

Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

Schleswig-Holsteinischer Landtag
Innen- und Rechtsausschuss
Die Vorsitzende

per E-Mail:

innenausschuss@landtag.ltsh.de

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

Durchwahl: 988-1200

Aktenzeichen:
LD-

Kiel, 8. September 2021

Bericht des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Drucksache 19/2807

Beratung im Rahmen der 124. Sitzung des Innen- und Rechtsausschusses am 1. September 2021 (TOP 2)

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

ich bedanke mich für die Gelegenheit, in der Sitzung des Innen- und Rechtsausschusses vom 1. September 2021 mit Ihnen unseren 39. Tätigkeitsbericht für das Jahr 2020 beraten. Wie zugesagt, übersende ich hiermit den dazu verwendeten Sprechzettel.

Mit freundlichen Grüßen

gez. Marit Hansen
Landesbeauftragte für Datenschutz

Sprechzettel zur Beratung des Tätigkeitsberichts der Landesbeauftragten für Datenschutz

Ich freue mich, dass ich heute – wie auch in den vergangenen Jahren – mit Ihnen zu unserem Tätigkeitsbericht ins Gespräch kommen kann.

Alle erinnern sich noch an das Jahr 2018, als die **europäische Datenschutzreform** neue Regeln mit sich brachte: Einerseits in Form der unmittelbar anwendbaren Datenschutz-Grundverordnung (Verordnung (EU) 2016/679), andererseits die in Bundes- und Landesrecht umzusetzende europäische Richtlinie (EU) 2016/680 für den Bereich Justiz und Inneres. Dass bei einer grundlegenden Reform, die Vorgaben für *alle* EU-Staaten macht, nicht sofort alles reibungslos funktioniert, ist nicht überraschend. Das gilt im Land, im Bund, in der EU und auch im internationalen Kontext.

Allerdings hätte man für das Jahr 2020 erwartet, dass sich mittlerweile das meiste gut eingespielt hat und man der Umsetzung der Anforderungen aus Europa einen passablen Reifegrad attestieren kann. In einigen Punkten stimmt das sicherlich, aber die Anforderungen und Veränderungen, die die Corona-Pandemie mit sich brachte, haben immer wieder gezeigt, wo es hakt. Damit meine ich keinesfalls, dass die Datenschutz-Grundverordnung sich als untauglich herausgestellt hätte – im Gegenteil! Nur waren die Datenschutz-Prozesse in Unternehmen, Behörden und beim Staat noch nicht so stabil aufgesetzt und die Anforderungen nicht so verinnerlicht, wie es aus meiner Sicht nötig gewesen wäre, um schnell zu tragbaren Lösungen zu kommen, die *alle* Bedingungen – nicht nur, aber auch die Datenschutzerfordernisse – erfüllen.

Die betrifft beispielsweise die **Verpflichtung nach § 17 Abs. 4 LDSG, die Landesbeauftragte über Planungen des Landes zum Aufbau oder zu wesentlichen Änderungen von Systemen zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu informieren**. Das hat manchmal sehr gut funktioniert, oft aber auch nicht. So wurden wir einige Male völlig überrascht, wenn wir von Ministeriumsseite zu zwei Verarbeitungsalternativen befragt wurden, um dann aber ohne weitere Rückkopplung die nie vorher ins Gespräch gebrachte dritte Alternative umzusetzen. Das ist auch deswegen ungut, weil zumeist im Nachgang Presseanfragen oder Beschwerden bei uns eingehen, in denen vorausgesetzt wird, dass wir über die neue Datenverarbeitung informiert sind und ihr vielleicht sogar zugestimmt hätten.

Gerne unterstützen wir die **behördlichen Datenschutzbeauftragten**, die von den Verantwortlichen bei Datenschutzfragen einzubeziehen sind. Der Vorteil: Das konkrete Wissen ist vor Ort, es gibt weniger Berührungängste der Beschäftigten in der Behörde, und eine Rückkopplung mit meiner Dienststelle ist den behördlichen Datenschutzbeauftragten stets möglich. Nur: Im Jahr 2020 wurden sie anscheinend vielfach nicht einbezogen, obwohl sich viele Datenverarbeitungen veränderten oder neu eingeführt wurden (z. B. Homeoffice, Videokonferenzen, Verarbeitung von Gesundheitsdaten oder Kontaktdaten).

Zugegeben: Das Jahr 2020 war für alle schwierig. Einige Zeiten in dem Jahr erforderten ein schnelles Agieren, beispielsweise wenn Digitalisierungslösungen ohne den üblichen Vorlauf der Beratungen eingeführt werden mussten. Aber nach meinem Eindruck ist in Schleswig-Holstein noch nicht verinnerlicht, dass man mit den behördlichen Datenschutzbeauftragten eine wichtige Instanz vor Ort hat, deren Kompetenz es zu nutzen gilt, um Recht und Gesetz zu erfüllen und die Risiken zu beherrschen.

Seit kurzem wird uns von den Datenschutzbeauftragten vor Ort berichtet, dass sie zunehmend Angriffen ausgesetzt sind, wenn sie korrekt gemäß den rechtlichen Regelungen und der höchst-richterlichen Rechtsprechung beraten. Das verbale Eindringen auf den Datenschutz kann dann auch persönlich werden. Damit wird den behördlichen Datenschutzbeauftragten die Arbeit schwer- gemacht und engagierte Menschen werden abgeschreckt. Dabei brauchen wir doch für ein gutes Datenschutzniveau in der Fläche kompetente und motivierte behördliche und betriebliche Datenschutzbeauftragte!

Mehrere EuGH-Urteile haben im Jahr 2020 Konkretisierungen und Klarstellungen zur Auslegung des Datenschutzrechts mit sich gebracht. Am prominentesten ist das **EuGH-Urteil „Schrems II“**, das den „EU-US-Privacy Shield“ für ungültig erklärte, der vorher als Grundlage für Datenübertragungen in die USA herangezogen worden war. Das führte nicht nur zu zahlreichen Beratungsersuchen, sondern es gab auch Nachfragen der bundesweiten Presse in den verschiedenen Bundesländern bezüglich der Auswirkungen von „Schrems II“, zum Beispiel: *„Müssen die Schulen nach den Sommerferien aus Datenschutzgründen ihren Distanzunterricht auf ein anderes Videosystem umstellen?“* In Schleswig-Holstein hatte es keine Duldung gegeben, die hätte auslaufen können. Für uns war das Schrems II-Urteil keine Überraschung, auf die offensichtlichen Probleme mit dem Privacy Shield hatten wir daher auch stets in unseren Beratungen gegenüber dem Bildungsministerium und den Schulen hingewiesen. Kinderdaten sind sensibel und müssen geschützt werden.

Nicht nur in diesem Bereich, sondern generell müssen wir bei der **Digitalisierung auf Lösungen setzen, die für Rechtskonformität und digitale Souveränität** stehen. Wir beteiligen uns an der europäischen Debatte, welche technischen und organisatorischen Maßnahmen ausreichen, um die Anforderungen des EuGH umzusetzen, bzw. wo Alternativen oder Änderungen in den Produkten und Services geboten sind. Das ist die Grundlage für unsere Beratung vor Ort, denn hier brauchen wir europäisch harmonisierte Lösungen, auch als Basis für die nötigen Verhandlungen auf der Ebene der Europäischen Kommission.

Zum Tätigkeitsbericht

Wie immer finden Sie in unserem Tätigkeitsbericht eine Mischung von grundsätzlichen Themen und besonderen Einzelfällen, die zumeist nicht nur für den konkreten Sachverhalt Relevanz haben, sondern es ermöglichen, daraus Erkenntnisse mitzunehmen.

Das Jahresthema „Corona“ – so auch auf dem Titelbild des Tätigkeitsberichts visualisiert – durchzieht den Bericht (Tz. 4.1.1, 4.1.2, 4.3.2, 5.3, 5.4.1, 5.4.2, 5.4.3, 7.1, 8.1, 6.3.3):

- Maßnahmen wie Fragebögen, Temperaturmessung oder Kontaktdatenerfassung beim Einlass
- Verfahren zur Messung einer großen Personendichte
- die Corona Warn App
- Technikeinsatz und Regeln im Homeoffice, im Homeschooling und in Online-Sitzungen

Die Zahlen zu Beschwerden und Datenpannen-Meldungen sind erneut gestiegen:

- 1.219 Verfahren auf Basis von Beschwerden betroffener Personen, d. h. 27 % mehr als im Vorjahr, weiterhin ca. 1/3 im öffentlichen und 2/3 im nichtöffentlichen Bereich
- 406 Datenpannen-Meldungen, d. h. 16 % mehr als im Vorjahr
- 808 Beratungen, d. h. knapp 7 % mehr als im Vorjahr

Anmerkungen zum aktuellen Stand: Die Zahl der bis zum 31.08.2021 eingegangenen Datenpannen-Meldungen liegt bereits deutlich höher als im Jahr 2020 gesamt.

Ich hatte im vergangenen Jahr im Innen- und Rechtsausschuss herausgestellt, dass wir aufgrund der weitgehend ausgebliebenen Datenpannen-Meldungen in den Bereichen Polizei und Justiz Zweifel hatten, ob hier die Meldepflicht überhaupt bekannt war. Das hat sich größtenteils bestätigt. Die daraufhin geführten Gespräche im Bereich der Polizei haben Besserung gebracht – zwar noch nicht für 2020, aber für 2021: Es gibt nun Prozesse für die Meldung von Datenpannen. Im Bereich der Justiz ist dies etwas komplexer, weil die Meldepflicht an meine Dienststelle nicht gilt, wenn die Datenschutzverletzung bei der Ausübung justizieller Tätigkeiten erfolgte. Wir werden weiter berichten.

Zusätzlich bauen wir unseren **Prüfbereich** aus. Das war im Jahr 2020 pandemiebedingt nicht ganz einfach, weil Vor-Ort-Prüfungen ausfielen oder immer wieder verschoben werden mussten. Für den Polizeibereich besteht eine Verpflichtung zu Prüfungen durch die Datenschutzaufsichtsbehörden. Deswegen finden Sie regelmäßig unsere Berichte dazu im Tätigkeitsbericht. Die Prüfergebnisse werden zudem direkt mit den Zuständigen im Polizeibereich besprochen, um strukturelle Fragen zu lösen.

Weitere Prüfungen betrafen zum Beispiel:

- Partnervermittlungen und die von ihnen eingebundenen Werbe-Dienstleister,
- Kommunale Rechenzentren,
- Panoramaaufnahmen durch Befahrungen im Auftrag der Stadtwerke.

Fortschreiben der gesetzlichen Regelungen zu Datenschutz und Informationsfreiheit

Die Aufgaben und Befugnisse meiner Dienststelle sind insbesondere im Landesdatenschutzgesetz und im Informationszugangsgesetz festgelegt. In diesen Gesetzen haben wir einige Nachbesserungsbedarfe ausgemacht. Darin verankert sind bereits Evaluationsklauseln, d. h. wir werden gerne uns an dem Evaluationsprozess beteiligen und unsere Stellungnahmen einbringen (siehe Tz. 1.4).

Eine generelle Anmerkung, die wir bereits mehrfach in Anhörungen dieses Ausschusses vorgebracht haben: Bei allen Gesetzgebungsverfahren im Bereich Justiz und Inneres muss ebenso wie bei der Nutzung von Öffnungs- oder Spezifikationsklauseln der DSGVO das europäische Datenschutzkonzept und die dort eingeführte Terminologie berücksichtigt werden. Sonst ist fraglich, ob die europarechtlichen Vorgaben korrekt umgesetzt wurden, und es entstehen ebenso Schutzlücken wie Regelungslücken. Das deutlichste Beispiel ist die „Verarbeitung“, die nunmehr zum Oberbegriff für alle Arten der Verarbeitung geworden ist und insbesondere die auch im Landesrecht noch häufig verwendeten Begriffe „Erhebung“, „Nutzung“, „Übermittlung“ und die vormals restriktiver definierte „Verarbeitung“ einschließt. Auch Begriffe wie „pseudonymisiert“ oder „anonymisiert“ wurden früher in unserem Landesrecht teilweise in anderen Definitionen verwendet, als dies nach der Datenschutzreform der Fall ist. Mein Appell: Im Sinne der Rechtssicherheit bitte ich den Gesetzgeber, die Gesetze daraufhin zu prüfen und ggf. zu überarbeiten.

Klarheit auch bei den Corona-Regeln

Der hochdynamische Bereich der Pandemiebekämpfung und die zugrunde liegenden Gesetze und Verordnungen sind ein komplexes Thema. Wenn dies in der Praxis funktionieren soll, muss man sich konkret vor Augen führen, wie die Verpflichteten vor Ort die Anforderungen erfüllen können. Aus Datenschutzsicht stellt sich vor allem die Frage nach der Verarbeitung der Daten: Welche Daten müssen von den Verpflichteten geprüft werden, wie sind erfolgte Prüfungen zu dokumentieren, wann müssen Daten gelöscht sein? Wir bemerken auf der einen Seite einen „Viel hilft viel“-Ansatz,

bei dem die Verpflichteten aus Angst, bei etwaigen Prüfungen der Ordnungsbehörden ihr korrektes Verhalten nicht belegen zu können, (zu) viele Daten abfragen und speichern – damit verstoßen sie aber vielfach gegen das Datenminimierungsgebot des Datenschutzrechts und haben auch öfter Probleme, die Sicherheit der personenbezogenen Daten gewährleisten zu können. Auf der anderen Seite gibt es Verpflichtete, die völlig überfordert sind: sowohl von den Verpflichtungen aus Gründen des Pandemie-Schutzes als auch von Datenschutzfragen, die vorher bei ihnen gar keine Rolle spielten. **Um hier Wildwuchs und Datenschutzverletzungen zu vermeiden, sind klare Regeln und vor allem Praxishinweise erforderlich.** Wir tun seit März 2020, was wir können, um Hilfestellung zu geben, aber die Aufgabe sehe ich primär bei dem Verordnungsgeber, also den zuständigen Ministerien, die Material über ihre Webseiten zur Verfügung stellen könnten. Das wäre auch vorteilhaft für einen Praxis-Check der sich immer wieder verändernden Regeln. Dies betrifft für die nächste Zeit z. B. die etwaigen Anforderungen von 2G oder 3G am Arbeitsplatz. Hier ist natürlich auch der Bund am Zug, aber in jedem Fall stellen sich die Fragen der **Übersetzung der rechtlichen Regelungen in die Praxis.**

Vorschau auf die Jahre 2022 und 2023

Bei den länderübergreifenden Konferenzen in unseren Tätigkeitsbereichen Informationsfreiheit und Datenschutz wechselt der Vorsitz jährlich. Die Landesbeauftragte für Datenschutz wird daher in den nächsten Jahren mehr Verantwortung übernehmen, wenn Schleswig-Holstein Vorsitzland wird:

- 2022: Vorsitz der Konferenz der Informationsfreiheitsbeauftragten (IFK)
- 2023: Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Ich bedanke mich für Ihre Aufmerksamkeit und stehe Ihnen gerne jetzt und bei Bedarf zu einem späteren Zeitpunkt für Ihre Nachfragen zur Verfügung.