

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Jan Korte, Dr. André Hahn,
Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/5665 –**

Neuregelung des Beschäftigtendatenschutzes

Vorbemerkung der Fragesteller

Mit dem Gesetzentwurf zur Regelung des Beschäftigtendatenschutzes reagierte die damalige Bundesregierung auf die Datenschutzskandale der späten 2000er-Jahre. Durch fehlende gesetzliche Vorgaben entstand bei den Arbeitgeberinnen und Arbeitgebern offenbar der Eindruck, dass das Überwachen ihrer Beschäftigten völlig legitim sei. Immer wieder gab es Berichte über heimliche Videoüberwachungen und PC-Durchsuchungen durch Arbeitgeber, über Bespitzelungen von Bewerbern oder Angestellten in sozialen Netzwerken oder das Sammeln, Weitergeben sowie den Abgleich von Sozialdaten weit über das Notwendige hinaus.

Der Gesetzentwurf der damaligen Bundesregierung wurde in der 17. Wahlperiode parlamentarisch in erster Lesung und in einer Sachverständigenanhörung im Innenausschuss des Deutschen Bundestages behandelt. Die Kritik am Entwurf war deutlich und vielfältig. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder war „enttäuscht“ von dem neuen Entwurf und attestierte ihm trotz bzw. wegen eingearbeiteter Änderungen in einer Entschließung vom 25. Januar 2013 „erhebliche Mängel“ (www.bfdi.bund.de „Beschäftigtendatenschutz nicht abbauen, sondern stärken!“). Dabei schätzten die Datenschutzbeauftragten insbesondere zwei Punkte als bedenklich ein: Zum einen die im Gesetzentwurf enthaltenen Vorgaben zur Videoüberwachung. Zwar seien versteckte Videoaufzeichnungen nun untersagt; offene dürften dafür exzessiver eingesetzt werden. Zudem seien die Regelungen diesbezüglich unverständlich und der Rechtssicherheit nicht zuträglich. Zum anderen standen die Regelungen zu Datenerhebungsbefugnissen im Bewerbungsverfahren im Fokus der Kritik. Hier wurde besonders der durch Änderungen quasi entfallene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale scharf kritisiert; so werde der Grundsatz der Direkterhebung bei den Betroffenen unterlaufen.

Massive Kritik äußerten auch die Gewerkschaften. Hier waren es insbesondere der Deutsche Gewerkschaftsbund (DGB) und die ver.di –

Vereinte Dienstleistungsgewerkschaft, die sich über eine ungenügende Einbindung der Gewerkschaften in die Regelungen beschwerten und die fehlende Sanktionsmöglichkeiten bei Datenschutzverstößen rügten. Zudem wurde angemerkt, dass der Entwurf nicht die Arbeitnehmer schütze, sondern lediglich die Arbeitgeber davon profitierten (Passauer Neue Presse, 26. August 2010).

Konsequenz der heftigen Kritik waren der Verzicht auf eine Beschlussfassung im Parlament und die Ankündigung weiterer Gespräche. Bis zu diesem Datum existieren nach wie vor keine, die Beschäftigten angemessen und ausreichend schützenden Vorgaben.

Dass gesetzliche Regelungen zum Beschäftigtendatenschutz allerdings unerlässlich sind, wird jedoch immer wieder deutlich. Neben den weiter wachsenden technischen Möglichkeiten zu profilingähnlichen Recherchen über Mitarbeiterinnen und Mitarbeiter, automatisierten Kontrollen und Überwachungen werden von Arbeitgebern auch andere schon vorhandene Datenbanken und Dateien genutzt, um ihre Belegschaften auszuforschen. Hierher gehören Meldungen, dass der Daimler-Konzern nun die Daten seiner Beschäftigten mit Anti-Terrorlisten abgleicht. Dies wurde am 12. November 2014 per Konzernvereinbarung durch den Vorstand der Daimler AG zusammen mit dem ansässigen Betriebsrat beschlossen. Demnach werden nun die Stammdaten der 280 000 Beschäftigten des Unternehmens einmal im Quartal mit den geführten Terrorlisten abgeglichen. Bei Übereinstimmungen folgen die Freistellung der Betroffenen und ein Gehaltszahlungsstopp. Darüber hinaus unterscheidet sich die Methodik der Überprüfung abhängig vom Status der Beschäftigten: Leitende Angestellte werden einem anderen Verfahren unterzogen als lohnabhängig Beschäftigte. Weiter soll der Abgleich nicht mehr, wie bisher, über die die Mitarbeiterkonten verwaltende Bank durchgeführt werden, sondern durch das Unternehmen selbst. Begründet wird diese Maßnahme mit den Antiterrorgesetzen der Europäischen Union (EU) und darüber hinausgehend mit denen der USA (www.datenschutz.de vom 18. Januar 2015 „Mitarbeiter-Screening mit Terrorlisten“).

Die bestehende Möglichkeit des anlasslosen Datenabgleichs bei einem Verdacht auf Straftaten wurde im Zusammenhang mit der Gesetzentwurfsevaluierung zum Beschäftigtendatenschutz durch den damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Peter Schaar, kritisiert, der konkrete Nachbesserungen forderte. Eine Reaktion seitens der Bundesregierung in Form von parlamentarischen Initiativen gab es bisher nicht. Offenbar vertraut man auf Regelungen, die irgendwann die europäische Ebene vorgeben soll.

Die Datenschutz-Grundverordnung der EU (DS-GVO) soll auch den Beschäftigtendatenschutz zumindest im Mindestmaß regeln. Im Streit um die seit Jahren geplante EU-Datenschutzreform warnt der DGB indes aktuell davor, „einer weitflächigen Überwachung im Betrieb Tür und Tor zu öffnen“. Als Beispiel nannte DGB-Vorstandsmitglied Annelie Buntenbach in der „Neuen Osnabrücker Zeitung (NOZ)“ vom 28. Januar 2015 die Möglichkeit von „Nacktschnüffeln“ an Werkstufen und heimlicher Durchsuchungen von Beschäftigten-Computern. Nach derzeitigem Verhandlungsstand sehe die Verordnung für den Schutz von Beschäftigten lediglich minimale Standards vor, die nach Verabschiedung der DS-GVO unmittelbar bindendes Recht für die Mitgliedstaaten der Europäischen Union würden (vgl. NOZ vom 28. Januar 2015).

Vorbemerkung der Bundesregierung

Aus dem Kontext der Kleinen Anfrage versteht die Bundesregierung den verwendeten Begriff der „Sicherheitsüberprüfungen“ nicht als Sicherheitsüberprüfungen im Geheim- oder Sabotageschutz nach dem Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz – SÜG). Das SÜG findet nur dann Anwendung, wenn eine Person von der zuständigen Stelle mit einer sicherheitsempfindlichen Tätigkeit betraut worden ist oder betraut werden soll. Das SÜG ist auch wichtigste Rechtsgrundlage bei der Sicherheitsüberprüfung von Unternehmenspersonal im Rahmen der Geheimschutzbetreuung von Unternehmen durch das Bundesministerium für Wirtschaft und Energie. Zum Schutz von zu überprüfenden Beschäftigten sieht das SÜG neben diversen speziellen datenschutzrechtlichen Regelungen insbesondere die vorherige schriftliche Zustimmung der betroffenen Person zur Sicherheitsüberprüfung vor. Anlasslose Datenabgleiche sind nach dem SÜG unzulässig. Unternehmen haben dabei keinen Zugriff auf Datenbanken der Sicherheitsbehörden oder der Nachrichtendienste.

Unabhängig von Sicherheitsüberprüfungen, die anlässlich einer Betrauung mit einer sicherheitsempfindlichen Tätigkeit durch das SÜG vorgeschrieben sind, müssen Arbeitgeber die sog. EU-Sanktionsverordnungen in ihrer jeweils aktuellen Fassung beachten: Der Rat der Europäischen Union hat zum Zwecke der Terrorismusbekämpfung die Verordnungen (EG) Nr. 2580/2001 vom 27. Dezember 2001, (EG) Nr. 881/2002 vom 27. Mai 2002 und (EU) Nr. 753/2011 vom 1. August 2011 erlassen, die Teil der Gemeinsamen Außen- und Sicherheitspolitik der Europäischen Union sind. Sie sehen unter anderem vor, dass den in den Anhängen der Verordnungen aufgeführten („gelisteten“) Personen keine Gelder und wirtschaftlichen Ressourcen zur Verfügung gestellt werden dürfen (sog. Bereitstellungsverbot). Welche Personen betroffen sind, wird dabei in den Anhängen durch die Angabe bestimmter Identifizierungsmerkmale wie Geburtsdatum oder Geburtsort konkretisiert. Die Verordnungen sind gemäß Artikel 288 Absatz 2 des Vertrages über die Arbeitsweise der Europäischen Union in allen ihren Teilen verbindlich und gelten allgemein und unmittelbar in jedem Mitgliedstaat der Europäischen Union.

Sie müssen von allen Bürgern und Unternehmen mit Sitz in der EU beachtet werden. Maßnahmen zur Umsetzung der Verordnungen und zur Vermeidung von Verstößen gegen die Verordnungen durch deutsche Unternehmen sind von den betroffenen Unternehmen eigenständig zu veranlassen. Dies gilt auch für das Bereitstellungsverbot. Welche Vorkehrungen zur Vermeidung eines Verstoßes gegen die EU-Verordnungen im Einzelnen getroffen werden, ist von jedem Unternehmen entsprechend den dortigen Verfahrensabläufen und Risiken selbst zu prüfen und festzulegen. Die EU-Mitgliedstaaten sind verpflichtet, Verstöße gegen die EU-Verordnungen angemessen zu sanktionieren. Das Außenwirtschaftsgesetz und die Außenwirtschaftsverordnung beinhalten deshalb nationale Regelungen zur Straf- und Bußgeldbewehrung von Verstößen gegen die oben genannten Verordnungen. Die Verordnungen einschließlich der Anhänge mit den („gelisteten“) Personen sind im Amtsblatt der Europäischen Union veröffentlicht und damit für jedermann einsehbar.

1. Auf welcher gesetzlichen Grundlage ist es Arbeitgebern möglich, die Daten ihrer Angestellten mit welchen Fahndungslisten, Antiterrorlisten oder ähnlichen, zum Zweck der Strafverfolgung und der Prävention geführten

Datenbanken abzugleichen, und wie ist nach Kenntnis der Bundesregierung der unternehmerische Zugang jeweils geregelt (bitte nach polizeilichen und nachrichtendienstlichen Datenbanken und Dateien unterscheiden)?

2. Unter welchen gesetzlichen Voraussetzungen können Akteure der Privatwirtschaft auf die Datenbanken der nationalen und europäischen Sicherheitsdienste zurückgreifen?
3. Welche Datenbanken und Listen werden nach Kenntnis der Bundesregierung von welchen Sicherheitsbehörden zum Abgleich von Beschäftigtendaten mit welchem Zweck und auf welcher gesetzlichen Grundlage den Unternehmen zur Verfügung gestellt?

Die Fragen 1 bis 3 werden wegen ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Privatwirtschaftlichen Unternehmen wird weder der Zugriff auf Datenbanken der nationalen und europäischen Sicherheitsbehörden gestattet noch werden privatwirtschaftlichen Unternehmen Datenbanken oder Listen der Sicherheitsbehörden zum Abgleich von Beschäftigtendaten zur Verfügung gestellt. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

4. Welche Konsequenzen sieht die Bundesregierung für Beschäftigte, die unbegründet unter Terrorismusverdacht gesetzt werden?

Zu 4.

Die Bundesregierung sieht zurzeit keinen Handlungsbedarf.

5. Welche Rechtsschutzmöglichkeiten haben die Beschäftigten bisher in Fällen eines Anti-Terrorlisten-Abgleichs, und plant die Bundesregierung diesbezüglich Regelungen zu schaffen, die es den Beschäftigten ermöglichen, sich juristisch gegen ihre Arbeitgeberinnen und Arbeitgeber zu wehren?

Zu 5.

Hier bestehen die allgemeinen Rechtsschutzmöglichkeiten. Im Übrigen wird auf die Antwort zu Frage 4 verwiesen.

6. Gibt es nach Kenntnis der Bundesregierung Regelungen, z.B. in Arbeitsverträgen, Betriebsvereinbarungen o.ä., in denen die Beschäftigten ihre Einwilligung zu einem solchen Abgleich erklären (müssen)?

Zu 6.

Der Bundesregierung liegen über die der Presse zu entnehmenden Informationen hinaus keine Erkenntnisse vor. Insbesondere werden keine Daten zu den Inhalten von Einzelarbeitsverträgen und Betriebsvereinbarungen erhoben.

7. Erfahren die Beschäftigten nach Kenntnis der Bundesregierung von einem konkret anstehenden Abgleich und existieren vor dem Vollzug des Abgleichs

Widerspruchsmöglichkeiten für die Beschäftigten?

Zu 7.

Ob die Beschäftigten von einem Abgleich erfahren, ist der Bundesregierung nicht bekannt. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

8. Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus der von der Daimler AG und dem hausinternen Betriebsrat am 12. November 2014 beschlossenen Konzernvereinbarung aus juristischer Perspektive und unter Datenschutzaspekten?

Zu 8.

Die Überprüfung, ob die genannte Konzernvereinbarung mit geltendem Recht vereinbar ist, obliegt nach dem Gewaltenteilungsprinzip den Gerichten.

9. Ist der Bundesregierung bekannt, auf welche EU-Gesetzgebung sich die Daimler AG konkret als gesetzliche Grundlage der Sicherheitsüberprüfung ihrer Beschäftigten beruft?

Wenn ja, welche ist dies, und welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung diesbezüglich?

Zu 9.

Der Bundesregierung liegen über die der Presse zu entnehmenden Informationen hinaus keine Erkenntnisse vor.

10. Wie wurden die EU-Verordnungen EG-VO 2580/2001, EG-VO 881/2002 und EU-VO 753/2011, die der Europäische Rat aufgrund eines UN-Sicherheitsratsbeschlusses im Dezember 2001 erlassen hat, nach Kenntnis der Bundesregierung in deutschen Unternehmen umgesetzt (bitte nach Arbeitsstätten in der Bundesrepublik Deutschland und im Ausland darstellen)?

Welche weiteren europäischen und deutschen Gesetze, Verordnungen bzw. Richtlinien beziehen sich nach Kenntnis der Bundesregierung auf diese Verordnungen?

Zu 10.

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

11. Hat die Bundesregierung die Verfassungskonformität dieser Verordnung und ihrer Folgeregelungen überprüft?

Wenn ja, wann, und mit welchem Ergebnis?

Wenn nein, warum nicht?

Zu 11.

Die in Frage 10 genannten Verordnungen der Europäischen Union zur Bekämpfung des Terrorismus sind unmittelbar geltendes Unionsrecht. Die Verordnungen und ihre Folgeregelungen wären daher grundsätzlich nicht anhand des nationalen Rechts, sondern allein anhand des Unionsrechts zu prüfen. Die Bundesregierung ist der Ansicht, dass die Verordnungen den Anforderungen des Grundrechtsschutzes auf EU-Ebene entsprechen.

12. Stimmt die Bundesregierung der Beurteilung des Bund Deutscher Arbeitgeber (BDA) zu, der in seinem Leitfaden „Anti-Terrorgesetzgebung“ feststellt, dass „[i]n den Verordnungen [...] nicht auf die Frage eingegangen [wird], was konkret zu unternehmen ist“, und hält sie vor diesem Hintergrund die aktuelle Ausgestaltung der Grundrechtseingriffe für zulässig (bitte begründen)?

Zu 12.

Auf die Vorbemerkung der Bundesregierung und die Antwort zu Frage 11 wird verwiesen.

13. In welcher Form ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle in diese Screenings bzw. Abgleiche eingebunden, auf welcher Rechtsgrundlage geschieht das, wer kontrolliert die Arbeit des Bundesamtes, und welche weiteren Bundes- und Landesbehörden sind grundsätzlich, welche im Falle von Treffern eingebunden?

Zu 13.

Weder das Bundesamt für Wirtschaft und Ausfuhrkontrolle noch weitere Bundes- und Landesbehörden sind in interne Maßnahmen von Unternehmen zur Einhaltung der EU-Sanktionsverordnungen eingebunden. Ergänzend wird auf die Vorbemerkung der Bundesregierung verwiesen.

14. Ist der Bundesregierung bekannt, auf welche Datenbanken und Listen die Daimler AG bei der Sicherheitsüberprüfung konkret zurückgreift?
Wenn ja, welche sind dies, und auf welcher gesetzlichen Grundlage basiert jeweils der Abgleich?

Zu 14.

Der Bundesregierung liegen über die der Presse zu entnehmenden Informationen hinaus keine Erkenntnisse vor.

15. Welche Schlussfolgerungen und Konsequenzen zieht die Bundesregierung aus der Tatsache, dass die Daimler AG die Art der Sicherheitsüberprüfung vom Status ihrer Mitarbeiterinnen und Mitarbeiter abhängig macht?

Zu 15.

Der Bundesregierung liegen über die der Presse zu entnehmenden Informationen hinaus keine Erkenntnisse vor. Sie sieht im Übrigen keine Veranlassung, sich zum internen Verfahren der Daimler AG zu äußern.

16. Ist der Bundesregierung bekannt, ob weitere privatwirtschaftliche Konzerne und Unternehmen die Daten ihrer Beschäftigten regelmäßig mit den Datenbanken der deutschen und europäischen Sicherheitsbehörden abgleichen (bitte aufschlüsseln nach Konzern bzw. Unternehmen, Datenbank, Anzahl der abgeglichenen Datensätze, Behörde, gesetzlicher Grundlage und Begründung)?
17. In welchen Unternehmen wurden nach Kenntnis der Bundesregierung solche Abgleiche ohne Beteiligung der Personalvertretungen eingeführt?
18. Kann die Bundesregierung bestätigen, dass bei Siemens ohne Betriebsvereinbarung und bei jeder Gehaltszahlung ein Abgleich mit EU- und US-Terrorlisten durchgeführt wird (www.datenschutz.de vom 18. Januar 2015) und welche Schlussfolgerungen und Konsequenzen zieht sie aus diesem Verfahren?
19. Welche Unternehmen verzichten nach Kenntnis der Bundesregierung auf gesonderte Abgleiche und führen stattdessen bei den Gehaltszahlungen direkt bei den Banken diesen Abgleich durch?
20. Welche Unternehmen unterscheiden nach Kenntnis der Bundesregierung bei den Screenings bzw. den Abgleichen, wie beispielsweise Thyssen-Krupp (www.datenschutz.de vom 18. Januar 2015), der nur einen Teil seiner Beschäftigten, nämlich die im Kriegsschiffbau Tätigen, screenen, nach Unternehmenssparten (z.B. Rüstungssparte, Sicherheitstechnologien, etc.)?

Die Fragen 16 bis 20 werden gemeinsam beantwortet.

Der Bundesregierung liegen über die der Presse zu entnehmenden Informationen hinaus keine Erkenntnisse vor.

21. Inwieweit und ggf. auf welcher Rechtsgrundlage werden auch Geschäftspartner und Kunden der Unternehmen mit welchen Terrorlisten abgeglichen, und in welcher Form werden diese Abgleiche nach Kenntnis der Bundesregierung mit welchen Daten der Geschäftspartner und Kunden durchgeführt, in welcher Form werden sie wann über dieses Verfahren informiert, und wie informieren sie wiederum ihre Mitarbeiterinnen und Mitarbeiter?

Zu 21.

Auf die Vorbemerkung der Bundesregierung wird verwiesen.

22. Ist der Bundesregierung bekannt, ob auch Daten der Beschäftigten im öffentlichen Dienst außerhalb vorgeschriebener

Sicherheitsüberprüfungsregelungen zum Zwecke der Terrorismusbekämpfung mit den Datenbanken der nationalen und europäischen Sicherheitsbehörden abgeglichen werden?

Wenn ja, welche öffentliche Stelle gleicht die Daten ihrer Beschäftigten auf welcher gesetzlichen Grundlage mit den Datenbanken der nationalen und europäischen Sicherheitsbehörden ab (bitte aufschlüsseln nach öffentlicher Stelle, Anzahl der abgeglichenen Daten, Abgleichsbehörde, Abgleichsdatenbank und jeweiliger gesetzlicher Grundlage)?

23. Existieren für Angestellte im öffentlichen Bereich andere Regelungen hinsichtlich des Abgleichs ihrer Daten mit den Datenbanken und Listen der Sicherheitsbehörden in Bezug auf Methode und Häufigkeit?

Wenn ja, welche, und mit welcher Begründung?

Zu 22. und 23.

Die Fragen 22 und 23 werden wegen ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Die Daten der Beschäftigten des Bundes (Beamte und Tarifbeschäftigte) werden außerhalb vorgeschriebener Sicherheitsüberprüfungen nicht anlasslos mit den Datenbanken der Sicherheitsbehörden zwecks Terrorismusbekämpfung abgeglichen.

24. Wie viele Treffer haben sich seit dem Jahr 2002 in der Bundesrepublik Deutschland außer dem öffentlich gewordenen Fall des Daimler-Mitarbeiters S. I. im Jahre 2006 ergeben (www.datenschutz.de vom 18. Januar 2015) und welche Folgen hatte das nach Kenntnis der Bundesregierung für die jeweils Betroffenen?

Zu 24.

Der Bundesregierung liegen über die der Presse zu entnehmenden Informationen hinaus keine Erkenntnisse vor.

25. Gibt es konkrete Planungen der Bundesregierung, noch in dieser Legislaturperiode explizite Regelungen zum Beschäftigtendatenschutz in Form eines eigenen Beschäftigtendatenschutzgesetzes zu schaffen?

Wenn ja, wie ist diesbezüglich der aktuelle Stand, und welcher Zeitplan existiert?

Wenn nein, warum nicht?

26. Plant die Bundesregierung beim Beschäftigtendatenschutz unterschiedliche gesetzliche Regelungen für den öffentlichen und den privaten Bereich?

Wenn ja, mit welcher Begründung, und worin wird der Unterschied bestehen?

27. Plant die Bundesregierung, verbindliche Regelungen für den Abgleich von Beschäftigtendaten mit Drittstellen zu schaffen?

Wenn ja, zu welchem Zweck, wie sollen diese aussehen, und welche davon sollen automatisiert erfolgen (bitte unter Angabe der gedachten Drittstellen)?

Wenn nein, warum nicht?

28. Welche Auskunftspflichten des Arbeitgebers gegenüber dem Arbeitnehmer hinsichtlich der von ihm gespeicherten Daten bezüglich der Erhebung, Speicherung und Weitergabe an Dritte sieht die Bundesregierung in möglichen Neuerungen zum Beschäftigtendatenschutz vor?
29. Welche Regelungen für die Videoüberwachung am Arbeitsplatz plant die Bundesregierung einzuführen?
30. Welche Regelungen hinsichtlich von PC-Durchsuchungen von Arbeitnehmern plant die Bundesregierung einzuführen?
31. Plant die Bundesregierung die Einführung von einheitlichen Regelungen zum Datenschutz im Bewerbungsverfahren, insbesondere der Erhebung und Verarbeitung von Bewerberdaten aus sozialen Netzwerken?

Wenn ja, welche?

32. Welche Regelungen plant die Bundesregierung hinsichtlich des Einsatzes von biometrischen Verfahren zur Erfassung und Überwachung von Arbeitnehmerinnen und Arbeitnehmern?

Zu 25. bis 32.

Die Fragen 25 bis 32 werden wegen ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Erst nach der endgültigen Annahme der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) kann beurteilt werden, ob und gegebenenfalls welche Regelungen im Bereich der Datenverarbeitung im Beschäftigungskontext auf nationaler Ebene möglich und erforderlich sein werden. Die Trilogverhandlungen zwischen dem Europäischen Parlament, dem Rat und der Europäischen Kommission laufen zurzeit und sollen Ende 2015 abgeschlossen sein.

Nach Artikel 82 des Vorschlags der Europäischen Kommission für eine Datenschutz-Grundverordnung vom 25. Januar 2012 können die Mitgliedstaaten die Datenverarbeitung im Beschäftigungskontext in den Grenzen der Verordnung in eigener Verantwortung regeln. Die Einigung im Rat vom 15. Juni 2015 über eine allgemeine Ausrichtung zur Datenschutz-Grundverordnung entspricht dem im Wesentlichen. Sie sieht zusätzlich die Befugnis vor, spezifischere Regelungen durch Gesetz oder Kollektivvereinbarungen zu treffen. Der Standpunkt des Europäischen Parlaments vom 12. März 2014 enthält demgegenüber ausführlichere Regelungen zur Datenverarbeitung im Beschäftigungskontext. Der Koalitionsvertrag zwischen CDU, CSU und SPD für die 18. Legislaturperiode enthält in Kapitel 2.2. unter der Überschrift „Beschäftigtendatenschutz gesetzlich regeln“ die Aussage, dass die Verhandlungen zur europäischen Datenschutz-Grundverordnung mit dem Ziel verfolgt werden sollen, das bestehende nationale Datenschutzniveau - auch bei der grenzüberschreitenden Datenverarbeitung - zu

erhalten und über das europäische Niveau hinausgehende Standards zu ermöglichen.

33. Welche konkrete Rolle misst die Bundesregierung den Personal- und Betriebsräten bei der Datenerhebung, -verwaltung und -speicherung bei?

Zu 33.

Der Personalrat hat die allgemeine Aufgabe, darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen durchgeführt werden (§ 68 Absatz 1 Nummer 2 des Bundespersonalvertretungsgesetzes). Hierunter fällt auch die Einhaltung datenschutzrechtlicher Bestimmungen. Gleiches gilt für Betriebsräte nach § 80 Absatz 1 Nummer 1 des Betriebsverfassungsgesetzes.

34. Plant die Bundesregierung die Einführung von betriebsinternen Einschränkungs- oder Ausschlussmöglichkeiten der gesetzlichen Regelungen zum Beschäftigtendatenschutz durch beispielsweise Kollektiv- oder Betriebsvereinbarung?

Zu 34.

Nein. Auf die Antwort zu den Fragen 25 bis 32 wird Bezug genommen.

35. Welche Rolle misst die Bundesregierung den betrieblichen Datenschutzbeauftragten bei, welche Voraussetzungen sollten diese ihrer Meinung nach erfüllen, und plant sie, diesen bei einer Neuregelung des Beschäftigtendatenschutzes mehr Befugnisse, beispielsweise Sanktionsmöglichkeiten bei Datenschutzverstößen, zukommen zu lassen?

Zu 35.

Die Datenschutz-Grundverordnung wird voraussichtlich auch Regelungen zum betrieblichen Datenschutzbeauftragten enthalten. Die Bundesregierung setzt sich in den Verhandlungen weiterhin dafür ein, dass die Mitgliedstaaten durch die Datenschutz-Grundverordnung verpflichtet werden, dieses in Deutschland bewährte Konzept zu übernehmen. Im Übrigen wird auf die Antwort zu den Fragen 25 bis 32 verwiesen.

36. Inwieweit, aus welchen Gründen und in welchen konkreten Punkten hält die Bundesregierung die zukünftige DS-GVO für eine geeignete Grundlage zur Regelung des Beschäftigtendatenschutzes, und in welcher Form sollten diese Vorgaben in die nationale Gesetzgebung implementiert werden?

Zu 36.

Die Datenschutz-Grundverordnung wird aufgrund ihres Rechtscharakters als EU-Verordnung in allen Teilen verbindlich sein und in jedem Mitgliedstaat unmittelbar gelten. Im Übrigen wird auf die Antwort zu den Fragen 25 bis 32 verwiesen.

37. Teilt die Bundesregierung die Befürchtung von DGB-Vorstandsmitglied Annelie Buntenbach, dass „audiovisuelle Überwachungsmaßnahmen oder der Einsatz von Chipkarten im Betrieb“ mangels eines ausdrücklichen Regelungsverbots dieser Schutzlücke im Verordnungsentwurf erlaubt wären (bitte begründen)?

Zu 37.

Die Datenschutz-Grundverordnung soll den geltenden Grundsatz des EU-Datenschutzrechts fortführen, nach dem die Verarbeitung personenbezogener Daten nur unter bestimmten unionsrechtlich normierten Voraussetzungen rechtmäßig ist. Ob die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach dem aktuellen Entwurf der Datenschutz-Grundverordnung bei einem bestimmten Sachverhalt zu bejahen wäre, kann nicht abstrakt, sondern nur in Kenntnis aller relevanten Aspekte des Einzelfalls beurteilt werden. Auf die laufenden Trilogverhandlungen wird hingewiesen (siehe Antwort zu den Fragen 25 bis 32).

38. Trifft es zu, dass Betriebsvereinbarungen, die solche Praktiken heute verbieten, wegen des Vorrangs des Europarechts nach Verabschiedung der DS-GVO ihre Wirkung verlieren würden?

Zu 38.

Nach der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union genießt das Unionsrecht unter den in dieser Rechtsprechung festgelegten Bedingungen Anwendungsvorrang vor kollidierendem nationalem Recht. Die Vereinbarkeit einer Vereinbarung mit der zukünftigen Datenschutz-Grundverordnung kann dennoch nicht abstrakt, sondern nur in Kenntnis der finalen Fassung der Verordnung und aller relevanten Fakten des Einzelfalls beurteilt werden. Es ist in diesem Zusammenhang jedoch darauf hinzuweisen, dass Artikel 82 Absatz 1 der Datenschutz-Grundverordnung in der Fassung des Standpunktes des Rates vom 15. Juni 2015 vorsieht, dass spezifischere Regelungen zur Gewährleistung des Schutzes von personenbezogenen Arbeitnehmerdaten nicht nur durch Rechtsvorschriften, sondern auch durch Kollektivvereinbarungen getroffen werden können. Der Erwägungsgrund 124 der Datenschutz-Grundverordnung in dieser Fassung stellt klar, dass die genannten Kollektivvereinbarungen auch Betriebsvereinbarungen umfassen. Die Bundesregierung setzt sich in den Verhandlungen weiterhin für diese Regelung und diesen Erwägungsgrund ein.

39. Trifft es zu, dass sich die europäischen Innen- und Justizminister im Dezember 2014 darauf verständigt haben, dass nach Verabschiedung der DS-GVO nationale Gesetze die EU-Vorgaben nicht im Sinne des Datenschutzes strenger ausformen dürften, wodurch strengere deutsche Regelungen und die Urteile des Bundesverfassungsgerichts ggf. unterlaufen würden?

Zu 39.

Die Datenschutz-Grundverordnung in der Fassung des Standpunktes des Rates vom 15. Juni 2015 sieht vor, dass die Mitgliedstaaten in einigen explizit genannten Bereichen - zum Beispiel für die Verarbeitung personenbezogener Daten im Beschäftigungskontext und im öffentlichen Bereich - spezifischere Vorschriften erlassen können. Darüber hinaus enthält Erwägungsgrund 8 der Datenschutz-Grundverordnung in dieser Fassung auf deutschen Vorschlag hin die Klarstellung,

dass die Mitgliedstaaten sektorspezifische Rechtsvorschriften, die sie zur Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) erlassen haben, beibehalten können. Die Bundesregierung wird sich im Trilog für die Beibehaltung dieser Regelungen und die Ausgestaltung des Artikels 82 als Mindestnorm einsetzen. Ergänzend wird auf die Antwort zu den Fragen 25 bis 32 und die Antwort zu Frage 40 verwiesen.

40. Ist die Bundesregierung bemüht, Öffnungsklauseln in diesem Bereich der Datenschutzgrundverordnung zu integrieren, und wenn ja, an welcher Stelle, mit jeweils welcher Begründung und welchem Ziel?

Zu 40.

Im Standpunkt des Rates vom 15. Juni 2015 zur Datenschutz-Grundverordnung sind bereits eine Reihe von Öffnungsklauseln vorgesehen. Insbesondere Artikel 1 Absatz 2a stellt eine allgemeine Öffnungsklausel dar, nach der die Mitgliedstaaten nach Maßgabe der dort genannten Kriterien spezifischere Regeln zur Anpassung der Anwendung der Verordnung beibehalten oder erlassen können. Eine ähnliche Regelung findet sich auch in dem für die Datenverarbeitung im Beschäftigungskontext relevanten Artikel 82. Ferner setzt sich die Bundesregierung im Rahmen ihrer Möglichkeiten auch im laufenden Trilogverfahren weiterhin dafür ein, dass die Datenschutz-Grundverordnung für die Datenverarbeitung im Beschäftigungskontext nur Mindeststandards setzt und die Mitgliedstaaten darüber hinausgehende Regelungen erlassen können.

41. Welche EU-Mitgliedsstaaten verfolgen nach Kenntnis der Bundesregierung aus welchen Gründen oder mit welcher Begründung ggf. die Absicht, zentrale Datenschutzprinzipien, wie die Zweckbindung und die Datensparsamkeit, in der EU-Datenschutz-Grundverordnung aufzuweichen, wie es Jan Philipp Albrecht, der Berichterstatter des Europäischen Parlaments für die DS-GVO, kritisierte (www.heise.de vom 4. März 2015 „Rote Linie überschritten“: Scharfe Kritik an Aufweichung der EU-Datenschutzreform“), welche Regelungen sind hierfür derzeit angedacht, und welche Position hat die Bundesregierung selbst bei den entsprechenden Beratungen dazu jeweils vertreten?

Zu 41.

Nach Beobachtung der Bundesregierung verfolgt kein Mitgliedstaat die Absicht, zentrale Datenschutzprinzipien aufzuweichen.

Der Grundsatz der Datensparsamkeit findet sich in Artikel 5 Absatz 1 (c) aller Fassungen der Datenschutz-Grundverordnung. Die Formulierung im Standpunkt des Rates vom 15. Juni 2015 entspricht im Wesentlichen der Formulierung in der geltenden EG-Datenschutzrichtlinie 95/46/EG. Die Bundesregierung hatte sich für die Beibehaltung des ursprünglichen Kommissionsvorschlags ausgesprochen.

Den Grundsatz der Zweckbindung enthält Artikel 5 Absatz 1 (b) aller Fassungen der Datenschutz-Grundverordnung. Auch hier entspricht die Formulierung im Wesentlichen derjenigen in der geltenden EG-Datenschutzrichtlinie 95/46/EG.

42. Soll künftig nach Auffassung der Bundesregierung die EU-Datenschutzgrundverordnung Behörden und Unternehmen erlauben, Daten auch für Zwecke zu verwenden, die die Verbraucher zuvor nicht genehmigt haben, und dass diese Daten auch an Dritte weitergeben dürfen?

Wenn ja, warum?

43. Befürwortet die Bundesregierung, dass künftig auf Grundlage der EU-Datenschutzgrundverordnung Unternehmen oder Behörden den Verbraucher nicht über eine Datenweitergabe an Dritte oder eine andere als die genehmigte Verwendung informieren müssen, wenn sie begründen können, dass ihr Interesse überwiegt, und wer definiert und kontrolliert das Überwiegen des Unternehmensinteresses?

Zu 42. und 43.

Die Fragen 42 und 43 werden wegen ihres inhaltlichen Zusammenhangs gemeinsam beantwortet.

Eine Verarbeitung personenbezogener Daten ist nach Artikel 6 Absatz 1 der Datenschutz-Grundverordnung in der Fassung des Standpunktes des Rates nur rechtmäßig, wenn eine der dort genannten Bedingungen erfüllt ist. Nach Artikel 6 Absatz 1 f) ist die Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Das entspricht der geltenden Rechtslage in Deutschland für Privatunternehmen. Die Bundesregierung setzt sich weiterhin dafür ein, dass die Befugnis zur zweckändernden Datenverarbeitung ohne Rechtsgrundlage und allein auf Grundlage einer Interessenabwägung für den öffentlichen Bereich nicht in der Datenschutz-Grundverordnung enthalten sein wird. Das Bundesdatenschutzgesetz (BDSG) enthält zahlreiche Regelungen zur zweckändernden Weiterverarbeitung von Daten (vgl. etwa § 28 Absatz 2 BDSG). Über die Weiterverarbeitung hat der Datenverarbeiter den Betroffenen zu informieren. Diese Informationspflicht sieht die Datenschutz-Grundverordnung in der Fassung des Standpunktes des Rates in Artikel 14 Absatz 1b) und in Artikel 14a Absatz 3a vor.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.