Deutscher Bundestag **Drucksache 19/5988**

19. Wahlperiode 23.11.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/5560 –

Nutzung von Software ausländischer Hersteller im Sicherheitsbereich

Vorbemerkung der Fragesteller

Laut einem Bericht der „Süddeutschen Zeitung“ vom 19. Oktober 2018 arbeitet Hessens Polizei als erste in Deutschland mit Software des privat geführten US-Unternehmens Palantir Technologies (vgl. www.sueddeutsche.de/digital/palantir-in-deutschland-wo-die-polizei-alles-sieht-1.4173809). Dabei soll der Auftrag an Palantir vergeben worden sein, ohne Angebote von Bewerbern einzuholen. Die für Hessen angepasste Version heißt „Hessendata“. Sie greift auf drei Polizeidatenbanken für Kriminalfälle und Fahndungen, Verbindungsdaten aus der Telefonüberwachung, Daten aus ausgelesenen Handys Verdächtiger und Fernschreiben sowie auf Daten aus sozialen Medien zu.

Laut Bericht räumte der technische Direktor der Hessischen Zentrale für Datenverarbeitung (HDZ) im Palantir-Untersuchungsausschuss im Hessischen Landtag ein, er könne nicht 100-prozentig ausschließen, dass über eine heimlich installierte digitale Hintertür der Software Daten abfließen.

Vorbemerkung der Bundesregierung

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen in offener Form in einigen Fällen gar nicht, in anderen nur teilweise erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie eine Fülle an sicherheitsrelevanten Angaben enthalten, deren Bekanntwerden für die Sicherheit der Bundesrepublik Deutschland nachteilig sein könnte oder ihre Sicherheit gefährden bzw. ihr schweren Schaden zufügen könnte.

Detaillierte Angaben zu der in der Bundesverwaltung eingesetzten Software oder zu IT-Sicherheitssystemen würden gezielte elektronische Angriffe auf einzelne Ressorts oder Behörden ermöglichen. Die Handlungsfähigkeit zumindest von Teilen der Bundesregierung könnte damit empfindlich verringert werden. Für die Sicherheit der Bundesrepublik Deutschland, insbesondere die Sicherheit der Regierungskommunikation, könnte die Veröffentlichung der geforderten Informationen also nachteilig sein.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 21. November 2018 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Deshalb sind einzelne Angaben gemäß des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) als „VS – Nur für den Dienstgebrauch“ eingestuft und werden als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt. Dies betrifft im Einzelnen ganz oder teilweise die Antworten der Sicherheitsbehörden zu Frage 1.

Hinsichtlich des Bundeskriminalamtes gelten bei der Beantwortung der Kleinen Anfrage folgende Einschränkungen:

Die Beantwortung der Frage zu der beim Bundeskriminalamt (BKA) eingesetzten Software ausländischer Hersteller kann selbst in eingestufter Form nicht vollständig erfolgen. Zu dieser Entscheidung ist die Bundesregierung nach sorgfältiger Abwägung der widerstreitenden Interessen gelangt. In einen angemessenen Ausgleich zu bringen waren dabei einerseits das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Parlaments (Artikel 38 Absatz 1 Satz 2 und Artikel 20 Absatz 2 Satz 2 des Grundgesetzes) und andererseits das ebenfalls Verfassungsrang genießende schutzwürdige Interesse des Wohls des Bundes (Staatswohl) sowie das Interesse an einer funktionsgerechten Aufgabenwahrnehmung des BKA im Zusammenhang mit der Verbrechensbekämpfung sowie der Abwehr von Gefahren des internationalen Terrorismus.

Im Einzelnen:

Von der Fragestellung sind auch Informationen über Softwareprodukte betroffen, die im Rahmen der Entwicklung und des Einsatzes von Software zur informationstechnischen Überwachung sowie zur operativen Analyse von Hacking bzw. Malware als auch zur IT-Forensik innerhalb des BKA genutzt werden und über gängige Standardsoftware hinausgehen. Diese Informationen berühren in besonders hohem Maße das Wohl des Bundes und sind besonders geheimhaltungsbedürftig, weil sie im Ergebnis weitgehende Rückschlüsse auf die technische Ausstattung und damit mittelbar auch auf die (geplanten) technischen Fähigkeiten und das Know-how des BKA zulassen. Dadurch könnten die zur effektiven Strafverfolgung und Gefahrenabwehr notwendigen Fähigkeiten des BKA zur informationstechnischen Überwachung, der operativen Analyse von Hacking bzw. Malware als auch der IT-Forensik in erheblicher Weise negativ beeinflusst und somit auch zukünftige Maßnahmen in diesen Bereichen erheblich erschwert bzw. unmöglich werden.

Bereits das Bekanntwerden eines konkreten vom BKA zur informationstechnischen Überwachung bzw. zur operativen Analyse von Hacking/Malware oder zur IT-Forensik eingesetzten Softwareproduktes würde mit hoher Wahrscheinlichkeit erhebliche negative Auswirkungen auf zukünftige Einsätze des jeweiligen Instrumentes haben, da betroffene Personen mit Kenntnis der Spezifika der Software gezielt Maßnahmen ausweichen oder deren Durchführung entdecken könnten und ein Ersatz aufgrund des Mangels an alternativen Softwareprodukten vor dem Hintergrund der umfangreichen Spezialanforderungen in der Regel nicht möglich ist. Daraus würden erhebliche Ermittlungsdefizite für das BKA entstehen, die keinesfalls toleriert werden können. Eine VS-Einstufung und Weiterleitung der angefragten Informationen an die Geheimschutzstelle des Deutschen Bundestages kommt angesichts ihrer erheblichen Brisanz im Hinblick auf die Bedeutung der vorgenannten Ermittlungsinstrumente für die Aufgabenerfüllung des BKA und aus den zuvor benannten Gründen nicht in Betracht, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]).

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen des BKA sowie mittelbar der weiteren zur Durchführung von Maßnahmen der informationstechnischen Überwachung bzw. der operativen Analyse von Hacking/Malware oder IT-Forensik befugten Sicherheitsbehörden zurückstehen.

Hinsichtlich des Zollkriminalamtes (ZKA) gelten bei der Beantwortung der Kleinen Anfrage folgende Einschränkungen:

Frage 1d begehrt Auskünfte zu Daten des ZKA, die aufgrund der Folgen, die bei ihrer Veröffentlichung zu erwarten sind, als geheimhaltungsbedürftig im Sinne des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der VSA einzustufen sind. Die Kenntnisnahme von Einzelheiten zu technischen Fähigkeiten des Zollkriminalamtes könnte sich – bei Annahme einer möglichen Veröffentlichung – schädlich auf die Interessen der Bundesrepublik Deutschland auswirken. Aus dem Bekanntwerden könnten sowohl seitens staatlicher als auch nichtstaatlicher Akteure Rückschlüsse auf „Modi Operandi“ und die Fähigkeiten des Zollkriminalamtes gezogen werden. Im Ergebnis würden dadurch die Funktionsfähigkeit und Aufgabenwahrnehmung des Zollkriminalamtes beeinträchtigt sowie ermittlungstaktische Verfahrensweisen und mithin die Sicherheit der Bundesrepublik Deutschland gefährdet.

Die Antwort zu Frage 1d wird daher als Verschlusssache im Sinne des SÜG in Verbindung mit der VSA mit dem Geheimhaltungsgrad „VS – Vertraulich“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Hinsichtlich des Bundesamtes für Verfassungsschutz (BfV) gilt bei der Beantwortung der vorliegenden Kleinen Anfrage folgende Einschränkung:

Gegenstand der Kleinen Anfrage sind solche Informationen, die in besonders hohem Maße das Staatswohl berühren, dass die entsprechenden Fragen daher selbst in eingestufter Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung findet seine Grenzen in den gleichfalls Verfassungsrang genießenden schutzwürdigen Interessen des Staatswohls. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten zu spezifischen IT-Systemen aber auch zur konkreten Methodik und zu in hohem Maße schutzwürdigen spezifischen Fähigkeiten des Bundesamtes für Verfassungsschutz (BfV) bekannt würden.

Detailinformationen würden konkrete Anhaltspunkte für potenzielle Angriffsvektoren auf IT-Systeme des BfV bieten und den Schutz der nachrichtendienstlichen, operativen Sicherheit gefährden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten des BfV ziehen. Dies könnte folgenschwere Einschränkungen der Informationsgewinnung zur Folge haben, womit letztlich der gesetzliche Auftrag des BfV – die Sammlung und Auswertung von Informationen gemäß § 3 Absatz 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) – nicht mehr sachgerecht erfüllt werden könnte.

Die Gewinnung von inlandsbezogenen Informationen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des BfV jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen

sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Selbst eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung des BfV nicht ausreichend Rechnung tragen. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweisen des BfV so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzen Kreis von Empfängern ihrem Schutzbedürfnis widersprechen würde. Bei einem Bekanntwerden der schutzbedürftigen Informationen wäre kein Ersatz durch andere Instrumente der Informationsgewinnung möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen in ihrer Detailtiefe derart schutzbedürftige Geheimhaltungsinteressen so berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht in diesem besonderen Einzelfall wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

Hinsichtlich des Bundesnachrichtendienstes (BND) gelten bei der Beantwortung der Kleinen Anfrage folgende Einschränkungen:

Informationen zur im BND eingesetzten Software, ihrer IT-sicherheitlichen Bewertung sowie den Rahmenbedingungen der Softwarebeschaffung (Arbeitsmethoden und Vorgehensweisen) sind in Hinblick auf die künftige Erfüllung des gesetzlichen Auftrags aus § 1 Absatz 2 des Gesetzes über den Bundesnachrichtendienst (BNDG) besonders schutzwürdig. Eine Veröffentlichung von Einzelheiten hierzu würde für die Auftragserfüllung des Bundesnachrichtendienstes erhebliche Nachteile zur Folge haben. Sie kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Die Antwort zu Frage 1f sowie Teile der Antworten zu Frage 4 werden daher als Verschlusssache im Sinne des SÜG in Verbindung mit der VSA mit dem Geheimhaltungsgrad „VS – Vertraulich“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

Hinsichtlich des Bundesamtes für den Militärischen Abschirmdienst (BAMAD) gelten bei der Beantwortung der Kleinen Anfrage folgende Einschränkungen:

Gegenstand der Kleinen Anfrage sind solche Informationen, die in besonders hohem Maße das Staatswohl berühren, dass die entsprechenden Fragen daher selbst in eingestufter Form nicht beantwortet werden können. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung findet seine Grenzen in den gleichfalls Verfassungsrang genießenden schutzwürdigen Interessen des Staatswohls. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten zu spezifischen IT-Systemen aber auch zur konkreten Methodik und zu in hohem Maße schutzwürdigen spezifischen Fähigkeiten des BAMAD bekannt würden.

Detailinformationen würden konkrete Anhaltspunkte für potenzielle Angriffsvektoren auf IT-Systeme des BAMAD bieten und den Schutz der nachrichtendienstlichen, operativen Sicherheit gefährden. Infolgedessen könnten sowohl staatliche als auch nichtstaatliche Akteure Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten des BAMAD ziehen.

Dies könnte folgenschwere Einschränkungen der Informationsgewinnung zur Folge haben, womit letztlich der gesetzliche Auftrag des BAMAD – die Sammlung und Auswertung von Informationen – nicht mehr sachgerecht erfüllt werden könnte. Die Gewinnung von nachrichtendienstlichen Informationen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des

BAMAD jedoch unerlässlich. Sofern solche Informationen entfallen oder wesentlich zurückgehen sollten, würden empfindliche Informationslücken auch im Hinblick auf die Sicherheitslage der Bundesrepublik Deutschland drohen. Selbst eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Bedeutung für die Aufgabenerfüllung des BAMAD nicht ausreichend Rechnung tragen. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweisen des BAMAD so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen könnte. Bei einem Bekanntwerden der schutzbedürftigen Informationen wäre kein Ersatz durch andere Instrumente der Informationsgewinnung und -verarbeitung möglich.

Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen in ihrer Detailtiefe derart schutzbedürftige Geheimhaltungsinteressen so berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht in diesem besonderen Einzelfall wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen.

1. Mit welcher Software ausländischer Hersteller arbeiten jeweils

Zum Einsatz von Betriebssystemen, Office-Paketen, freier Software und Schutzsoftware ausländischer Hersteller im Zusammenhang mit den in den Fragen 1a bis 1g genannten Bundesbehörden wird auf die Antwort der Bundesregierung zu den Fragen 1, 3, 6 und 13 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13069 verwiesen.

a) das Bundesamt für Sicherheit in der Informationstechnik (BSI),

Die Antwort auf die Frage zu der beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eingesetzten Software ausländischer Hersteller kann nicht offen erfolgen. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die Antwort wird als Anlage („VS – Nur für den Dienstgebrauch“) gesondert übermittelt.[1] Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

b) die Bundespolizei (BPOL),

Die Antwort auf die Frage zu der bei der Bundespolizei (BPOL) eingesetzten Software ausländischer Hersteller kann nicht offen erfolgen. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die Antwort wird als Anlage („VS – Nur für den Dienstgebrauch“) gesondert übermittelt.[1] Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

c) das Bundeskriminalamt (BKA),

Die Antwort auf die Frage zu der beim BKA eingesetzten Software ausländischer Hersteller kann in Teilen nicht offen, in Teilen gar nicht erfolgen. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die Antwort wird als Anlage („VS – Nur für den Dienstgebrauch“) gesondert übermittelt.[1] Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

[1] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

d) das Zollkriminalamt (ZKA),

Die Antwort auf die Frage zu der im ZKA eingesetzten Software ausländischer Hersteller kann nicht offen erfolgen. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die Antwort wird als Anlage („VS – Vertraulich“) gesondert an die Geheimschutzstelle des Deutschen Bundestages zur Einsichtnahme übermittelt.[2] Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

e) das Bundesamt für Verfassungsschutz (BfV),

Die Bundesregierung ist nach sorgfältiger Abwägung zu dem Schluss gekommen, dass die Frage nicht beantwortet werden kann. Eine Bekanntgabe von Einzelheiten zu Hersteller und Funktionsweise von Software sowie deren konkreter Anwendung im BfV würde zu weitgehenden Rückschlüssen auf technische Fähigkeiten sowie Aufklärungspotenzial des BfV schließen lassen und die Erkenntnisgewinnung gefährden. Ergänzend wird auf die Vorbemerkung der Bundesregierung verwiesen.

f) der Bundesnachrichtendienst (BND) sowie

Die Antwort auf die Frage zu der beim BND eingesetzten Software ausländischer Hersteller kann nicht offen erfolgen. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die Antwort wird als Anlage (VS-V) gesondert an die Geheimschutzstelle des Deutschen Bundestages zur Einsichtnahme übermittelt.[2] Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

g) das Amt für Militärischen Abschirmdienst (MAD)

(bitte nach Produkt, Hersteller und Hauptsitz des Unternehmens aufschlüsseln)?

Die Bundesregierung ist nach sorgfältiger Abwägung zu dem Schluss gekommen, dass die Frage nicht beantwortet werden kann. Eine Bekanntgabe von Einzelheiten zu Hersteller und Funktionsweise von Software sowie deren konkreter Anwendung im BAMAD würde zu weitgehenden Rückschlüssen auf technische Fähigkeiten sowie Aufklärungspotenzial des BAMAD schließen lassen und die Erkenntnisgewinnung gefährden. Ergänzend wird auf die Vorbemerkung der Bundesregierung verwiesen.

2. Wie schätzt die Bundesregierung die informationstechnische Sicherheit der in der Antwort zu Frage 1 genannten Software jeweils ein?

3. Welche Schlussfolgerungen zieht die Bundesregierung aus ihren Antworten zu den Fragen 1 und 2 hinsichtlich der jeweiligen Hersteller und mit ihnen verbundener Unternehmen?

Die Fragen 2 und 3 werden gemeinsam beantwortet.

Gemäß der Leitlinie für Informationssicherheit in der Bundesverwaltung, dem sog. Umsetzungsplan Bund 2017, müssen für alle in einer Bundesbehörde betriebenen Verfahren Informationssicherheitskonzepte auf Grundlage des IT-Grund-

[2] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Vertraulich“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

schutzes des BSI erarbeitet, wirksam umgesetzt und in angemessenen Abständen aktualisiert werden, um den Schutz der in den Systemen verarbeiteten Informationen angemessen sicherzustellen.

Für IT-Systeme, die für die Verarbeitung von eingestuften Informationen vorgesehen sind bzw. eingesetzt werden, sind darüber hinaus die Regelungen der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz maßgeblich.

Der Einsatz von Software in den Bundesbehörden hat nach den Grundsätzen der Informationssicherheit zu erfolgen. Hiermit ist jeweils auch eine Risikoanalyse in Bezug auf die informationstechnische Sicherheit verbunden. Dabei erfolgen nach den Grundsätzen der BSI-Richtlinien zur Gewährleistung der Informationssicherheit gegebenenfalls weitere Maßnahmen, um den Abfluss von Informationen genau wie die Einhaltung der Schutzziele der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) zu gewährleisten.

Durch die Einhaltung der vorstehenden Maßnahmen wird ein Sicherheitsniveau erreicht, das den Betrieb von Software (nationaler wie ausländischer Hersteller) in Bundesbehörden erlaubt. Sollten Anhaltspunkte Zweifel an dem Sicherheitsniveau aufwerfen, werden weitere Maßnahmen ergriffen.

4. Wie schätzt die Bundesregierung die Gefahr von Cyberspionage beim Einsatz von Sicherheitssoftware-Produkten aus Nicht-EU-Staaten ein?

Generell ist vor dem Einsatz von Software abzuwägen, welche Risiken mit deren Einsatz verbunden sind. Produkte, die innerhalb von IT-Systemen, mit denen eingestufte Informationen verarbeitet werden (sollen), Sicherheitsfunktionen übernehmen, sind vor ihrem Einsatz durch das BSI zuzulassen (§ 51 Absatz 1 VSA). Hierbei findet seitens des BSI auch eine Risikoabschätzung statt.

Darüber hinaus kann eine Beantwortung der Frage in Bezug auf die beim BND vorliegenden Erkenntnisse im Sinne der Fragestellung nicht offen erfolgen. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die Antwort wird als Anlage („VS – Vertraulich“) gesondert an die Geheimschutzstelle des Deutschen Bundestages übermittelt.[2]

5. Auf welche Datenbanken und welche Daten kann mit dem Programm „Hessendata“ nach Kenntnis der Bundesregierung zugegriffen werden?

Die Bundesregierung nimmt zu Verfahren in Zuständigkeit eines Bundeslandes keine Stellung.

6. Hält die Bundesregierung die Verbindung verschiedener Polizeidatenbanken mit Verbindungsdaten, Daten aus ausgelesenen Handys Verdächtiger und Fernschreiber sowie mit Daten aus sozialen Medien für mit dem deutschen Recht vereinbar?

Ja, sofern die gesetzlichen Voraussetzungen für eine entsprechende Datenerhebung vorliegen, ist auch die Speicherung der Daten solange zulässig, bis Löschfristen greifen oder die Speicherung der Daten nicht mehr erforderlich ist. Die Zulässigkeit der Erhebung und Speicherung korrespondiert mit der Zulässigkeit der Nutzung der Daten zu ihrem bestimmungsgemäßen Erhebungszweck im Rahmen der Strafverfolgung und Gefahrenabwehr.

[2] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Vertraulich“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

7. Plant die Bundesregierung, die Software des US-Unternehmens Palantir Technologies auch in Bundesbehörden zu nutzen?

   Falls ja, welche Bundesbehörden sollen mit der Software arbeiten, und ab wann?

Derzeit laufen keine Vergabeverfahren von Bundesbehörden zum Einsatz derartiger Software.

8. Auf welcher rechtlichen Grundlage werden Aufträge für ausländische Softwarehersteller vergeben?

Das geltende europäische wie nationale Vergaberecht ist einheitlich für alle Unternehmen gleich welcher Nationalität anzuwenden. Eine Bevorzugung oder Benachteiligung von Bietern allein auf Grund ihres Unternehmenssitzes im Ausland ist gemäß § 97 Absatz 2 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) unzulässig.

Dies gilt auch für Beschaffungen in den Bereichen Verteidigung und Sicherheit, die nach der Vergabeverordnung Verteidigung und Sicherheit (VSVgV) ausgeschrieben werden.

9. In wie vielen Verträgen von Bundesbehörden mit ausländischen Softwareherstellern sind sogenannte No-Spy-Klauseln enthalten (bitte in prozentualen Anteil und Nennwert aufschlüsseln)?

Bundesbehörden beschaffen Software in der Regel über Abrufe aus Rahmenverträgen des Beschaffungsamtes/der Zentralstelle für IT-Beschaffung des Bundesministeriums des Innern, für Bau und Heimat (BeschA). Diesbezüglich hatte das Bundesministerium des Innern, für Bau und Heimat das BeschA bereits im Juli 2015 per Erlass angewiesen, bei allen Verträgen zur Beschaffung von IT Hard- und Software eine sog. No-Spy-Klausel aufzunehmen.

Für die Beschaffung von Software, für die es keinen Rahmenvertrag beim BeschA gibt, werden grundsätzlich für Beschaffungen die EVB-IT-Vertragsmuster verwendet Über diese EVB-IT-Überlassungsverträge werden die EVB-IT-Überlassung-AGB (Typ A) in den Vertrag einbezogen. Inhalt dieser AGB ist unter anderem eine sog. technische No-Spy-Klausel (Ziffer 2.3).

Lediglich in Ausnahmefällen wird bei Beschaffungen von Software bei Vorliegen von zwingenden fachlichen Gründen auf das Vertragswerk des Anbieters zurückgegriffen. Je nach Inhalt der Verträge des Anbieters müssen in diesen Fällen ausnahmsweise auch Verträge ohne „No-Spy-Klausel“ geschlossen werden.

Die Beschaffung von Unternehmenslizenzen erfolgt so weit wie möglich über Unternehmen in Deutschland.

Nach Kenntnis der Bundesregierung sind daher nur in einer geringen Zahl von unmittelbar mit ausländischen Herstellern geschlossenen Verträgen keine „No-Spy-Klauseln“ enthalten.

In Bezug auf die Nachrichtendienste des Bundes und auf das BKA wird darüber hinaus auf die Vorbemerkung der Bundesregierung verwiesen.

10. Wie wird sichergestellt, dass die sogenannten No-Spy-Klauseln eingehalten werden?

Grundsätzlich wird bei allen Verträgen, die vom Beschaffungsamt des BMI geschlossen werden, eine vertragliche Verpflichtung aufgenommen, die festlegt, wie die Einhaltung der „No-Spy-Klauseln“ seitens des Auftragnehmers nachweislich sichergestellt werden muss. Eine weiterführende Auditierung erfolgt im Beschaffungsamt des BMI nicht, sondern obliegt dem jeweiligen Bedarfsträger auf Grundlage der mit dem jeweiligen Hersteller getroffenen Regelungen.

Unabhängig von den vereinbarten „No-Spy-Klauseln“ ist eine wesentliche Maßnahme, die Kommunikation der Software ausländischer Hersteller mit Servern im Herkunftsland möglichst zu unterbinden. Ist das nicht möglich, werden die betreffenden Anwendungen so weit wie möglich auf abgekoppelten Rechnern betrieben.

Umfangreiche Sicherheitsmaßnahmen in den Regierungsnetzen „Informationsverbund Berlin-Bonn“ (IVBB)/„Netze des Bundes“ (NdB) sowie in internen Netzwerken der Bundesregierung zielen zudem darauf ab, einen ungewollten Informationsabfluss zu verhindern.

11. Welche Schlussfolgerungen zieht die Bundesregierung in diesem Zusammenhang aus der in der Vorbemerkung zitierten Aussage des Direktors der HDZ im hessischen Palantir-Untersuchungsausschuss?

Auf die Antwort zu den Fragen 2 und 3 wird verwiesen.

12. Welche Schlussfolgerungen zieht die Bundesregierung daraus, dass die Fernwartung von Software ausländischer Hersteller durch den jeweiligen Hersteller erfolgt?

In der Regel ist eine Fernwartung von Software ausländischer Hersteller durch den jeweiligen Betreiber nicht zugelassen. Vielmehr werden erforderliche Wartungen so weit wie möglich vor Ort und unter Aufsicht vorgenommen. Sofern ein Fernwartungszugang in Ausnahmefällen dennoch erforderlich ist, ist dies bei der Erstellung der Sicherheitskonzeption kritisch zu begutachten und im Rahmen einer Risikoabwägung geeignet zu würdigen. Entsprechende Konzepte für eine sichere Fernwartung sollten dabei konsequent nach Empfehlungen des BSI umgesetzt werden.

Grundsätzlich wird der Fernwartungszugang durch technisch-organisatorische Maßnahmen besonders überwacht und geschützt. So werden z. B. Fernwartungszugänge nur nach vorheriger schriftlicher Beantragung für den Zugang temporär aktiviert. In einigen Fällen werden für die Fernwartungsverbindung BSI-zugelassene Rendezvous-Server verwendet.

13. Welche Schlussfolgerungen zieht die Bundesregierung daraus, dass die Fernwartung von Software des Herstellers Palantir durch Palantir selbst erfolgt?

Die Bundesregierung hat keine Kenntnisse über die Fernwartung des Herstellers Palantir. Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

14. Benötigt nach Kenntnis der Bundesregierung die Software des Herstellers Palantir eine Internetverbindung, um zu funktionieren?

15. Baut die Software im Regelbetrieb Verbindungen zu den Servern des Herstellers Palantir auf?

    Wenn ja, zu welchem Zweck?

16. Findet nach Kenntnis der Bundesregierung die gesamte Datenverarbeitung auf Servern im Eigentum der Sicherheitsbehörden bzw. im Eigentum der HDZ statt, oder wird ein Teil der Datenverarbeitung auf amerikanischen Servern durchgeführt?

Die Fragen 14 bis 16 werden gemeinsam beantwortet.

Die Bundesregierung hat keine Kenntnisse zu der Funktionsweise der genannten Software.

17. Kann die Bundesregierung ausschließen, dass durch die Nutzung von Software ausländischer Hersteller ausländische Geheimdienste, die Hersteller selbst oder Dritte an deutsche Personendaten bzw. andere Daten deutscher Sicherheitsbehörden gelangen?

Der Beweis, dass deutsche Personendaten oder Daten deutscher Sicherheitsbehörden mittels ausländischer Software nicht ins Ausland gelangen, kann nicht erbracht werden. Es können lediglich „Best Practices“ (z. B. in Form von Sicherheitskonzepten und BSI-Empfehlungen) umgesetzt werden, um einen solchen Datenabfluss zu erschweren und äußerst unwahrscheinlich zu machen. Hierzu sind insbesondere der größtmögliche Einsatz von quelloffener Software, Eigenentwicklungen und der vollständige Verzicht auf Fernwartung durch Externe oder der gänzliche Verzicht auf einen Internetzugang zu nennen.

Zu allen relevanten Risiken, so auch einem möglichen Abfluss von Daten, sind im Rahmen einer Risikoabwägung nach den Vorgaben des IT-Grundschutzes angemessene Maßnahmen zu ergreifen und unter Berücksichtigung und Anwendung der BSI-Standards in einer auf die jeweilige Bundesbehörde bezogene Sicherheitskonzeption festzulegen.

18. Kann die Bundesregierung ausschließen, dass durch die Nutzung von Software des Herstellers Palantir durch deutsche Behörden ausländische Geheimdienste, das private Unternehmen Palantir selbst oder Dritte an deutsche Personendaten bzw. andere Daten deutscher Sicherheitsbehörden gelangen?

Auf die Antwort zu den Fragen 7 sowie 14 bis 16 wird verwiesen.

19. Welche Behörden sind für die Aufsicht bzw. Überwachung der Fernwartung von Software ausländischer Hersteller zuständig?

Nach BSI IT-Grundschutz ist die jeweils zuständige Behörde auch verantwortlich für die Einhaltung der Schutzziele der IT-Sicherheit und damit der Überwachung der Fernwartung. Eine Behörde, welche für die Überwachung der Fernwartung sämtlicher Software ausländischer Hersteller zuständig ist, gibt es nicht.

20. Wie viele Warnhinweise zu Software ausländischer Unternehmen, die von Bundesbehörden genutzt werden, sind seit dem 1. Januar 2016 bei Bundesbehörden eingegangen (bitte nach Monat aufschlüsseln)?

    Wie geht die Bundesregierung mit solchen Warnhinweisen um?

Das BSI betreibt einen Warn- und Informationsdienst (WID) für Schwachstellen in Software-Produkten. Dieser adressiert primär Bundesbehörden. Der WID differenziert nicht nach deutschen oder ausländischen Produkten, sondern orientiert sich an den im BSI bekannten, in der Bundesverwaltung eingesetzten Software-Produkten.

Veröffentlichte Kurzinformationen nach Jahr (Stand: 13. November 2018):

– 2016: 2 041 Kurzinformationen

– 2017: 2 225 Kurzinformationen

– 2018: 1 088 Kurzinformationen.

Der Umgang mit entsprechenden Warnhinweisen ist im Umsetzungsplan Bund 2017 geregelt. Hiernach haben die Bundesbehörden unverzüglich auf Warnhinweise des BSI zu reagieren. Die Ressorts und Einrichtungen haben zudem angemessene Informationssicherheitsmaßnahmen zur Reaktion auf und zur Behandlung von informationssicherheitsrelevanten Ereignissen umzusetzen.

21. In wie vielen Fällen wurde das BSI oder eine andere Stelle damit beauftragt, die Sicherheit von Software ausländischer Hersteller zu überprüfen?

Das BSI wurde bislang in einem Fall damit beauftragt, die Sicherheit von Software ausländischer Hersteller zu überprüfen. Bei diesem Fall handelt es sich um den Beschluss der Konferenz der IT-Beauftragten der Ressorts vom 16. Dezember 2015 (Beschluss Nr. 2015/5), wonach das BSI IT-Sicherheitsaspekte beim Einsatz des Betriebssystems Windows 10 zu überprüfen hat.

Andere Stellen wurden bislang nicht damit beauftragt, die Sicherheit von Software ausländischer Hersteller zu überprüfen.

22. In wie vielen Fällen wurde dabei Einsicht in den Quellcode genommen?

Eine Einsicht in den Quellcode von Software ausländischer Hersteller wurde in Fällen von beauftragten Überprüfungen bislang nicht genommen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333