

Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit**1. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit nach der Europäischen Datenschutzgrundverordnung und Stellungnahme des Senats**

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 8. Mai 2019 den 1. Jahresbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit vom 27. März 2019 (Drucksache 19/2128) und in ihrer Sitzung am 15. August 2019 die dazu erfolgte Stellungnahme des Senats vom 25. Juni 2019 (Drucksache 20/3) an den Ausschuss für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Beratung und Berichterstattung.

Der Ausschuss stellte bei den nachfolgend aufgeführten Punkten des 1. Jahresberichts Beratungsbedarf fest:

- Ziffer 2 Zahlen und Fakten
- Ziffer 5 Übergreifende IT-Verfahren
- Ziffer 6 Inneres
- Ziffer 7 Justiz
- Ziffer 8 Gesundheit und Soziales
- Ziffer 10 Beschäftigtendatenschutz
- Ziffer 11 Videoüberwachung
- Ziffer 16 Internationales und Europa

In seinen Sitzungen am 13. November 2019 und 18. Dezember 2019 erörterte der Ausschuss die beratungsbedürftigen Punkte mit der Landesbeauftragten für Datenschutz und Informationsfreiheit sowie mit den Vertreterinnen und Vertretern der betroffenen Ressorts.

Der Ausschuss begrüßt, dass es in vielen Fällen, die Anlass zur Kritik gegeben haben, bereits zu einer Klärung mit den zuständigen Ressorts und Dienststellen gekommen ist beziehungsweise im Rahmen von Gesprächen zwischen den Beteiligten konstruktiv an Lösungsmöglichkeiten gearbeitet wird.

Der Ausschuss nimmt mit Blick auf Ziffer 2 des Berichts zur Kenntnis, dass sich seit Geltung der Datenschutzgrundverordnung (DSGVO) die Anzahl der bei der Landesbeauftragten monatlich eingehenden Beschwerden verdoppelt und damit der Arbeitsanfall erheblich erhöht hat. Dies liege unter anderem auch darin begründet, dass die Verantwortlichen nach der DSGVO verpflichtet seien, Datenschutzverstöße bei der Landesbeauftragten zu melden. Zusätzlich zu den bestehenden seien bei der Behörde durch die Regelungen der DSGVO weitere Aufgaben hinzugekommen, wie zum Beispiel die Akkreditierung von Zertifizierungsstellen sowie diverse Genehmigungs-, Dokumentations- und Kooperationspflichten mit anderen europäischen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss. Der Ausschuss erkennt an, dass diese Arbeitsbelastung ohne zusätzliches Personal kaum bewältigt werden kann. Durch

die neu geschaffene Möglichkeit, bei bestimmten Datenschutzverstößen Bußgelder zu verhängen, bestehe jedoch die Aussicht, weitere Stellen künftig zumindest teilweise durch eingenummene Bußgelder zu refinanzieren.

Aus dem Bereich „Übergreifende IT-Verfahren“ hat sich der Ausschuss mit der Problematik Blockchains und Datenschutz befasst (Ziffer 5.3). Auch wenn Blockchains aus Gründen der Datensicherheit gewisse Vorteile mit sich brächten, sei die Technologie aus Sicht der Betroffenen und aus datenschutzrechtlichen Gründen kritisch zu betrachten, da Daten irreversibel gespeichert würden und somit nicht gelöscht werden könnten. Der Ausschuss begrüßt daher, dass die bremische Verwaltung zurzeit keine Blockchains einsetzt und keine IT-Systeme aufbaut, die gegen die DSGVO oder andere datenschutzrechtliche Vorschriften verstoßen.

Im Hinblick auf die Gewährleistung der Sicherheit der Verarbeitung bei der Übertragung personenbezogener Daten per Fax (Ziffer 5.4) nimmt der Ausschuss zur Kenntnis, dass die Übermittlung per Fax inzwischen nicht mehr sicherer ist als diejenige per Email. Beide Verfahren nutzen heutzutage IPbasierte Telekommunikationsnetze, sodass die Sicherheitsstufe bei unverschlüsselter Übermittlung identisch sei.

Zum Themenbereich „Inneres“ begrüßt der Ausschuss, dass die bei der Kontrolle der Antiterror- und der Rechtsextremismuseinheit (Ziffer 6.1) im Einzelfall festgestellten Mängel inzwischen behoben worden sind. Die Landesdatenschutzbeauftragte kritisiert jedoch weiterhin, dass nach Ablauf der Speicherfrist keine automatisierte Löschung der Daten erfolge, sondern eine sogenannte Löschrüflliste vorliege, die manuell abgearbeitet werde. Dies könne zu Fehlern und insbesondere zu langen Bearbeitungszeiten und damit zu verzögerten Löschungen führen.

Gleiches gelte für das polizeiliche Vorgangsbearbeitungssystem (Ziffer 6.3), das ebenfalls keine automatisierte Löschung vorsehe. Dies liegt nach Aussage des Ressortvertreters darin begründet, dass es insbesondere in polizeilichen Sachverhalten häufig einer weiteren Prüfung bedürfe, ob eine Verlängerung oder Veränderung der Speicherfrist erforderlich sei. Dies könne nicht automatisiert erfolgen.

Zur unbefugten Abfrage in den polizeilichen Informationssystemen (Ziffer 6.2) nimmt der Ausschuss zur Kenntnis, dass solche Vorkommnisse polizeiintern immer überprüft und auch geahndet werden. Grundsätzlich gäbe es für alle Informationssysteme innerhalb der Polizei Berechtigungskonzepte und nicht jede Person dürfe in jedem System Abfragen tätigen. Zudem werde jede Anfrage protokolliert und sei auch revisionsfähig. Ob eine Information der Betroffenen erfolge, deren Daten abgefragt wurden, werde unterschiedlich gehandhabt. Nach der DSGVO existiere zwar eine entsprechende Informationspflicht, jedoch gelte die DSGVO nicht für den Bereich der Polizei. Hier gelte die Europäische Datenschutzrichtlinie, die Bremen aber noch nicht umgesetzt habe.

Zum Fall der unerlaubten Speicherung von Daten auf einem USB-Stick beim Auftragsverarbeiter (Ziffer 7.1) hat sich der Ausschuss berichten lassen, dass es in der konkreten Konstellation schwierig sei, Zugriffsrechte von Mitarbeiterinnen und Mitarbeitern der Forensik weiter zu beschränken, da diese sonst nicht mehr arbeitsfähig seien. Datenschutzrechtlich handele es sich um einen speziellen Fall. Ob der Vorfall weitere datenschutzrelevante Maßnahmen beim Auftragsverarbeiter nach sich gezogen habe, konnte nicht geklärt werden.

Im Hinblick auf den Bereich „Gesundheit und Soziales“ begrüßt der Ausschuss, dass bei der Bewohner- und Quartiersmanagementsoftware für Flüchtlingsunterkünfte (Ziffer 8.1) zum Teil bereits nachgebessert und das von der Landesbeauftragten kritisierte Beschäftigtenmodul inzwischen abgeschaltet worden ist. Bei der Datenspeicherung im Hinblick auf die Essensausgabe seien Veränderungen vorgenommen worden, die jedoch aus Sicht der Landesbeauftragten noch nicht zufriedenstellend seien. Ein vollständiges Löschkonzept liege weiterhin nicht vor. Insbesondere über die Aufbewahrungs- beziehungsweise

Speicherfristen sei noch keine Einigkeit erzielt worden. Der Ausschuss erwartet, dass hier zeitnah eine Einigung zwischen den Beteiligten und eine zufriedenstellende Lösung erzielt wird, die alle berechtigten Interessen berücksichtigt. Der Bereich der Sozialdaten ist aus Sicht des Ausschusses sehr sensibel und verdient besondere Aufmerksamkeit, speziell im Hinblick auf die Schnittstellen.

Bei der datenschutzrechtlichen Problematik im Zusammenhang mit der Übermittlung von Blutalkoholwerten vom Krankenhaus an die Polizei (Ziffer 8.2) hat der Ausschuss zur Kenntnis genommen, dass es im Krankenhausdatenschutzgesetz keine gesetzliche Grundlage für eine solche Übermittlungsbefugnis an Strafverfolgungsbehörden gibt. Mangels Einwilligung und Schweigepflichtentbindung sei die Übermittlung daher unzulässig erfolgt. Der Ausschuss geht jedoch davon aus, dass es sich um einen Einzelfall gehandelt hat und solche Datenübermittlungen nicht regelmäßig erfolgen, sondern die Krankenhäuser grundsätzlich bei der Weitergabe von Informationen die geltenden datenschutzrechtlichen Bestimmungen beachten.

Bei der Kennzeichnung von Patientenbetten im Krankenhaus mit vollständigen privaten Adressdaten (Ziffer 8.3) nimmt der Ausschuss positiv zur Kenntnis, dass diese Praxis in allen Krankenhäusern abgestellt worden ist und nicht mehr angewendet wird.

Das Thema „Datenbank Haaranalysen“ (Ziffer 8.12) war bereits Gegenstand zahlreicher Jahresberichte und hat den Ausschuss im Hinblick auf die datenschutzrechtliche Problematik immer wieder beschäftigt. Auch wenn die Datenbank inzwischen konzeptionell überarbeitet worden sei, liege abschließend noch kein zufriedenstellendes Datenschutzkonzept vor, insbesondere kein Löschkonzept. Die Beteiligten arbeiteten jedoch konstruktiv an einer Lösung und seien zuversichtlich, in diesem Jahr weitere Fortschritte erzielen zu können.

Im Bereich des Beschäftigtendatenschutzes (Ziffer 10) stellten sich regelmäßig Fragen im Zusammenhang mit der Zulässigkeit von Überwachungen der Arbeitszeit, der Arbeitszeiterfassung, Zugangs- beziehungsweise Zutrittskontrollen sowie deren konkreten Ausgestaltungen im Einzelfall. Als wichtig erachtet der Ausschuss in diesem Zusammenhang, dass auch bei Vorliegen von Betriebsvereinbarungen, denen der Personal- beziehungsweise Betriebsrat zugestimmt hat, Vorgaben der DSGVO beachtet werden müssen. Durch Betriebsvereinbarungen könne lediglich gestaltend Einfluss genommen werden, nicht jedoch reduzierend.

Im Hinblick auf den Einsatz von Bodycams im Bahnhofsumfeld durch private Sicherheitsdienste (Ziffer 11.4) nimmt der Ausschuss positiv zur Kenntnis, dass diese unzulässige Praxis abgestellt worden ist, nachdem sich die Landesdatenschutzbeauftragte eingeschaltet hat. Insbesondere bei der öffentlichen Videoüberwachung im Bereich des Bahnhofsvorplatzes werde sehr darauf geachtet, dass die installierten Kameras nur das filmten, was rechtlich erlaubt sei. Schwieriger gestalte sich die Lage bei den privat installierten Videokameras, deren Besitzern häufig nicht bewusst sei, was rechtlich erlaubt sei und was nicht. Entscheidend sei auch hier das Kriterium der Erforderlichkeit. Auch im nicht öffentlichen Bereich gäbe es legitime private Interessen, zu deren Schutz Videokameras eingesetzt werden dürften.

Zu dem Themenbereich „Internationales und Europa“ nimmt der Ausschuss zur Kenntnis, dass der EU-U.S. Privacy Shield ebenso wie schon zuvor das Safe-Harbour-Abkommen aufgrund von datenschutzrechtlichen Einwänden vor den EuGH gebracht worden ist. Sowohl die Stellungnahme des Generalanwalts als auch eine endgültige Entscheidung stünden jedoch noch aus (Ziffer 16.1).

Durch den U.S.-amerikanischen Cloud-Act versuche die USA, sich Zugriff auf Daten von Personen aus der EU zu verschaffen, in dem sie europäische Unternehmen verpflichte, ihnen Daten zu übermitteln (Ziffer 16.2). Dieses Vorgehen werde von europäischen Datenschützer sehr kritisch beurteilt.

Die Bürgerschaft (Landtag) nimmt den Bericht des Ausschusses für Wissenschaft, Medien, Datenschutz und Informationsfreiheit zur Kenntnis.

Dr. Solveig Eschen