Hersteller sind außerdem nicht unmittelbar zur Datenschutz-Compliance verpflichtet. Die Anwender aus Behörden und Unternehmen müssen stärker **von ihren Dienstleistern Datenschutzgarantien und die notwendige Dokumentation einfordern**, da sie sonst ihre eigene Rechenschaftspflicht nicht erfüllen können.

   Datenschutz durch Gestaltung, Textziffer 2.3, S. 24

3. Die **Datenschutzaufsichtsbehörden** können nur im Rahmen der ihnen zur Verfügung stehenden Ressourcen tätig werden. Gerade im wichtigen Bereich der Digitalisierung sind sie als Korrektiv zu Fehlentwicklungen in der Verarbeitung von Daten notwendig. Eine effektive Wahrnehmung dieser Funktion im Sinne der Rechte und Freiheiten der Menschen erfordert jedoch eine **angemessene personelle und finanzielle Ausstattung**.

   Dienststelle, Textziffer 1.2, S. 11

Insgesamt sieht Hansen einen Silberstreif am Horizont: „Die Datenschutz-Grundverordnung hat im letzten Jahr **aufgerüttelt**, ein Großteil der Verantwortlichen aus Verwaltung und Wirtschaft hat sich selbst überprüft, die eigenen Datenverarbeitungsprozesse geordnet und die **Datenschutzmaßnahmen verbessert**. Der Weckruf aus 2018 darf aber nicht verhallen, sondern wichtig ist nun ein stetiges Anpassen an neue Risiken und an neue Schutzmöglichkeiten. Die Vielzahl der berechtigten Beschwerden, der deutliche Zuwachs an Meldungen von Datenpannen und die Ergebnisse unserer Kontrollen zeigen, dass dies alles kein Selbstgänger ist. Einen hohen Stellenwert haben **die behördlichen und betrieblichen Datenschutzbeauftragten**, die Kontrolleure und Ansprechpartner vor Ort sind. Alles in allem bin ich hoffnungsvoll, dass wir mit der europäischen Harmonisierung im Datenschutz nun die Hebel in die Hand bekommen haben, um die **weiterhin notwendigen Änderungen im Umgang mit personenbezogenen Daten** zu erreichen. Dies dient nicht nur den Grundrechten jedes einzelnen Menschen, sondern auch unserer demokratischen Gesellschaft in der zunehmend digitalisierten Welt. Die Digitalisierungsinitiativen in Schleswig-Holstein mögen hier mit gutem Beispiel vorangehen."

Der Tätigkeitsbericht 2019 ist abrufbar unter: **https://uldsh.de/tb37**

Bei Nachfragen wenden Sie sich bitte an:

Landesbeauftragte für Datenschutz
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstraße 98, 24103 Kiel
Tel.: 0431 988-1200, Fax: -1223
E-Mail: mail@datenschutzzentrum.de
Internet: www.datenschutzzentrum.de

**Der Tätigkeitsbericht 2019 des ULD – ausgewählte Ergebnisse**

Der diesjährige Tätigkeitsbericht des ULD beschreibt auf 200 Seiten aktuelle Entwicklungen und relevante Einzelfälle. Einige Beispiele werden im Folgenden genannt:

Zu den Aufgaben des ULD gehören anlassbezogene und anlasslose Prüfungen, um Datenschutzverstöße festzustellen und Hinweise zur Datenschutz-Compliance zu geben. Branchenprüfungen sind besonders wichtig, um die Prüfkriterien in vergleichbaren Verarbeitungssituationen anzuwenden und strukturelle Unzulänglichkeiten einer gesamten Branche aufspüren zu können. Anlass für die Branchenprüfung von **Sportverbänden zum Umgang mit Sportlerdaten** waren Beschwerden von Eltern zu den Spielerpässen ihrer mittlerweile aus dem Verein ausgetretenen Kinder, deren Daten angeblich dauerhaft zu speichern waren. Auch Fotos auf Webseiten ohne Information und Einwilligung waren Gegenstand der Prüfung. Die Landesverbände der verschiedenen Sportarten waren überwiegend kooperativ und passten im Laufe der Prüfung ihre Satzungen und Datenverarbeitungen an. Jedoch bestehen weitere Probleme durch Vorgaben einiger übergeordneter Bundesverbände; die zuständigen Aufsichtsbehörden wurden unterrichtet.

Textziffer 5.4.17, S. 105

Für Profi-Sportler: Datenschutz bei Dopingkontrollen, Textziffer 8.3.2, S. 150

Eine Pflichtaufgabe ist die **Prüfung des Datenschutzes in der Verarbeitung der Polizei und des Verfassungsschutzes**. So muss das ULD beispielsweise Speicherungen in bestimmten Informationssystemen, die Zugriffe darauf und bestimmte verdeckte Ermittlungsmaßnahmen alle zwei Jahre prüfen. Im Berichtszeitraum wurden die sog. „Antiterrordatei“ und die „Rechtsextremismus-Datei“ geprüft, die wenig Grund zur Beanstandung lieferten. Dass dies nicht immer so ist, zeigt der Umgang mit der bereits im vorherigen Berichtszeitraum geprüften „Falldatei Rauschgift“. Als Ergebnis unserer Prüfung wurden mehr als 15.000 Fälle – etwa 75 % des Gesamtdatenbestands – gelöscht, weil sie die Voraussetzungen für eine Speicherung nicht oder nicht mehr erfüllten.

Textziffer 4.2.1, S. 51

Den Pilotversuch der Landespolizei zu **Bodycams** (Körperkameras) wird vom ULD begleitet. Auch wenn er noch nicht ganz abgeschlossen ist, hat das ULD bereits wesentliche Erkenntnisse gewonnen, die im Falle eines weiteren Betriebs der Bodycams in die gesetzlichen Regelungen einfließen sollten, damit der Einsatz rechtssicher und überprüfbar ist.

Textziffer 4.2.3, S. 53

Ebenfalls mit Bildaufnahmen hatte der Fall zu tun, in dem eine Mitarbeiterin der Ausländerbehörde abends einen ausländischen EU-Bürger aufsuchte und seinen **Reisepass fotografierte – und zwar mit ihrem Privathandy**. Weder gab es eine Berechtigung für die Vollerhebung der Daten auf dem Pass noch hätten Daten auf einem Privatgerät gespeichert werden dürfen, bei dem mögliche Datenabflüsse – z. B. bei einer Synchronisation in einer Cloud – nicht ausgeschlossen sind.

Textziffer 4.4.2, S. 69

Um Geld ging es in dem Fall, in dem eine Gemeinde gemäß ihrer **Kurabgabesatzung von den ortsansässigen Kurkliniken** verlangte, die **Patientennamen** und die Dauer des Aufenthalts zu übermitteln. Die Kliniken verweigerten dies mit Hinweis auf die ärztliche Schweigepflicht – zu Recht. Kliniken und Krankenhäuser gehören nicht zu Betrieben des Beherbergungsgewerbes. Ein Arzt, der die Namen von Patienten weitergäbe, liefe Gefahr, sich strafbar zu machen.

Textziffer 4.6.4, S. 79

Auch die Erhebung der Gemeinden von **Zweitwohnungssteuern** war Gegenstand von mehreren Beschwerden. Hier wurden von den Steuerpflichtigen übermäßig viele Daten aus der Steuererklärung abverlangt, wo auch **teilgeschwärzte Unterlagen** oder andere Nachweise über die Dauervermietung einer Wohnung ausgereicht hätten. Die betroffenen Gemeinden müssen ihre Satzungen und Fragebögen an die Rechtslage anpassen und zudem die Informationspflichten der DSGVO umsetzen.

Textziffer 4.8.3, S. 83

Mehrere **Hundehalter** beschwerten sich darüber, dass ihre Stadt sie dazu verpflichtete, ihren Namen und ihre Anschrift deutlich sichtbar an der „Anleinvorrichtung“ anzubringen. Es handelte sich um die Auslegung des Hundegesetzes, das am 1. Januar 2016 in Kraft getreten war. Mit Intervention des ULD konnte erreicht werden, dass Name und Adresse nicht öffentlich sichtbar sein müssen. Da Hunde ohnehin gemäß Hundegesetz ab dem Alter von drei Monaten gechippt und registriert werden müssen, ist aber fraglich, welchen Sinn diese Vorschrift hat.

Textziffer 4.1.10, S. 47

Ein Dauerbrenner der Beschwerden ist die Videoüberwachung, die den öffentlichen Raum oder das eigene Grundstück betrifft. Den Fall der **Videoüberwachung im Fitnessstudio**, dort u. a. in Umkleideräumen, greift der Bericht erneut auf, da immer wieder Sportlerinnen und Sportler ähnliche Beschwerden vorbringen: Bereits im Jahr 2017 hat das ULD dem Fitnessstudio den Betrieb der Videoüberwachung in der gewählten Form untersagt. Gegen die Untersagungsverfügung hat der Betreiber Klage vor dem Verwaltungsgericht erhoben. Dort ist die Klage nun seit mehr als einem Jahr anhängig.

Textziffer 5.5.6, S. 115

Es melden sich häufig Personen, die ihre eigenen Daten im Internet gefunden haben und damit nicht einverstanden sind. Besonders verzweifelt waren Menschen, die Informationen über ihr schon vor Jahren abgeschlossenes **Insolvenzverfahren** entdeckten. Diese Daten werden häufig von Webseiten bereitgestellt, die **ohne Anbieterinformationen aus dem außereuropäischen Ausland** betrieben werden. Die betroffenen Personen hatten sich in der Zwischenzeit eine neue Existenz aufgebaut und ihren Arbeitgebern, Lebenspartnern und Bekannten nichts von der früheren Insolvenz erzählt. Das ULD konnte dabei unterstützen, die Löschung der Einträge aus den Suchmaschinen wie Google oder Bing zu erwirken. Eine Veröffentlichung dieser Informationen für eine kurze Zeitspanne ist im Insolvenzgesetz vorgesehen und wird in Deutschland zentral über ein amtliches Justizportal vorgenommen. Die Betroffenen konnten nicht damit rechnen, dass Jahre später die Daten auf ganz anderen Webseiten weiter zugänglich sind.

Textziffer 4.3.2, S. 65

Beschwerden erhielt das ULD auch, als bekannt wurde, dass mehrere Städte in der Fußgängerzone und anderen öffentlichen Bereichen die **Besucherströme messen** wollten, indem die von **Smartphones ausgesendeten technischen Daten erhoben und gespeichert** wurden (sog. Offline-Tracking). Ohne Rechtsgrundlage ist dies jedoch nicht erlaubt, die Städte sahen aufgrund der Kritik auch des ULD davon ab. Besucherströme könnte man allerdings auf andere Weise messen, z. B. mit Lichtschranken an Durchgängen. Auch könnten spezifische Apps Einwilligungen einholen oder statistische Informationen über die Besuche datenschutzfreundlich erheben.

Textziffer 5.4.8, S. 97

Tracking liegt im Trend: Das Nachverfolgen von Nutzerinnen und Nutzern nimmt immer krassere Züge an. Es sind Apps aufgetaucht, die das bei vielen Smartphones aktivierte Mikrofon verwenden, um für Menschen **nicht hörbare Ultraschallsignale** aus der Umgebung aufzufangen und zu interpretieren. Das Tracking findet damit geräteübergreifend statt (**Cross-Device Tracking**). Beispielsweise können solche Signale in Werbesendungen im Fernsehen oder in Computer-Aktivitäten eingestreut werden, die dann vom Smartphone mitgelauscht und weitergegeben werden. So sind Analysen zu Standorten, Gewohnheiten oder Interessen möglich. Dieser Möglichkeit sollte man sich bewusst sein, wenn eine App den Zugriff auf das Mikrofon verlangt.

Textziffer 10.3, S. 175

In vielen Behörden und Unternehmen werden Farblaser-Drucker oder Multifunktionsgeräte, die Kopier-, Druck- und Scan-Funktionalität vereinen, eingesetzt. Was vielen Anwendern nicht bewusst ist: Diese Geräte codieren **gelbe Mikropunkte („Yellow Dots“)** in die Farbausdrucke ein. Im IT-Labor hat das ULD die Farbausdrucke vom eigenen Multifunktionsgerät untersucht und die Marker unter Einsatz von Schwarzlicht und Mikroskop sichtbar gemacht. Nachfragen zur Rechtsgrundlage für das Einfügen dieser gerätespezifischen Punktmuster, die auch Informationen zu Datum und Uhrzeit enthalten können, konnte der Hersteller nicht zufriedenstellend beantworten. Geräte ohne „Yellow Dots“ werden kaum angeboten. Das ULD wird sich damit nicht zufriedengeben. In der Zwischenzeit informiert ein Schild am ULD-eigenen Gerät darüber, dass diese Punkte in Farbkopien enthalten sein werden und damit eine Nachverfolgung verschiedener Farbdrucke zum ULD nicht ausgeschlossen ist.

Textziffer 10.4, S. 177

Immer wieder wird Kritik laut, dass die Informationspflichten der DSGVO gar nicht handhabbar sind, weil die betroffenen Personen die notwendigen Texte ohnehin nicht verstehen können. Die DSGVO fordert aber eine Information in klarer und einfacher Sprache. Das ULD hat dazu Musterbeispiele erarbeitet und zum Abruf auf der Webseite bereitgestellt. Die mit simplen Piktogrammen illustrierten **„Datenschutz-Steckbriefe“** werden mittlerweile von mehreren Kommunen getestet. So wird es möglich, auf einen Blick die nötigen Informationen schnell zu verstehen – so wie von der DSGVO im Sinne der Transparenz verlangt.

Textziffer 6.1.4, S. 127

Leider ist **Informationssicherheit** noch lange keine Selbstverständlichkeit. Wenn es um personenbezogene Daten geht, darf dies nicht mit einem Achselzucken abgetan werden. Schließlich ist die Informationstechnik das Fundament der Informationsgesellschaft. **Meldungen zu Datenpannen** betreffen häufig Hacking-Angriffe auf Webservern oder bösartige Programme, die per E-Mail ins IT-System hineingekommen sind. Was ist aber mit gestohlenen Daten wie Konto-Namen und Passwörtern, die im Internet gehandelt werden? Zum Jahreswechsel 2018 / 2019 sind diese Datensammlungen mit dem sog. **Doxing-Skandal** ins Bewusstsein gerückt, weil viele Politikerinnen und Politiker – auch aus unserem Bundesland – betroffen waren. Das ULD beschäftigt sich nicht nur mit konkreten Maßnahmen der IT-Sicherheit, sondern ist auch an dem geförderten Forschungsprojekt „Effektive Information nach digitalem Identitätsdiebstahl“ (EIDI)“ beteiligt, damit die Betroffenen schneller erfahren, wenn sie zum **Opfer eines Datendiebstahls** geworden sind.

Textziffer 8.4, S. 151

Welche technischen und organisatorischen Sicherheitsmaßnahmen zu treffen sind, orientiert sich am Stand der Technik. Immer wieder empfiehlt das ULD Mehr-Faktor-Verfahren, beispielsweise indem nicht nur Konto-Name und Passwort abgefragt werden, sondern zusätzlich noch eine Transaktionsnummer, die beispielsweise per SMS – als gesonderter und unabhängiger Faktor – zugestellt wird. **Nicht um ein Mehr-Faktor-Verfahren** handelt es sich allerdings, wenn in einer E-Mail über unsichere Verbindungen eine passwortgeschützte Tabelle versandt wird und das Passwort, mit dem der Klartext sichtbar gemacht werden kann, gleich per nächster E-Mail auf demselben Weg folgt. Hier sei den **aufmerksamen behördlichen Datenschutzbeauftragten** gedankt, die der Vorgabe des Innenministeriums zum Verfahren nicht gedankenlos folgen wollten.

Textziffer 4.1.4, S. 38

Ein ständiges Kapitel in den Tätigkeitsberichten seit fast 20 Jahren heißt **„Gütesiegel und Audit“**. Darin werden traditionell gute Lösungen beschrieben, die sich einer genaueren Datenschutzüberprüfung unterzogen haben. Was vor knapp 20 Jahren im Kleinen als Modellprojekt in Schleswig-Holstein seinen Anfang nahm, hat es nun endlich zur europaweiten Geltung geschafft. Die DSGVO sieht Zertifizierungen als Instrument zur Auszeichnung von Datenschutz-Compliance vor. Damit ist das Ziel des Schleswig-Holsteinischen Gütesiegels als **Wegbereiter für Datenschutzzertifizierungen** erreicht. Das Schleswig-Holsteinische Gütesiegel und das Audit sind im neuen Landesdatenschutzgesetz daher nicht mehr enthalten. Es gilt die Zertifizierung nach der DSGVO. Für deren Umsetzung in die Praxis sind noch Details durch die Datenschutzaufsichtsbehörden der Mitgliedstaaten zu regeln. Hieran beteiligt das ULD sich intensiv.

Textziffer 9.1, S. 163

**Fortbildung im Datenschutz** – die neuen rechtlichen Regelungen haben in diesem Bereich einen Boom an Nachfrage ausgelöst, der leider nur teilweise mit den vorhandenen Ressourcen gestemmt werden konnte. Dennoch konnten in den Jahren 2017 und 2018 über 2.000 Teilnehmerinnen und Teilnehmer in den etablierten Kursen der DATENSCHUTZAKADEMIE und mehr als 4.600 Schülerinnen und Schüler speziell zu **Datenschutz- und Medienkompetenz** geschult werden. Das ist ganz im Sinne der DSGVO, die den Datenschutzaufsichtsbehörden die Aufgabe der Sensibilisierung der Öffentlichkeit zugeschrieben hat und sogar spezifische Maßnahmen für Kinder fordert.

Textziffer 13, S. 193