Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 3. Februar 2023[1]

Umsetzung des Studierenden-Energiepreispauschalengesetzes datenschutzkonform gestalten!

Am 21. Dezember 2022 trat das Studierenden-Energiepreispauschalengesetz (EPPSG) in Kraft. Es sieht vor, dass Studentinnen und Studenten, die am 1. Dezember 2022 an einer in Deutschland gelegenen Hochschule immatrikuliert waren, einen Anspruch auf Zahlung einer einmaligen Energiepreispauschale in Höhe von 200 Euro haben. Der Anspruch steht auch weiteren Personen zu, z. B. Schülerinnen und Schülern von Berufsfachschulen, Fachschulen und Fachoberschulen in bestimmten Bildungsgängen. Durch Zahlung der Pauschale ist beabsichtigt, den berechtigten Personen schnell und unbürokratisch einen Ausgleich für die durch die geopolitische Lage bedingt gestiegenen Energiekosten bereitzustellen.

Die Durchführung des Gesetzes obliegt den Ländern. In einer gemeinsamen Bund-Länder-Arbeitsgruppe werden gegenwärtig entsprechende Vorarbeiten durchgeführt. Hierzu gehören u.a. die Abstimmung einer Muster-Rechtsverordnung, die einheitlich in allen Bundesländern erlassen werden soll, und einer Verwaltungsvereinbarung zwischen Bund und Ländern, die den Betrieb einer zentralen Antragsplattform regelt. Parallel wurden mit hohem Zeitdruck Arbeiten zur Umsetzung der rechtlichen Regelungen, zur Konzipierung der Verarbeitungsprozesse und zur Bereitstellung der erforderlichen Software durchgeführt.

Die Ausbildungsstätten sollen verpflichtet werden, „zur Vorbereitung der Antragstellung“ Listen mit Rohdaten aller anspruchsberechtigten Personen zu erstellen und diese Listen in ergänzter und modifizierter (verschlüsselter) Form an eine vom Land

[1] Diese Stellungnahme wurde von der Konferenz durch Mehrheitsentscheidung mit zwei Gegenstimmen beschlossen.

bestimmte, für die Entscheidung über die Anträge zuständige Stelle zu übergeben – und zwar über einen sicheren Transportweg, den die zuständige Stelle vorgibt. Zuvor haben die Ausbildungsstätten ihre Listen in den ihnen von den zuständigen Stellen zur Verfügung gestellten Zugangsschlüssel-Generator einzugeben. Der Generator erzeugt für jede anspruchsberechtigte Person einen bei Antragstellung zu nutzenden kombinierten Zahlen- und Buchstabenschlüssel (Zugangsschlüssel) sowie zusätzlich eine persönliche Identifikationsnummer (PIN). Den Zugangsschlüssel und ggf. die PIN haben die Ausbildungsstätten der jeweils betroffenen Person zuzusenden.

Die zuständige Stelle hat jeweils nach Erhalt der Listen diese auf Plausibilität zu kontrollieren und sodann auf eine zentrale, von Sachsen-Anhalt allen Ländern zur Verfügung gestellte Plattform hochzuladen. Über ein zentrales Portal haben sich die antragstellenden Personen sodann anzumelden und neben ihren persönlichen Daten den von der Ausbildungsstätte erhaltenen Zugangsschlüssel anzugeben. Nach Antragstellung wird das Vorliegen der Bewilligungsvoraussetzungen geprüft. Hierzu erfolgt unter Einsatz des Zugangsschlüssels ein Abgleich zwischen den Listen der Ausbildungsstätten und den bereitgestellten Antragsdaten. Obwohl die Antragsteller in ihrem Antrag zu versichern haben, dass sie noch keinen Antrag gestellt haben, wird der Antrag im zentralen System automatisch mit allen bereits eingereichten Anträgen abgeglichen und geprüft, ob eine Auszahlung an die antragstellende Person bereits erfolgte. Die Entscheidung über die Anträge auf Zahlung der Pauschale erfolgt dann automatisiert in zentralen Verfahren (Fachverfahren, vermutlich pro Land), wobei der entsprechende Bescheid den Antragstellern per E-Mail übermittelt wird.

Der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutz-konferenz) liegen die Entwürfe der Musterverordnung (VO-E) sowie der Verwaltungsvereinbarung zwischen Bund und Ländern (VwV-E) für die zentrale Antragsplattform vor. Darüber hinaus wurden ihr einige Unterlagen zur technischen Realisierung übermittelt, insbesondere eine Kurzbeschreibung und eine Präsentation zu den Verarbeitungsprozessen sowie ein Leitfaden für die Ausbildungsstätten. Letzterer beschreibt u.a. die Erstellung der Rohdatenlisten sowie die Generierung von persönlichen Zugangscodes und PINs für die Anspruchsberechtigten. Hierfür ist auch eine entsprechende Software verfügbar. Die Konferenz nimmt hierzu wie folgt Stellung.

Die Datenschutzkonferenz unterstützt die Absicht von Bund und Ländern, den anspruchsberechtigten Personen unkompliziert einen Ausgleich für die gestiegenen Energiekosten zu zahlen. Sie stellt gleichwohl fest, dass das Gesetz selbst sowie die vorliegenden Entwurfstexte der Rechtsverordnungen und der Verwaltungsvereinbarung datenschutzrechtliche Defizite enthalten. Hierzu gehören insbesondere:

I. Inkonsistenzen und Widersprüche in den vorliegenden Dokumenten

Die der Datenschutzkonferenz gegenwärtig vorliegenden Unterlagen zur Rechtsverordnung, zur Verwaltungsvereinbarung und zur praktischen Umsetzung haben nicht nur einen unterschiedlichen Arbeitsstand und Reifegrad. Sie enthalten z. T. auch widersprüchliche Aussagen oder unvollständige Festlegungen. Diese erschweren eine datenschutzrechtliche Bewertung. Insbesondere die im Verordnungsentwurf beigefügten Kommentierungen lassen vermuten, dass die Mitglieder der Bund-Länder-Arbeitsgruppe sich des Überarbeitungsbedarfs bewusst sind.

Beispielsweise sind die Kategorien der personenbezogenen Daten der Anspruchsberechtigten, die in die Rohdatenlisten aufzunehmen sind, im Verordnungsentwurf anders festgelegt als im Leitfaden für die Ausbildungsstätten (siehe § 3 Absatz 3 VO-E und Kapitel 4 des Leitfadens). Laut Verordnungsentwurf sind mindestens Vor- und Nachnamen sowie das Geburtsdatum der anspruchsberechtigten Personen aufzunehmen. Der Leitfaden sieht darüber hinaus eine Reihe optionaler Daten vor, wobei unklar ist, ob und wie diese weiterverarbeitet werden (dürfen). Die zur Verfügung gestellte Software zur Generierung der Rohdatenliste berücksichtigt gegenwärtig jedenfalls nur den Vornamen, den Familiennamen und das Geburtsdatum der anspruchsberechtigten Personen.

Gemäß § 4 Absatz 1 VO-E sollen die im Land zuständigen Stellen die Rohdatenlisten auf Plausibilität prüfen. Welche konkreten Prüfschritte durchzuführen sind, ergibt sich aus dem Verordnungstext nicht. Wird der kurzen Prozessbeschreibung gefolgt, ist vorgesehen, lediglich die Existenz der Ausbildungsstätte und die ungefähre Anzahl der anspruchsberechtigten Personen (also die Anzahl der Datensätze in der Rohdatenliste) zu verifizieren.

Auch im Hinblick auf den nach § 4 Absatz 2 bzw. § 10 Absatz 3 VO-E vorzunehmenden Abgleich der im jeweiligen Antrag angegebenen Daten mit den entsprechenden Daten aus der Rohdatenliste bestehen Unklarheiten. Die in einem frühen Verordnungsentwurf enthaltenen Festlegungen ließen einen solchen Abgleich gar nicht zu, da die Datenfelder in Rohdatenliste und Antrag unterschiedlich waren. Aber noch in der aktuell diskutierten Version, die einen solchen Abgleich (auch zur Vermeidung von Doppelzahlungen) vorschreibt, bleibt offen, welche Datenfelder in welchen Schritten und durch wen und in wessen datenschutzrechtlicher Verantwortung gegen welche Listen abgeglichen werden soll.

II. Rechtliche Bewertung

1. Fehlende Rechtsgrundlage für die Verarbeitung personenbezogener Daten mangels ausreichender Verordnungsermächtigung und Datenerhebung „auf Vorrat“

Das diskutierte Modell sieht – wie beschrieben – zunächst vor, dass die Ausbildungsstätten ohne Rücksicht auf eine tatsächliche Antragstellung personenbezogene Daten aller Studierenden verarbeiten und der zentralen Landesstelle übermitteln und umgekehrt die Landesstellen solche Daten ohne Rücksicht auf eine Antragstellung erheben. Dabei kommt es für die Landesstellen nicht darauf an, ob – was angesichts des Umstandes, dass sie die Listen auf Plausibilität prüfen sollen, nicht sicher festzustellen ist – die Listen den Landesstellen gegenüber verschlüsselt sind oder nicht. Denn trotz einer etwaigen Verschlüsselung sind die Daten als personenbezogen anzusehen.

Gemäß Artikel 5 Absatz 1 Buchstabe a Datenschutz-Grundverordnung (DS-GVO) i. V. m. Artikel 6 Absatz 1 DS-GVO bedarf aber jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage. Eine solche Rechtsgrundlage kann die Datenschutzkonferenz für die genannten Verarbeitungsschritte indes nicht erkennen.

Der Verordnungsentwurf sieht insoweit in § 14 VO-E Folgendes vor:

> (1) Die zuständigen Stellen dürfen für die Erfüllung ihrer Aufgaben nach dem Studierenden-Energiepreispauschalengesetz und dieser Rechtsverordnung die erforderlichen personenbezogenen Daten verarbeiten.

(2) Die in § 1 Absatz 1 bis 4 des Studierenden-Energiepreispauschalengesetzes genannten Ausbildungsstätten dürfen für die Erfüllung ihrer Aufgaben nach dieser Rechtsverordnung die erforderlichen personenbezogenen Daten verarbeiten, soweit erforderlich auch zweckändernd. Die Ausbildungsstätten haben die Ausbildungsstätten-Listen nach Beendigung der Bewilligungsverfahren, spätestens jedoch zum 31.12.2023 zu löschen.

Dabei sollen sich die Regelungen offenbar auf die Öffnungsklausel in Artikel 6 Absatz 1 Buchstabe e, Absatz 2 und 3 DS-GVO stützen. Möglicherweise ist auch an die Öffnungsklausel aus Artikel 6 Absatz 1 Buchstabe c, Absatz 2 und 3 DS-GVO gedacht.

Die Regelungen können jedoch keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen, weil sie nicht von der Verordnungsermächtigung aus § 2 Absatz 1 Satz 2 EPPSG gedeckt sind. Diese soll schon nach ihrem Wortlaut nur eine bloße Zuständigkeitsbestimmung durch die Landesregierungen ermöglichen. Regelungen über Datenverarbeitungsbefugnisse sind somit nicht von der gesetzlichen Verordnungsermächtigung umfasst. Solche Eingriffsbefugnisse in das Recht auf informationelle Selbstbestimmung bedürfen aber nach deutschem Verfassungsrecht einer gesetzlichen Grundlage, wobei eine Regelung durch eine Rechtsverordnung nur dann genügt, wenn diese auf einer gesetzlichen Verordnungsermächtigung beruht. Entgegen der offensichtlich den Diskussionen der Länder zugrundeliegenden Einschätzungen kann die Verordnungsermächtigung in § 2 Absatz 1 Satz 2 EPPSG auch nicht so verstanden werden, dass der Gesetzgeber gleichsam konkludent die Landesregierungen auch zur Regelung von Datenverarbeitungsbefugnissen habe ermächtigen wollen, weil dies irgendwo im Gesetzgebungsverfahren zum Ausdruck gekommen sei. Dem widerspricht nicht nur der Wortlaut („Die Landesregierungen werden ermächtigt, die für die Bewilligung der einmaligen Energiepreispauschale nach § 1 zuständigen Stellen durch Rechtsverordnung zu bestimmen.“), sondern auch die systematische Auslegung, nachdem sich beide Regelungen in § 1 Absatz 1 EPPSG nur auf die Zuständigkeitsfrage beziehen und erst Absatz 2 mit dem Antragserfordernis eine Verfahrensfrage regelt.

Nun sehen die Landesdatenschutzgesetze – ebenfalls in Anwendung der Öffnungsklausel aus Artikel 6 Absatz 1 Buchstabe e, Absatz 2 und 3 DS-GVO – typischerweise eine Regelung vor, der zufolge die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig ist, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist (siehe z. B. § 4 LDSG BW). Auch diese Regelung berechtigt indes nicht zu der eingangs beschriebenen Datenverarbeitung im Vorfeld der Antragstellung. Denn zur Erfüllung der durch das Studierenden-Energiepreispauschalengesetz selbst festgelegten öffentlichen Aufgabe, die Energiepreispauschale an Berechtigte auszuzahlen, sind diese im Vorfeld der Antragstellung vorgesehenen Verarbeitungsschritte nicht erforderlich. Zu diesem Zeitpunkt steht noch gar nicht fest, ob die jeweils berechtigte Person einen Antrag stellt. Die Sammlung der Daten der Antragsberechtigung findet vielmehr „auf Vorrat“ statt.

Es kann dahinstehen, ob der Gesetzgeber selbst im Studierenden-Energiepreispauschalengesetz ein solches Verfahren hätte festlegen können, wenn er unter dem Gesichtspunkt der Verfahrensbeschleunigung bereits die vorbereitende Sammlung der Daten zur öffentlichen Aufgabe der zuständigen Stellen hätte erklären (und die Ausbildungsstätten zur Mitwirkung verpflichten) wollen. Denn jedenfalls hat der Bundesgesetzgeber dies nicht getan – und die Verordnungsgeber können auch eine solche Erweiterung der gesetzlichen Aufgabe nicht vornehmen, weil sie hierfür keine Verordnungsermächtigung haben.

Nach dem Verordnungsentwurf sollen die zuständigen Stellen der Länder die plausibilisierten Listen sodann „freigeben“, indem sie diese in das hierfür zentral bereitgestellte IT-System hochladen. Hierzu heißt es in dem Entwurf der Verwaltungsvereinbarung, die Hinterlegung erfolge „im Fachverfahren zum Zwecke der Überprüfung der Angaben der antragstellenden Person.“ Unklar ist dabei, wer die datenschutzrechtliche Verantwortung für die dort „hinterlegten“ Daten haben soll. Soweit dies nicht die jeweiligen Länder für ihre eigenen Datenbestände sein sollten, wäre das Hochladen eine Übermittlung personenbezogener Daten, für die ebenfalls eine Rechtsgrundlage nicht ersichtlich wäre.

In § 2 des Entwurfs einer Verwaltungsvereinbarung der Länder heißt es jedoch:

> „Das EPPSG-Portal besteht aus einem zentralen Antragssystem, in dem der ‚Online-Antrag EPPSG-Einmalzahlung' ausgefüllt, gespeichert und übermittelt werden kann, aus einer dem Antragssystem vorgeschalteten Internetseite „Einmalzahlung200.de", die die Betroffenen über die Möglichkeit der Online-Antragstellung und deren Ablauf informiert sowie aus den dezentralen Fachverfahren der Länder, in denen das Verwaltungsverfahren durchgeführt wird."

Und in § 4 wird des Entwurfs der Verwaltungsvereinbarung wird ausgeführt:

> „Die Bearbeitung der Anträge erfolgt in den dezentralen Fachverfahren der Länder. Die Fachverfahren werden den Ländern durch den vom Land Sachsen-Anhalt beauftragten Dienstleister zur Verfügung gestellt und, sofern nicht nachfolgend anders geregelt, verantwortet. Die Länder sind für die Verarbeitung der personenbezogenen Daten in den Fachverfahren datenschutzrechtlich allein verantwortlich.

Wir verstehen die Ausführungen in dem Entwurf der Verwaltungsvereinbarung daher so, dass das „Hochladen" noch innerhalb der datenschutzrechtlichen Verantwortung der Landesstellen erfolgen soll, was den Abschluss entsprechender Auftragsverarbeitungsverträge der Landesstellen mit dem Dienstleister und eine Mandantentrennung bei der Speicherung voraussetzen würde.

Da aber insgesamt die Verarbeitung durch die Landesstellen vor der Antragstellung rechtsgrundlos erfolgt, gilt dies auch für das Hochladen im Fachverfahren.

2. Zuweisung datenschutzrechtlicher Verantwortlichkeiten erfordert gesetzliche Grundlage

Nach § 11 Absatz 1 des Entwurfs der Verwaltungsvereinbarung soll für das Antragssystem sowie die diesem vorgeschaltete Internetseite das Ministerium für Infrastruktur und Digitales des Landes Sachsen-Anhalt (MID) gemäß Artikel 4 Nummer 7 Halbsatz 2 DS-GVO datenschutzrechtlich verantwortlich sein.

Für die datenschutzrechtliche Beurteilung dieser Lösung verweisen wir auf den „Sachstandsbericht des AK Verwaltung zur datenschutzrechtlichen Begleitung der OZG-Umsetzung durch die DSK – Hier: Datenschutzrechtliche Herausforderungen der OZG-Umsetzung insbesondere im Zusammenhang mit dem ‚Einer für alle/viele'-Prinzip" vom 24. November 2021, der dem BMI bereits seit längerer Zeit bekannt ist. Insbesondere ist zu beachten, dass die Zuweisung der Verantwortlichkeit durch eine Verwaltungsvereinbarung, wie sie in § 11 VwV-E vorgesehen ist, nicht ausreicht. Nach Ansicht der Datenschutzkonferenz wäre vielmehr eine entsprechende gesetzliche Regelung der Verantwortlichkeit gem. Artikel 4 Nummer 7 Halbsatz 2 DS-GVO erforderlich, welche bislang nicht vorliegt.

Wir zitieren insoweit aus dem o. g. Sachstandsbericht vom 24. November 2021, S. 6 ff:

„(3) Zuweisung der Verantwortlichkeit, Art. 4 Nr. 7 HS 2 DS-GVO

Einen weiteren Lösungsansatz stellt eine explizite Zuweisung der Verantwortlichkeit nach Art. 4 Nr. 7 HS. 2 DS-GVO dar. Sind die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedsstaaten vorgegeben, kann eine Stelle im mitgliedsstaatlichen Recht ausdrücklich als Verantwortliche benannt oder zumindest können entsprechende Kriterien der Benennung einer verantwortlichen Stelle definiert werden. Hier gilt es jedoch zu beachten, dass eine solche Zuweisung den tatsächlichen Einflussmöglichkeiten auf die Datenverarbeitung der beteiligten Akteure entsprechen muss. Liegt also tatsächlich eine gemeinsame Verantwortung i. S. d. Art. 26 DS-GVO vor, kann dies nicht einfach durch eine entgegengesetzte Regelung nach Art. 4 Nr. 7 HS 2 DS-GVO übergangen werden.

Grundsätzlich kann eine Verantwortungszuweisung nach Art. 4 Nr. 7 HS 2 DS-GVO im Wege eines formellen Gesetzes oder einer Rechtsverordnung erfolgen. Das BMI vertritt hierzu die Auffassung, eine solche Zuweisung könne auch durch Staatsverträge oder einfache Verwaltungsvorschriften erfolgen. Es ist jedoch

nicht davon auszugehen, dass reines Verwaltungsinnenrecht (wie Verwaltungsvereinbarungen oder Verwaltungsvorschriften) dem Begriff des „Rechts der Mitgliedsstaaten“ im Sinne des Art. 4 Nr. 7 HS 2 DS-GVO genügt. Wegen des strengen Gesetzesvorbehalts ist zumindest eine parlamentsgesetzliche Ermächtigung und eine Veröffentlichung in einem außenwirksamen Regelwerk erforderlich.

Aus Sicht des BMI stellt eine Konzentration der Verantwortlichkeit bei einer zentralen Behörde über den Art. 4 Nr. 7 HS 2 DS-GVO aus Gründen der Rechtssicherheit die vorzugswürdigste Lösung dar. Gesetzgeberischer Handlungsbedarf zeigt sich bei diesem Lösungsansatz insoweit, als dass – bei Vorliegen der Voraussetzungen des Art. 4 Nr. 7 Hs. 2 DS-GVO – eine eindeutige Zuweisungsregelung der Verantwortlichkeit im Sinne des Art. 4 Nr. 7 HS 2 DS-GVO beispielsweise im OZG geschaffen werden könnte, um hier Rechtssicherheit herzustellen. Dabei ist jedoch zu beachten, dass auch im Falle der Zuweisung der Verantwortlichkeit eine Rechtsgrundlage für die Verarbeitung durch den Verantwortlichen vorliegen muss. Angesichts des bevorstehenden Endes der Legislaturperiode hat das BMI bislang jedoch noch keine konkreten Vorschläge unterbreitet. Es gilt, hier insoweit zügig Vorschläge zu erarbeiten, um eine datenschutzkonforme OZG-Umsetzung zu ermöglichen.

Als Vorbild für eine zum Beispiel im OZG zu schaffende Regelung wird von der Literatur § 14 Absatz 1 Wirtschafts-Portal-Gesetz Nordrhein-Westfalen (WiPG NRW) vorgeschlagen. Hiernach ist ein Landesministerium für die Datenverarbeitung innerhalb des Antragsportals allein verantwortlich. Ferner enthält auch § 24b Abs. 2 S. 1 Bundeselterngeld- und Elternzeitgesetz (BEEG) eine ausdrückliche Zuweisung der Verantwortlichkeit für das Bundesministerium für Familie, Senioren, Frauen und Jugend für das durch den Bund nach Absatz 1 zu errichtende und betreibende Internetportal. Die Norm sieht vor, dass zur Unterstützung der elektronischen Antragstellung für das Elterngeld das Bundesministerium für das entsprechende Internetportal und damit auch für die dort verarbeiteten personenbezogenen Daten datenschutzrechtlich verantwortlich ist. Auch die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten im Bundesportal wurde in § 9c Abs. 1 Satz 1 E-Government-Ge-

setz des Bundes gesetzlich bestimmt. Insgesamt sind bei der Schaffung nationaler Rechtsgrundlagen im Rahmen der Öffnungsklauseln der DS-GVO die allgemeinen Vorgaben der DS-GVO, insbesondere hinsichtlich der Normklarheit und Bestimmtheit zu beachten (siehe insbesondere EG 41 DS-GVO). Zu diesen Anforderungen gehört vor allem auch, dass die konkrete Benennung eines Verantwortlichen selbst zumindest abgeleitete Normqualität haben muss, nicht allein der Modus der Benennung eines Verantwortlichen."

3. Nicht erforderlicher Abgleich der Antragsdaten mit den Daten in allen Fachverfahren

Nach § 11 Absatz 4 VO-E soll jeder Antrag automatisch mit allen bereits eingereichten Anträgen abgeglichen und geprüft werden, ob eine Auszahlung an die antragstellende Person bereits erfolgte, um eine mehrfache Auszahlung zu verhindern. In § 4 Absatz 2 VwV-E heißt es ähnlich – wenngleich nicht vollständig konsistent:

„Jedes Land kann zur Prüfung eines Antrags in den Fachverfahren der anderen Länder abfragen, ob die betroffene antragstellende Person dort in der Vergangenheit bereits eine Bewilligung der Energiepreispauschale nach dem EPPSG erhalten hat. Die Abfrage erfolgt automatisiert."

Auch hierfür ist eine Rechtsgrundlage nicht ersichtlich. Eine Einwilligung nach Artikel 6 Absatz 1 Buchstabe a DS-GVO scheidet schon wegen der fehlenden Freiwilligkeit und möglichen Widerrufbarkeit aus. Darüber hinaus ist die Durchführung des Abgleichs über alle bundesweit gestellten Anträge nicht zur Auszahlung der Energiepreispauschale erforderlich. Dabei ist zu bedenken, dass die antragstellenden Personen bereits im Antrag angehalten werden zu versichern, dass sie keinen weiteren Antrag gestellt haben. Anhaltspunkte dafür, dass die Studierenden zu Recht unter einen Generalverdacht zu stellen seien, sie würden versuchen, rechtswidrig die Energiepreispauschale mehrfach von verschiedenen Ländern erhalten, können wir nicht erkennen. Dabei ist zu bedenken, dass die Abfrage eines Landes, ob eine Person einen Antrag in den anderen Ländern gestellt hat, zunächst eine Übermittlung personenbezogener Daten an alle anderen Länder impliziert, die schon einer Rechtsgrundlage bedürfte (beispielsweise ähnlich wie in § 41 Absatz 4 BAföG).

g

4. Lösungsvorschlag

Das von Bund und Ländern derzeit projektierte Verfahren ist datenschutzrechtlich jedenfalls nicht ohne eine Änderung des Studierenden-Energiepreispauschalengesetzes zulässig.

Für eine bereits im Vorfeld – vor Antragstellung – erfolgende Übermittlung personenbezogener Daten an die zuständige Stelle und Erhebung seitens dieser Stelle fehlt es – wie ausgeführt – an einer tauglichen Rechtsgrundlage. Die DSK sieht jedoch die politische Eilbedürftigkeit und das unterstützendwerte Bestreben des Bundes und der Länder, die Energiepreispauschale möglichst rasch den Studierenden auszuzahlen, wobei sowohl die Entwicklung eines von der bereits projektierten Vorgehensweise grundlegend abweichenden Verfahrens als auch die Erwirkung einer Änderung des Studierenden-Energiepreispauschalengesetzes voraussichtlich eine weitere Verzögerung mit sich bringen würden. Vor diesem Hintergrund erschiene es den Aufsichtsbehörden ausnahmsweise hinnehmbar, wenn der in der vorzeitigen Übermittlung liegende Eingriff in das Recht auf informationelle Selbstbestimmungsrecht dadurch abgemildert würde, dass technische Maßnahmen – wie nachfolgend unter II. näher beschrieben – eine Kenntnisnahme vom Inhalt der übermittelten Daten durch die zuständige Stelle vor der jeweiligen Antragstellung faktisch wirksam verhindern. Die Möglichkeit, dass Studierende auch in diesem Falle gegen das Verfahren etwaige Rechte individuell geltend machen, bliebe freilich durch diese Einschätzung der DSK unberührt. Dasselbe gilt für die Frage, ob die Ausbildungsstätten angesichts der engen Verordnungsermächtigung zu den entsprechenden Datenverarbeitungen rechtlich angehalten werden könnten.

Auch bei einer derartigen Ausgestaltung des Verfahrens müsste freilich die datenschutzrechtliche Verantwortung für das Antragsportal klar geregelt sein. Insoweit wäre zu prüfen, ob das MID die Verarbeitung im Wege der Auftragsverarbeitung für die jeweils zuständige Landesstelle durchführen kann. Im Hinblick auf die Einbindung des Nutzerkontos Bund.ID bedarf es ebenfalls einer tragfähigen Legitimation. Auch der oben kritisierte Abgleich im Falle einer Antragstellung zum Ausschluss früherer Antragsstellung ließe sich so nicht legalisieren.

III. Weitere Ausführungen zu den vorgesehenen technisch-organisatorischen Maßnahmen:

1. Keine abschließende Klarheit hinsichtlich der Verschlüsselung personenbezogener Daten

Zur Generierung der Rohdatenlisten müssen Ausbildungsstätten nach § 5 Absatz 1 VO-E eine bereitgestellte Software verwenden, den sog. Zugangscode-Generator. Dieser erzeugt für jede anspruchsberechtigte Person einen individuellen Zugangsschlüssel und eine PIN. Gemäß einem frühen Verordnungsentwurf verschlüsselt der Generator die Listen und versieht den Zugangsschlüssel mit einer Hashfunktion.

Abgesehen von der terminologischen Unschärfe (dem Zugangsschlüssel wird keine Hashfunktion, sondern ein Hash als Prüfsumme hinzugefügt) weist die Datenschutzkonferenz darauf hin, dass die Verschlüsselung der Rohdatenliste als Ganzes keinen hinreichenden Schutz gegen die unbefugte Kenntnisnahme der Daten anspruchsberechtigter Personen bietet. Spätestens in der zentralen Antragsplattform, auf die die Rohdaten-listen hochgeladen werden sollen, würde bei dieser Vorgehensweise jede Liste als Ganzes entschlüsselt, um den Antrag mit der Anspruchsberechtigung abzugleichen. Dabei würden auch die Daten von Personen entschlüsselt, die keinen Antrag stellen.

Auch wenn nach den obigen rechtlichen Bewertungen bereits erhebliche Zweifel an der Zulässigkeit der Erstellung der Rohdatenlisten durch die Ausbildungsstätten und der Übermittlung der Listen an die im Land zuständige Stelle bestehen, kann auf technischer Ebene zumindest die unbefugte Entschlüsselung und Kenntnisnahme der Rohdaten durch geeignete kryptografische Verfahren verhindert werden.

Mittlerweile hat die Bund-Länder-Arbeitsgruppe die Entwürfe der Rechtsverordnung sowie der Verwaltungsvereinbarung geändert (siehe § 5 Absatz 1 VO-E und § 5 Absatz 1 VwV-E). Auch die Unterlagen zur praktischen Umsetzung des Verfahrens sowie die vorliegende Software zur Generierung der Rohdatenlisten sehen nun eine Verschlüsselung der einzelnen Datensätze jeweils mit einem zufällig gewählten, individuellen

Schlüssel (dem Zugangsschlüssel) vor. Jeder Datensatz wird darüber hinaus um eine Prüfsumme (Hash) dieses Schlüssels ergänzt. Anschließend wird die Liste einzeln verschlüsselter Datensätze mit den zugeordneten Prüfsummen der Schlüssel an die im Land zuständige Stelle übermittelt und auf die zentrale Plattform hochgeladen. Jede anspruchsberechtigte Person erhält von der Ausbildungsstätte ihren Schlüssel und gibt diesen beim Antrag mit an. In der Folge kann auf der Antragsplattform durch Berechnung der Schlüsselprüfsumme der zugehörige Rohdatensatz bestimmt und dieser durch Anwendung des beim Antrag angegebenen individuellen Schlüssels entschlüsselt werden. Das ermöglicht es, die Anspruchsberechtigung zu prüfen, ohne hierbei die Daten anderer Personen mitentschlüsseln zu müssen.

Die Datenschutzkonferenz begrüßt insoweit die während der Tätigkeit der Bund-Länder-Arbeitsgruppe erzielte Verbesserung des Verfahrens, durch kryptografische Mechanismen die frühzeitige und pauschale Offenlegung personenbezogener Daten zu verhindern. Allerdings sollte auch die Inkonsistenz in § 5 Absatz 2 VO-E behoben und klar formuliert werden, dass die der zuständigen Stelle im Land zu übergebende Liste individuell verschlüsselte Rohdaten und verschlüsselte PINs sowie die Hashwerte der Zugangsschlüssel enthält.

2. Umfang und Inhalt der Rohdatenlisten, Umgang mit Zugangsschlüsseln und PINs

Eine Diskrepanz besteht hinsichtlich der Aussagen zum Umfang und zu den Datenfeldern in den Rohdaten-listen. Gemäß § 5 Absatz 1 VwV-E erstellt die Ausbildungsstätte für die jeweils anspruchsberechtigten Personen auf Ebene der einzelnen Datensätze verschlüsselte Listen mit einem für die spätere Antragstellung relevanten eindeutigen Zugangsschlüssel und eine weitere Liste mit einer zusätzlichen persönlichen Identifikationsnummer (PIN). Die Beschreibung der Listen, insbesondere des Umstandes, dass die Ausbildungsstätten für die PINs eine gesonderte Liste generieren, widerspricht dem bekannten Konzept der Umsetzung. Sowohl die Kurzbeschreibung der Prozesse als auch die Implementierung des Zugangsschlüssel-Generators sehen vor, dass die Ausbildungsstätten zwei Listen generieren. Eine Liste enthält sowohl die individuellen Zugangsschlüssel als auch die PINs (beides im Klartext). Eine zweite Liste

enthält die mit den individuellen Zugangsschlüsseln verschlüsselten Daten der Anspruchsberechtigten und die verschlüsselten PINs sowie die Prüfsummen der jeweiligen Zugangsschlüssel.

Gemäß § 5 Absatz 2 VO-E stellen die Ausbildungsstätten der anspruchsberechtigten Person den durch den Zugangscode-Generator erzeugten individuellen Zugangsschlüssel, der bei der Antragstellung mit anzugeben ist, auf einem sicheren Transportweg zur Verfügung. Der Leitfaden für die Ausbildungsstätten empfiehlt den postalischen Versand oder den Versand individueller elektronischer Nachrichten über das jeweilige Campus Management bzw. Schulinformationssystem. Offensichtlich wird im Leitfaden davon ausgegangen, dass diese Systeme hinsichtlich der Übertragungswege und möglicher Zugriffe datenschutzgerecht und sicher sind, was nach Erfahrung der Datenschutzkonferenz nicht durchgehend garantiert sein dürfte.

§ 8 Absatz 2 VO-E und § 5 Absatz 2 VwV-E schreiben vor, dass die durch den Generator erzeugte PIN von der Ausbildungsstätte nur herausgegeben werden darf, wenn die anspruchsberechtigte Person ihre Identität mit einem amtlichen Lichtbildausweis oder auf andere geeignete Weise nachgewiesen hat. Welche Alternativen geeignet sind, bleibt offen. Im Leitfaden für die Ausbildungsstätten wird der Identitätsnachweis dagegen nur als „soll“ verlangt.

Weiterhin werden im Leitfaden für die Ausbildungsstätten die persönliche Übergabe der PIN, die Zustellung per Briefpost oder die elektronische Übersendung über ein IT-System der Ausbildungsstätte vorgesehen. Auch andere Versandalternativen sind zugelassen. Insbesondere wird bei einem hohen administrativen Aufwand vorgeschlagen, die PINs pauschal allen anspruchsberechtigten Personen zuzustellen und nicht nur denen, die diese auch tatsächlich benötigen.

Die Datenschutzkonferenz weist darauf hin, dass durch die Kenntnis von Zugangsschlüssel und PIN jede Person mit einer gültigen E-Mail-Adresse einen Antrag auf Zahlung der Energiepreispauschale stellen kann. Zur Verhinderung von Missbrauch sind an die Sicherheit der Übermittlung der Zugangsschlüssel und der PINs hohe Anforderungen zu stellen. Auf Ausnahmen sollte verzichtet werden. Soweit § 5 Absatz 2 VwV-

E die Länder für die Sicherstellung des sicheren Transportweges der Zugangsschlüssel bzw. PINs in die Pflicht nimmt, ist darauf hinzuweisen, dass den Ausbildungsstätten die Aufgabe der Übermittlung zukommt.

3. Ausschließliche Nutzung des OZG-Nutzerkontos Bund

§ 6 VO-E legt fest, dass eine Antragstellung zur Auszahlung der Energiepreispauschale ausschließlich auf elektronischem Weg erfolgt. Hierbei muss jede anspruchsberechtigte Person (bzw. ein vertretungsberechtigter Dritter) ein Nutzerkonto „bund.ID“ anlegen und sich gemäß § 7 VO-E entweder über ein Elster-Zertifikat oder den elektronischen Identitätsnachweis ausweisen. Alternativ kann als Identifizierungsmittel gemäß § 8 VO-E auch die durch den Zugangscode-Generator erzeugte PIN genutzt werden, vermutlich ebenfalls beim Nutzerkonto „bund.ID“. Gemäß § 3 Absatz 3 VwV-E sind jedenfalls andere OZG-Nutzerkonten ausgeschlossen.

Aus Sicht der Datenschutzkonferenz sollte der Zwang zur Verwendung des Nutzerkontos „bund.ID“ überdacht werden, auch wenn die Zielgruppe der Zahlungen technikaffin und elektronischen Verfahren gegenüber aufgeschlossen sein dürfte. Nicht zuletzt sieht auch die Kurzbeschreibung der Verarbeitungsprozesse in Ausnahmefällen einen „Sonderweg“ vor. Hierfür fehlen allerdings Festlegungen, wie der Abgleich mit den Rohdatenlisten erfolgt.

4. Unzureichende Aussagen zu Aufbewahrungsfristen und zur Löschung von Daten

Die vorliegenden Dokumente enthalten unzureichende und inkonsistente Festlegungen, wann die im Zusammenhang mit der Umsetzung des Gesetzes verarbeiteten personenbezogenen Daten zu löschen sind. § 4 Absatz 1 VwV-E enthält etwa die Vorgabe, dass die Daten mindestens bis zum 30.09.2024 in den Fachverfahren der Länder zu speichern sind. Gemäß § 16 Absatz 2 VwV-E endet die Verwaltungsvereinbarung jedoch am 30.06.2024 – was mit den Daten passiert, bleibt offen. § 14 Absatz 2 VO-E verlangt von den Ausbildungsstätten, die Rohdatenlisten (u. a. mit Zugangsschlüsseln und PINs) nach Beendigung der Bewilligungsverfahren, spätestens jedoch

zum 31.12.2023 zu löschen. Der Antragszeitraum endet gemäß § 2 Absatz 2 EPPSG jedoch am 30.09.2023. Insgesamt erschließen sich die genannten Fristen nicht in vollem Umfang.

Die Datenschutzkonferenz fordert die beteiligten Verantwortlichen in Bund und Ländern auf, im Vorhinein konkrete und ggf. differenzierte Regelungen zur Löschung personenbezogener Daten zu treffen und in Form eines klaren und handhabbaren Löschkonzepts umzusetzen. Diese Regelungen müssen die unterschiedlichen Rollen der jeweiligen Stellen (z. B. Ausbildungsstätten, zuständige Stellen in den Ländern als Betreiber der Fachverfahren, Betreiber der zentralen Antragsplattform) genauso berücksichtigen wie die einzelnen Datenkategorien und die Erforderlichkeit der Aufbewahrung (z. B. Rohdaten, Zugangsschlüssel, PINs, Antragsdaten, Bewilligungs- bzw. Ablehnungsbescheide, persönliche Antragskonten auf der zentralen Antragsplattform).