UNABHÄNGIGES
DATENSCHUTZ
ZENTRUM SAARLAND

Saarbrücken, 6. März 2023

Az.:
Bearbeiter/in: [redacted]
Durchwahl:
E-Mail:

Vorschlag zur Risikoabschätzung des Fachverfahrens EPPSG

Einleitung

Gemäß Art. 35 Abs. 1 ist bei Verfahren, die aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen beinhalten, durch den Verantwortlichen vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Mit vorliegender Risikoabschätzung soll ermittelt werden, ob das Fachverfahren EPPSG voraussichtlich hohe Risiken für die Rechte und Freiheiten der betroffenen Antragssteller (Studenten, Fachschüler) beinhaltet, mit der Folge, dass bejahendenfalls eine Datenschutz-Folgenabschätzung (DSFA) durch den Verantwortlichen durchzuführen wäre.

Gegenstand der vorliegenden Risikoabschätzung

[redacted]

Das gesamte Verfahren zur Beantragung und Zahlung einer einmaligen Energiepreispauschale gliedert sich im Wesentlichen in fünf Verfahrenskomplexe. Zunächst sind durch die Ausbildungsstätten Listen mit antragsberechtigten Personen zu erstellen, diese zu verschlüsseln und die so verschlüsselten Listen an die zuständige Stelle (§ 2 Abs. 1 EPPSG) zu übermitteln; zudem erhalten die Antragsberechtigten von der Ausbildungsstätte einen individuellen Zugangsschlüssel. Die zuständigen Stellen plausibilisieren die Listen der Bildungseinrichtungen anhand formaler Kriterien und laden die verschlüsselten Datensätze in das Fachverfahren EPPSG. Die Antragstellung erfolgt über einen Online-Dienst, der vom Bundesland Sachsen-Anhalt bereitgestellt und betrieben wird („Antragsassistent"). Innerhalb dieses Antragassistenten authentifizieren sich die Antragsteller, geben ihre persönlichen Informationen ein. Zudem erfolgt eine erste Validierung der Zugangsschlüssel. Für jeden validen Antrag wird dann im Fachverfahren EPPSG ein Bearbeitungsfall angelegt, über den vollautomatisch entschieden wird. Im Falle einer positiven Entscheidung (Erlass eines Bewilligungsbescheides) werden die Kassendateien erzeugt und zur Auszahlbarmachung an die Bundeskasse übermittelt.

Gegenstand der vorliegenden Risikoabschätzung sind ausschließlich die Verarbeitungsvorgänge, die in die Verantwortung der zuständigen Stelle (§ 2 Abs. 1 EPPSG) fallen („Fachverfahren EPPSG"). Nicht betrachtet werden

daher die Generierung der Listen auf Seiten der Ausbildungsstätten, die Datenverarbeitung im Zusammenhang mit dem Antragsassistenten sowie die Datenverarbeitung bei der Bundeskasse. Die entsprechenden Verantwortlichen müssen in eigener Verantwortung eine Risikoabschätzung und ggfs. eine DSFA durchführen.

Vorwegnahme nach § 14 Abs. 1 SDSG

Gemäß § 14 Abs. 1 SDSG kann eine DSFA unterbleiben, soweit eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Ministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Datenschutz-Folgenabschätzung erfolgt ist, es sei denn, dass dies in der Rechtsgrundlage ausdrücklich bestimmt ist. Zwar sind die oben skizzierten Verfahrensabläufe in der EPPSG-VO vorgegeben. Eine DSFA wurde im Rechtssetzungsverfahren zur EPPSG-VO jedoch nicht durchgeführt. In Frage kommt daher nur der Ausnahmetatbestand nach § 14 Abs. 1 Nr. 1 SDSG. Denn als Anlage 4 des Datenschutzkonzepts hat das Land Sachsen-Anhalt den Entwurf einer DSFA vorgelegt.

Wenn man davon ausgeht, dass das Land Sachsen-Anhalt im Auftrag der Länder die Entwicklung des Online- und Fachverfahrens EPPSG übernommen hat, ließe sich argumentieren, dass diese Beauftragung konkludent auch die Ermächtigung enthält, die DSFA durchzuführen. Insbesondere weil bei Sachsen-Anhalt zusammen mit der Entwicklerfirma allein das notwendige Detailwissen über die technischen und organisatorischen Abläufe der unterschiedlichen Verarbeitungsvorgänge existiert, um eine solche DSFA auch belastbar durchführen zu können.

Derzeit noch hinderlich ist allerdings der Reifegrad der als DSFA bezeichneten Anlage zum Datenschutzkonzept. Dem Entwurf der DSFA vom 14.02.2023 mangelt es derzeit noch an wesentlichen von Art. 35 Abs. 7 DSGVO verlangten Inhalten. Insbesondere die bereits enthaltene funktionale Beschreibung des Verarbeitungsverfahrens im Entwurf kann die von Art. 35 Abs. 7 lit. a DSGVO verlangte systematische Beschreibung der geplanten Verarbeitungsvorgänge nicht ersetzen, mit der Folge, dass auch die enthaltene Risikoermittlung und -bewertung nicht nachvollzogen kann. Erforderlich wäre eine konkrete Bezeichnung und Beschreibung der Wirtschaftsgüter, Schnittstellen und Übertragungswege, auf die sich die Verarbeitung personenbezogener Daten stützt (Hardware, Software, Netzwerke, Personen, Übertragungsmedien, -wege).

Sollten die vorgenannten Defizite im Rahmen weiterer Iterationen der Dokumentation behoben werden, erscheint die Anwendung von § 14 Abs. 1 SDSG vertretbar. Derzeit liegen h.E. die Voraussetzungen des § 14 Abs. 1 SDSG jedoch nicht vor.

Durchführung einer DSFA obligatorisch

Gemäß Art. 35 Abs. 3 DSGVO ist die Durchführung einer DSFA obligatorisch, wenn eines der dort genannten Regelbeispiele erfüllt ist. Alternativ ist eine DSFA zwingend durchzuführen, wenn sich das beabsichtigte Verfahren

auf der nach Art. 35 Abs. 4 DSGVO von den Aufsichtsbehörden zu erlassenen Blacklist findet. Beide Voraussetzungen sind hier nicht erfüllt.

Schwellwertanalyse

Auch wenn nach den vorgenannten Schritten keine DSFA erforderlich ist, muss im Rahmen einer Schwellwertanalyse geprüft werden, ob nach den Kriterien des Art. 35 Abs. 1 DSGVO gegebenenfalls gleichwohl eine hochriskante Verarbeitungstätigkeit ausgeübt wird. In den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt'" (WP 248, Stand 04.10.2017) schlägt die Art. 29-Datenschutzgruppe ein heuristisches Verfahren vor. Danach erfolgt die Einordnung der Verarbeitungstätigkeit anhand von 10 Kriterien. Je mehr dieser 10 Kriterien erfüllt sind, desto eher die Wahrscheinlichkeit, dass der geplante Verarbeitungsvorgang ein hohes Risiko für die Rechte und Freiheiten von Betroffenen mit sich bringt und somit die Durchführung einer DSFA erforderlich ist. Im Regelfall wird jedoch bereits das Vorliegen von zwei Kriterien die Durchführung einer DSFA obligatorisch machen. Gleichzeitig soll eine DSFA eher die Ausnahme als die Regel sein, mit der Folge, dass die 10 Kriterien eher restriktiv auszulegen sind.

- Verarbeitungen zum Bewerten oder Einstufen
  Unter dieses Kriterium fällt das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von *„Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen"* (ErwG 70 und 91 DS-GVO). Dieses Kriterium ist hier nicht erfüllt.

- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
  Verarbeitung, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „die Rechtswirkung gegenüber natürlichen Personen entfalten" oder diese „in ähnlich erheblicher Weise beeinträchtigen" (Artikel 35 Absatz 3 Buchstabe a DSGVO). Auch im Bereich der Leistungsverwaltung kann dieses Kriterium erfüllt sein, da – wenn der Betroffene einen Rechtsanspruch hat - auch die Ablehnung die betroffene Person beeinträchtigt. Verarbeitungsvorgänge hingegen, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium. Dies ist insbesondere dann der Fall, wenn die automatisierte Entscheidung – wie hier – anhand fester, gesetzlich vorgegebener Kriterien (§ 1 EPPSG) erfolgt. In diesen Fällen besteht dann kein spezielles Risiko aufgrund der Automatisierung.

- Systematische Überwachung
  Dies sind Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „eine systematische [...]

Überwachung öffentlich zugänglicher Bereiche" (Art. 35 Abs. 3 lit. c) zurückgreifen. Beides ist hier nicht einschlägig.

- Vertrauliche Daten oder höchst persönliche Daten
  Hierzu zählen besondere Kategorien personenbezogener Daten (Art. 9 DSGVO sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten – Art. 10 DSGVO), aber auch Finanzdaten, die für Zahlungsbetrug missbraucht werden könnten, unterfallen diesem Kriterium. Die zuständige Stelle verarbeitet hier die IBAN der Antragsberechtigten, um die Auszahlung bewirken zu können. Dieses Kriterium dürfte daher hier erfüllt.

- Datenverarbeitung in großem Umfang
  Zwar ist „in großem Umfang" in der DSGVO nicht definiert, aber Erwägungsgrund 91 liefert einige Hinweise. Letztlich wird man aus Sicht der jeweils verantwortlichen Stelle eine Gesamtbewertung unter Einbeziehung der Zahl der Betroffenen, der verarbeiteten Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente, der Dauer oder Dauerhaftigkeit der Datenverarbeitung sowie des geografischen Ausmaßes der Datenverarbeitung anstellen müssen.

  Von den drei Verantwortlichen bzw. zuständigen Stellen im Saarland dürfte das [redacted] als für den tertiären Bildungsbereich zuständige Stelle mit ca. 30.000 Antragsberechtigten die größte Zahl an Daten Betroffener verarbeiten. Auch wenn keine konkreten Schwellenwerte[1] existieren, dürfte allein die Anzahl von 30.000 Betroffenen noch keine Verarbeitung in großen Umfang ausmachen. Auch der reduzierte Datenkranz aus Namen, Adresse und Bankdaten sprechen gegen einen großen Umfang der Verarbeitung, ebenso wie die kurze Verarbeitungsdauer (sofortige Bescheidung und ggf. Zahlbarmachung, Ausschlussfrist 30. September 2023). In der Gesamtschau stellt die geplante Verarbeitung somit h.E. keine Datenverarbeitung in großem Umfang dar.

- Abgleichen oder Zusammenführen von Datensätzen
  Dieses Kriterium betrifft Datensätze, die aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht.

  Im vorliegenden Verfahren erfolgt ein bundesländerübergreifender Abgleich, ob bereits bei anderen zuständigen Stellen ein Antrag auf Zahlung der Energiepreispauschale gestellt wurde („Duplettenprüfung"). Es dürfte allerdings nicht über die vernünftigen Erwartungen der Betroffenen

[1] In der Blacklist des BfDI (Version 1.0-BfDI vom 23.05.2018) ging der Bundesbeauftragte noch von einem Schwellenwert von 5.000.000 Betroffenen bzw. 40% der betroffenen Personengruppe aus. Auch wenn der BfDI an diesem Schwellenwert in der neuesten Fassung seiner Blacklist (Version 1.1-BfDI vom 01.10.2019) nicht mehr festhält, dürfte weiterhin einen Betroffenenzahl im Mio.-Bereich notwendig sein.

hinausgehen, dass sichergestellt wird, dass Antragsberechtigte die Leistung nach dem EPPSG nur einmal beantragen können, zumal nach hiesigem Erkenntnisstand auf diesen Abgleich vorab und frühzeitig im Antragsprozess hingewiesen wird. Dieses Kriterium ist daher hier nicht erfüllt.

- Daten zu schutzbedürftigen Betroffenen

  Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein größeres Machtungleichgewicht vorliegt; d. h. den Personen ist es unter Umständen nicht ohne weiteres möglich, der Verarbeitung ihrer Daten zuzustimmen bzw. zu widersprechen oder ihre Rechte auszuüben. Auch die Verarbeitung personenbezogener Daten von Kindern oder auch Minderjährigen kann dieses Kriterium erfüllen. Dies beruht auf der Erwägung, dass bei ihnen nicht davon ausgegangen werden kann, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zu widersprechen bzw. zuzustimmen.

  Da auch Fachschülerinnen und Fachschüler antragsberechtigt sind, ist es denkbar, dass auch Daten zu Minderjährigen im Fachverfahren EPPSG verarbeitet werden. Allerdings ist zweifelhaft, ob diese in der konkreten Situation schutzbedürftig sind. Denn im Rahmen der Beantragung der Energiepreispauschale besteht zwischen den eventuell minderjährigen Antragstellern und der zuständigen Stelle kein Machtungleichgewicht, das die Betroffenen an der Ausübung ihrer Rechte hindern könnte. Ganz im Gegenteil geht der Gesetzgeber davon aus, dass auch minderjährige Studierende und Fachschüler in der Lage sind, einen Antrag nach § 2 Abs. 1 EPPSG zu stellen. Warum dies bei der Geltendmachung datenschutzrechtlicher Betroffenenrechte anders sein sollte, leuchtet nicht ein. Nach hiesiger Auffassung ist dieses Kriterium daher hier nicht erfüllt.

- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen

  Aus der DSGVO (Art. 35 Abs. 1, ErwG 89 und 91) wird deutlich, dass der Einsatz einer neuen Technologie der Grund für die Notwendigkeit einer DSFA sein kann. Das liegt daran, dass der Einsatz einer solchen Technologie mit neuartigen Formen der Datenerfassung und -nutzung einhergehen kann, was möglicherweise ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt. Schließlich sind die persönlichen und gesellschaftlichen Folgen, die der Einsatz einer neuen Technologie haben kann, kaum absehbar.

  Die automatisierte, anhand fester vorgegebener Kriterien erfolgende Bescheidung im Fachverfahren EPPSG stellt keine neuartige technische oder organisatorische Lösung dar. Anders wäre dies etwa beim Einsatz von künstlicher Intelligenz zu bewerten. Hier jedoch handelt es sich lediglich um ein Verfahren der Prozessautomatisierung, das – nach hiesigem Kenntnisstand - weder technisch noch organisatorisch neuartige Ansätze implementiert.

- Hürde für den Betroffenen, ein Recht auszuüben bzw. einen Dienst nutzen

  Hierzu zählen Verarbeitungsvorgänge, die an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern". Die Dublettenprüfung stellt keinen Verarbeitungsvorgang im vorgenannten Sinne dar, da sie lediglich darauf abzielt die Antragsberechtigung festzustellen. Da die Energiepreispauschale nur „einmalig" (§ 1 Abs. 1 EPPSG) gewährt wird, zielt dieser Verarbeitungsvorgang nicht darauf ab, den Betroffenen von der Geltendmachung eines Rechts abzuhalten, da bei Doppeleinreichung schon kein Anspruch / Recht besteht.

- Verarbeitung außerhalb des EWR

  Dieses Kriterium beruht auf der Erwägung, dass bei einer Verarbeitung personenbezogener Daten außerhalb des EWR die Gefahr besteht, dass das durch die DSGVO gewährleistete Schutzniveau untergraben wird. Insbesondere unter Anwendung alternativer Transferinstrumente nach Artt. 46, 47 & 49 DSGVO können diese in Konflikt zu den rechtlichen Vorgaben im Drittstaat stehen, denen der Verantwortliche oder einer seiner Auftragsverarbeiter unterliegt. Die sich hieraus ergebenden Risiken, bspw. eines Zugriffs der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten müssen daher im Rahmen einer DSFA adressiert werden.

  Im Fachverfahren EPPSG ist in wenigen Ausnahmefällen im Rahmen eines Second-Level-Supports eine Übermittlung personenbezogener Daten an einen Auftragsverarbeiter im Vereinigten Königreich (UK) vorgesehen. Für UK existiert ein Angemessenheitsbeschluss (Art. 45 Abs. 1 DSGVO) der Europäischen Kommission, mit dem diese festgestellt hat, dass die Rechtslage dort ein Schutzniveau gewährleistet, das dem durch die DGSVO garantierten Niveau der Sache nach gleichwertig ist. Es ist daher im Fall von UK nicht notwendig die Defizite im Drittstatt durch alternative Transferinstrumente zu kompensieren bzw. entsprechende Risiken im Rahmen der Durchführung einer DSFA zu betrachten.

  H.E. ist das vorliegende Kriterium im Falle eines Angemessenheitsbeschlusses nach Art. 45 Abs. 1 DSGVO bei der Schwellwertanalyse nicht zu berücksichtigen.

Ergebnis

Die Schwellwertanalyse hat ergeben, dass lediglich eines („Vertrauliche Daten oder höchst persönliche Daten") der 10 Kriterien beim Fachverfahren EPPSG erfüllt ist. Auch darüber hinaus sind keine weiteren hohen Risiken für die Rechte und Freiheiten der betroffenen Personen erkennbar. Die Durchführung einer DSFA ist daher hier nicht erforderlich.