Abgeordnetenhaus BERLIN

Drucksache 18 / 21 508
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Bernd Schlömer (FDP)

vom 06. November 2019 (Eingang beim Abgeordnetenhaus am 06. November 2019)

zum Thema:

Einhaltung und Organisation datenschutzrechtlicher Standards in öffentlichen Stellen Berlins

und **Antwort** vom 25. Nov. 2019 (Eingang beim Abgeordnetenhaus am 28. Nov. 2019)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Inneres und Sport

Herrn Abgeordneten Bernd Schlömer (FDP)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 18/21508
vom 6. November 2019
über Einhaltung und Organisation datenschutzrechtlicher Standards in öffentlichen Stellen Berlins

---

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorbemerkung:
Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung – DSGVO) ist eine Verordnung der Europäischen Union, mit der die Verarbeitung personenbezogener Daten durch private wie auch durch öffentliche Stellen EU-weit geregelt wird. Die DSGVO gilt unmittelbar in allen EU Mitgliedstaaten und damit auch für die in der Schriftlichen Anfrage genannten öffentlichen Einrichtungen. Bei der Beantwortung der Fragen wird daher, abgesehen von den genannten Fällen, keine weitere Differenzierung vorgenommen.

1. Ist der Berliner Senat (und nicht die Berliner Beauftragte für den Datenschutz) der Auffassung, dass Einrichtungen der öffentlichen Hand (bitte explizit und differenziert beantworten für Schulen, Universitäten, Krankenhäuser und öffentliche Wohnungsunternehmen) stets und flächendeckend Softwarebibliotheken (CVE) und sonstige Softwarekomponenten vor deren Verwendung zur Verarbeitung bzw. Speicherung von personenbezogenen Daten umfassenden Tests hinsichtlich
   a) der Einhaltung der Datenschutzgrundsätze nach Art. 5 DSGVO,
   b) der Anforderungen an Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nach Art. 25 DSGVO sowie
   c) der Anforderungen an Datensicherheit nach Art. 32 DSGVO unterziehen müssen?

Zu 1.:
Ob eine Testung von Softwarebibliotheken und sonstigen Softwarekomponenten vor deren Verwendung zur Verarbeitung von personenbezogenen Daten hinsichtlich Art. 5, 25 und 32 DSGVO vorgenommen werden muss, ist eine Frage des Einzelfalles, für die eine Risiko- und Folgenabschätzung erforderlich ist. Die Voraussetzungen ergeben sich unmittelbar aus der DSGVO selbst.

So trifft der Verantwortliche gemäß Artikel 25 Absatz 1 DSGVO unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen - wie z. B. Pseudonymisierung -, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen.

Gemäß Artikel 32 Absatz 1 DSGVO treffen der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Verantwortlicher ist gemäß Artikel 4 Nummer 7 DSGVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Für den Bereich der Schulen weist die Senatsverwaltung für Bildung, Jugend und Familie darauf hin, dass Schulen in ihrem Verwaltungsbereich eine standardisierte IT-Infrastruktur, die „Zentrale Schulverwaltungsumgebung“ (ZSVU) einsetzen. Die in der ZSVU eingesetzten Datenverarbeitungsverfahren sind durch das ITDZ IT-sicherheitstechnisch geprüft. Die datenschutzrechtliche Betrachtung bei diesen berlinweiten Verfahren obliegt der Berliner Beauftragten für Datenschutz und Informationsfreiheit.

2. Ist der Berliner Senat (und nicht die Berliner Beauftragte für den Datenschutz) Senat der Auffassung, dass Einrichtungen der öffentlichen Hand (bitte explizit und differenziert beantworten für Schulen, Universitäten, Krankenhäuser und öffentliche Wohnungsunternehmen) vor und während der Verarbeitung bzw. Speicherung von personenbezogenen Daten stets und flächendeckend zur Umsetzung der Anforderung nach Art. 32 DSGVO selbst spezifische technische und organisatorische Maßnahmen (wie Netzwerksegmentierung, Mobilgeräte-Richtlinie, Authentifizierung von Diensten) umsetzen müssen?

Zu 2.:
Ja. Artikel 32 Absatz 1 DSGVO verlangt, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen ergreift, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3. Ist der Berliner Senat (und nicht die Berliner Beauftragte für den Datenschutz) der Auffassung, dass Einrichtungen der öffentlichen Hand (bitte explizit und differenziert beantworten für Schulen, Universitäten, Krankenhäuser und öffentliche Wohnungsunternehmen) vor und während der Verarbeitung bzw. Speicherung von personenbezogenen Daten stets und flächendeckend zur Umsetzung der Anforderung nach Art. 32 DSGVO eine Risikobewertung von Drittanbietern (wie z.B. Cloud-Dienste Anbietern), die bei der Verarbeitung von personenbezogenen Daten als Auftragsverarbeiter nach Art. 28 DSGVO eingesetzt werden, durchführen müssen?

Zu 3.:
Die Voraussetzungen für die Auswahl des Auftragsverarbeiters ergeben sich aus Artikel 28 Absatz 1 DSGVO. Danach darf der Verantwortliche nur mit Auftragsverarbeitern arbeiten, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Für den Bereich der Schulen weist die Senatsverwaltung für Bildung, Jugend und Familie darauf hin, dass hinsichtlich der standardisierten IT-Infrastruktur ZSVU eine datenschutzrechtliche Betrachtung durch die Berliner Beauftragten für Datenschutz und Informationsfreiheit erfolgt.

Die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung weist darauf hin, dass nach Artikel 9 Absatz 1 DSGVO die Verarbeitung von Gesundheitsdaten grundsätzlich untersagt ist, sofern nicht die Ausnahmen nach Artikel 9 Absatz 2 bis 4 DSGVO einschlägig sind. Davon sind unter anderem die Verarbeitung für Zwecke der Versorgung und Behandlung im Gesundheitsbereich erfasst, sofern die Verarbeitung durch Fachpersonal erfolgt, das dem Berufsgeheimnis oder einer gesetzlich geregelten Geheimhaltungspflicht unterliegt. Artikel 9 Absatz 4 DSGVO erlaubt den Mitgliedstaaten die Einführung oder Aufrechterhaltung von zusätzlichen Bedingungen oder Beschränkungen soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist. Im Übrigen enthalte § 24 Berliner Landeskrankenhausgesetz (LKG) Regelungen für alle Krankenhäuser zur Auftragsdatenverarbeitung, die eine Verarbeitung von Patientendaten durch Drittanbieter regeln.

4. Ist der Berliner Senat (und nicht die Berliner Beauftragte für den Datenschutz) der Auffassung, dass Einrichtungen der öffentlichen Hand (bitte explizit und differenziert beantworten für Schulen, Universitäten, Krankenhäuser und öffentliche Wohnungsunternehmen) bei einer gegebenenfalls durchzurührenden Risikobewertung gemäß Frage 3 stets und flächendeckend das Zusammenspiel der technischen und organisatorischen Maßnahmen der Einrichtung der öffentlichen Hand mit den technischen und organisatorischen Maßnahmen von Drittanbietern, (wie z.B. Cloud-Dienste Anbietern), die bei der Verarbeitung von personenbezogenen Daten als Auftragsverarbeiter nach Art. 28 DSGVO eingesetzt werden, bewerten müssen?

Zu 4.:
Die Voraussetzungen für die Auswahl des Auftragsverarbeiters ergeben sich aus Artikel 28 Absatz 1 DSGVO. Ob der Auftragsverarbeiter hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet, hängt auch von dem Zusammenspiel mit den ggf. durchzuführenden technischen und organisatorischen Maßnahmen der genannten Einrichtungen ab.

Berlin, den 25. November 2019

In Vertretung

Torsten Akmann
Senatsverwaltung für Inneres und Sport