UNABHÄNGIGES DATENSCHUTZZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Straße 12 . 66111 Saarbrücken
Postfach 10 26 31 . 66026 Saarbrücken
Telefon 0681/94781 – 0
Telefax 0681/94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de

Unabhängiges Datenschutzzentrum Saarland - Fritz-Dobisch-Str. 12 - 66111 Saarbrücken

Ministerium der Finanzen
und für Wissenschaft
Herrn Staatssekretär Wolfgang Förster
Am Stadtgraben 6-8

66111 Saarbrücken

Saarbrücken, 6. Januar 2023

Az: DS.9.4-2023-39
Bearbeiter/in: Herr Gisch
Durchwahl: -12
E-Mail: gisch@datenschutz.saarland.de

Studierenden-Energiepreispauschalengesetz - EPPSG

Sehr geehrter Herr Förster,

für das neue Jahr wünsche Ihnen ebenfalls alles Gute und freue mich auf eine weiterhin gute Zusammenarbeit.

In der oben genannten Angelegenheit wurden wir durch Ihr Haus dankenswerterweise bereits vorab beteiligt. Am 19. Dezember 2022 fand auf Einladung des Ministeriums der Finanzen und für Wissenschaft eine erste Vorstellung des geplanten Verfahrens statt, in der auch schon erste datenschutzrechtliche Implikationen angerissen werden konnten.

Wir hatten im Rahmen des damaligen Termins bereits auf potenzielle datenschutzrechtliche Probleme hingewiesen, die aus der gesamtheitlichen Zurverfügungstellung der personenbezogenen Daten aller Anspruchsberechtigten an die nach § 2 Abs. 1 EPPSG durch Landesrecht zu bestimmende, zuständige Stelle herrühren. Zum damaligen Zeitpunkt war allerdings noch unklar, ob tatsächlich personenbezogene Daten der Anspruchsberechtigten an die zuständige Stelle übermittelt werden sollen oder ob nicht nur der so genannte Zugangsschlüssel übertragen werden soll. Nach Auswertung der uns von Ihnen mit Schreiben vom 3. Januar 2023 übersandten Unterlagen, insbesondere der Kurzbeschreibung „Gesamtprozess Einmalzahlung“, dem Entwurf der sich in Länderabstimmung befindlichen Verordnung (EPPSG-VO) und dem Entwurf der Rohdatenliste – Mustervorlage scheint der derzeitige Planungsstand eine Übermittlung von Namen, Geburtsdaten,

Adressinformationen, sonstige Kontaktdaten (E-Mail, Telefon) sowie der Matrikelnummer aller Anspruchsberechtigten vorzusehen.

Bevor ich auf unsere datenschutzrechtliche Bewertung dieser Übermittlung an die nach § 2 Abs. 1 EPPSG zu bestimmende zuständige Stelle eingehe, möchte ich beschreiben, wie wir den Prozess der Erstellung der sog. Rohdatenlisten technisch verstehen und interpretieren. Insbesondere zur Frage der Art und Weise der Verschlüsselung finden sich in der Kurzbeschreibung des Gesamtprozesses bisher keine detaillierten technischen Angaben, so dass ich es für notwendig halte zunächst darzulegen, von welchen technischen Annahmen wir bei der folgenden datenschutzrechtlichen Bewertung ausgehen.

Generierung der Rohdatenliste / Liste mit verschlüsselten Daten für das Fachverfahren

Der Prozess der Generierung der sog. Rohdatenlisten ist in den §§ 3, 5 Abs. 1 EPPSG–VO und unter Schritt zwei der Kurzbeschreibung des Gesamtprozesses näher beschrieben. Danach sollen die Ausbildungsstätten zunächst Listen mit allen Anspruchsberechtigten und einem definierten Datenkranz aus ihren Campus- bzw. Schul-Informationssystemen erstellen und exportieren (§ 3 Abs. 1 EPPSG-VO). Unklar ist derzeit noch der konkrete Datenumfang. Die mitgesendete Mustervorlage enthält einen sehr umfassenden Datenkranz, § 3 Abs. 3 EPPSG-VO spricht daneben von mindestens Vorname, Nachname, Geburtsort und Geburtsdatum. Die Kurzbeschreibung schließlich erwähnt ebenfalls Name und Geburtsdaten der Anspruchsberechtigten als in die Rohdatenliste aufzunehmende Personendaten.

Diese Rohdatenliste wirddann durch die Ausbildungsstätte mit einer eigens hierfür zur Verfügung gestellten Offline-Anwendung (sog. Zugangscode-Generator) um sog. Zugangsschlüssel (§ 5 EPPSG-VO) angereichert, indem zu jedem Datensatz eines Anspruchsberechtigten jeweils ein Zugangsschlüssel generiert wird. Die Verwendung des Begriffs Offline-Anwendung soll dabei wohl implizieren, dass diese Anwendung keine Daten an andere Stellen überträgt. Bei diesen individuellen Zugangsschlüsseln handelt es sich um eine Zahlen- und Buchstabenkombination. In der Kurzbeschreibung des Gesamtprozesses findet sich ein Beispiel eines solchen Zugangsschlüssels (dort als Zugangscode bezeichnet). Demnach handelt es sich um eine 36-stellige Buchstaben-Ziffernkombination, die an den Positionen 9, 14, 19 und 24 ein Trennzeichen enthält (32 alphanumerische Zeichen plus 4 Trennzeichen).[1]

Die (technische) Funktion dieses Zugangsschlüssels, der aus datenschutzrechtlicher Sicht wohl als Pseudonym zu qualifizieren ist, ist in der Kurzbeschreibung des Gesamtprozesses wie folgt beschrieben: „Antragsberechtigte auf der Gesamtplattform zu identifizieren". Nach hiesigem Verständnis handelt es sich bei dem Zugangsschlüssel

[1] Zusätzlich wird eine obligatorische persönliche Identifikationsnummer (PIN) von unbekannter Länge generiert (in der Kurzbeschreibung des Gesamtprozesses ist dieser Schritt noch als optional bzw. fakultativ dargestellt). Diese PIN ist für die datenschutzrechtliche Bewertung jedoch nicht von Relevanz.

daher um einen Universally Unique Identifier (UUID), also um eine nach standardisierten Verfahren (ISO/IEC 9834-8:2005 bzw. RFC 4122) generierte global eindeutige 128-bit-Zahl, die den zu einer bestimmten anspruchsberechtigten Person gehörenden Datensatz der Rohdatenliste eindeutig referenziert.

Demgegenüber handelt es sich bei dem Zugangsschlüssel – auch wenn die Bezeichnung als „..s*chlüssel*" dies suggeriert – *nicht* um einen kryptographischen Schlüssel. Insbesondere wird der Zugangsschlüssel nach hiesigem Verständnis *nicht* dazu verwendet, um den einzelnen Datensatz jedes Anspruchsberechtigten individuell zu verschlüsseln. Für Art und Umfang der Verschlüsselung spielt der Zugangsschlüssel keine Rolle.

Zwar ist das in der EPPSG-VO erwähnte Verschlüsselungsverfahren in den übersandten Unterlagen nicht im Detail beschrieben. Sowohl § 3 Abs. 2 EPPSG-VO als auch § 5 Abs. 1 Satz 3 EPPSG-VO verlangen aber, dass die Verschlüsselung lediglich auf die (Gesamt)Liste anzuwenden ist, die von der Ausbildungsstätte an die nach § 2 Abs. 1 EPPSG zu bestimmende zuständige Stelle übermittelt wird. Nach hiesigem Verständnis ist hingegen eine Verschlüsselung auf Datensatzebene derzeit nicht vorgesehen. Mithin soll die in der EPPSG-VO derzeit schon vorgesehene Verschlüsselung wohl lediglich den Transportweg absichern.

Aus der Rohdatenliste erstellt der Zugangscode-Generator zwei neue Listen (Dateien): eine Liste für den Versand der Zugangsschlüssel durch die Ausbildungsstätte, die bei der Ausbildungsstätte verbleibt, sowie eine weitere Liste mit verschlüsselten Daten für das Fachverfahren, die an die nach § 2 Abs. 1 EPPSG zuständige Stelle übermittelt wird.

Konsequenz aus dem oben geschilderten technischen Ablauf ist, dass nach dem unter Schritt 3 der Gesamtprozessdarstellung erfolgenden Import der von der Ausbildungsstätte zur Verfügung gestellten Liste mit verschlüsselten Daten für das Fachverfahren, die darin enthaltenen personenbezogenen Daten aller Antragsberechtigten in der Datenbank des Fachverfahrens im Klartext vorliegen. Zwar ist es hierfür zunächst erforderlich, dass die nach § 2 Abs. 1 EPPSG zuständige Stelle beim Import der Daten ins Fachverfahren auf irgendeine Weise Kenntnis der kryptographischen Schlüssel erhält, die bei der Erzeugung der verschlüsselten Rohdatenliste auf Seiten der Ausbildungsstätte verwendet wurden (das Verfahren des Schlüsselaustauschs zwischen Ausbildungsstätte und zuständiger Stelle ist bisher nicht beschrieben bzw. dokumentiert). Mit Kenntnis dieses kryptgraphischen Schlüsselmaterials hat die zuständige Stelle aber Zugang zu allen Klartextdaten, die in Schritt 1 aus dem Campus- bzw. Schul-Informationssystem generiert wurden.

Vorläufige datenschutzrechtliche Bewertung

Wie oben ausgeführt, gehen wir nach Auswertung und Interpretation der uns bisher vorliegenden Unterlagen davon aus, dass der nach § 2 EPPSG-VO zuständigen Stelle bereits im Vorfeld und unabhängig vom Vorliegen

eines konkreten Antrags auf Zahlung der Energiepreispauschale personenbezogene Daten aller Anspruchsberechtigten übermittelt werden. Die vorgesehene Verschlüsselung sichert dabei lediglich den Transportweg ab, verhindert allerdings nicht, dass die nach § 2 Abs. 1 EPPSG zuständige Stelle jedenfalls im rechtlichen Sinne bereits zu einem Zeitpunkt, zu dem noch kein Antrag nach § 2 Abs. 2 EPPSG vorliegt, Kenntnis von den Daten aller Anspruchsberechtigten erhält.

Im datenschutzrechtlichen Sinne handelt es sich im Zeitpunkt der Zurverfügungstellung der Liste mit verschlüsselten Daten für das Fachverfahren durch die Ausbildungsstätte um eine rechtfertigungsbedürftige Übermittlung personenbezogener Daten. Erforderlich ist hierfür eine gesetzliche Grundlage, die Art und Umfang der Weitergabe der personenbezogenen Daten aller Anspruchsberechtigten der Ausbildungsstätte an die nach § 2 Abs. 1 EPPSG zuständige Stelle gestattet. Korrespondierend dazu bedarf es einer Rechtsgrundlage, die der nach § 2 Abs. 1 EPPSG zuständigen Stelle die Verarbeitung personenbezogener Daten im vorgenannten Umfang gestattet.

Als Rechtsgrundlage in Betracht kommen die in § 14 iVm § 3 EPPSG-VO genannten Tatbestände.

Allerdings ist bereits zweifelhaft, ob die im Entwurf der EPPSG-VO genannten Rechtsgrundlagen verfassungsrechtlichen Vorgaben standhalten mit der Folge, dass diese schon aus formellen Gründen als Erlaubnisgrundlage im datenschutzrechtlichen Sinne ausscheiden. Jedenfalls mit Blick auf die Verordnungsermächtigung in § 2 Abs. 1 Satz 2 EPPSG bestehen aus hiesiger Sicht doch erhebliche Bedenken, dass hierüber die Normierung datenschutzrechtlicher Verarbeitungstatbestände möglich ist.

Legt man die Maßstäbe des Verfassungsgerichtshofs des Saarlandes zugrunde, so wäre es erforderlich, dass sich aus der Verordnungsermächtigung jedenfalls die zu erhebenden personenbezogenen Daten als solche, der Anlass und der spezifische Zweck der Erhebung, die Art und Dauer der Aufbewahrung sowie die Löschung in normenklarer Weise bestimmen lassen (Verfassungsgerichtshof des Saarlandes, Beschluss vom 28.08.2020, Az. Lv 15/20, Seite 27f.). Daran fehlt es hier.

Dabei kann dahinstehen, ob die Verordnungsermächtigung die vom Verfassungsgerichtshof genannten Kriterien ausdrücklich benennen muss oder ob es ausreicht, dass sich die Grenzen der durch die Verordnungsermächtigung ermöglichten Datenverarbeitung durch Auslegung ermitteln lassen. Denn vorliegend lassen sich auch aus den Gesetzesmaterialien keine Anhaltspunkte dafür entnehmen, zu welchem Zeitpunkt (Anlass) und in welchem Umfang personenbezogene Daten der Anspruchsberechtigten durch die Ausbildungsstätte übermittelt und bei der nach § 2 Abs. 1 EPPSG zuständigen Stelle verarbeitet werden dürfen. Neben der Unsicherheit mit Blick auf den zur Verfügung zu stellenden Datenkranz (nach § 3 Abs. 3 EPPSG-VO sollen **mindestens** die dort genannten Datenfelder exportiert werden) ist hier insbesondere von datenschutzrechtlicher Relevanz, dass die Daten aller Anspruchsberechtigten bereits vorab, und damit ohne das Vorliegen eines konkreten Antrags lediglich in der (zugegebenermaßen wohl berechtigten) Annahme, dass die

überwiegende Mehrheit aller Anspruchsberechtigten einen entsprechenden Antrag stellen wird und daher die Daten jedenfalls zu einem späteren Zeitpunkt erforderlich sein werden, übermittelt und durch die nach § 2 Abs. 1 EPPSG zuständige Stelle in Erwartung einer späteren Antragstellung verarbeitet werden. Die Befugnis zur Regelung einer solchen vorsorglichen Datenverarbeitung lassen sich nach hiesiger Auffassung nicht aus der Verordnungsermächtigung des § 2 Abs. 1 Satz 2 EPPSG entnehmen. Die Regelungen des § 14 EPPSG-VO scheiden daher als datenschutzrechtliche Erlaubnisgrundlage aus.

Aus den vorgenannten Gründen ist auch ein Rückgriff auf die Generalklausel des § 4 SDSG nicht möglich. Im Rahmen der Erforderlichkeit wäre auch nach § 4 SDSG eine Übermittlung der Daten eines individuellen Anspruchsberechtigten durch die Ausbildungsstätte erst im Zeitpunkt der konkreten Antragstellung zulässig. Zudem käme § 4 SDSG ausschließlich bei staatlichen Ausbildungsstätten nicht jedoch bei etwaigen privaten Ausbildungsstätten zur Anwendung.

Ergebnis

Zusammenfassend sehen wir nach unserer vorläufigen datenschutzrechtlichen Bewertung derzeit keine Rechtsgrundlage für eine vorsorgliche Übermittlung der personenbezogenen Daten aller Anspruchsberechtigten an die nach § 2 Abs. 1 EPPSG zuständige Stelle, ohne dass ein konkreter Antrag nach § 2 Abs. 2 EPPSG bereits dort vorliegt. Insofern wäre die Schaffung einer entsprechenden Rechtsgrundlage im Bundes- oder Landesrecht notwendig.

Als Alternative zu einer legislativen Lösung ist aber auch eine technische Lösung denkbar, um den datenschutzrechtlichen Anforderungen gerecht zu werden. Eine solche Lösung könnte nach hiesiger Auffassung darin bestehen, dass die der nach § 2 Abs. 1 EPPSG zuständigen Stelle von der Ausbildungsstätte zur Verfügung gestellten Datensätze individuell verschlüsselt werden, und nicht wie derzeit geplant nur die Gesamtliste (siehe oben). Eine solche Lösung hätte den Vorteil, dass die personenbezogenen Daten der Anspruchsberechtigten erst im Zeitpunkt der Antragstellung durch ein vom Antragsteller einzugebendes Passwort durch die nach § 2 Abs. 1 EPPSG zuständige Stelle entschlüsselt werden könnten. Bis zu diesem Zeitpunkt lägen dort nur verschlüsselte Daten vor.

Eine solche technische Lösung würde im Detail wie folgt aussehen: Neben dem in Schritt 1 pro Anspruchsberechtigten zu erstellenden Zugangsschlüssel müsste der Zugangscode-Generator auch ein individuelles Passwort zufällig generieren. Dieses Passwort dürfte nicht an die nach § 2 Abs. 1 EPPSG zuständige Stelle übermittelt werden, sondern würde allein in der Liste für den Versand der Zugangsschlüssel durch die Ausbildungsstätte verbleiben und lediglich dem Anspruchsberechtigten zusammen mit dem Zugangsschlüssel mitgeteilt werden. Aus diesem zufälligen Passwort würde der Zugangscode-Generator auf der Grundlage eines standardisierten Algorithmus (bspw. PBKDF2 oder einer anderen Funktion zur Schlüsselableitung - (Key

derivation function)) einen kryptographischen Schlüssel generieren bzw. ableiten. Mit Hilfe diese kryptographischen Schlüssel würde der Zugangscode-Generator die personenbezogenen Daten aus dem Campus- bzw. Schul-Informationssystem individuell je Anspruchsberechtigten symmetrisch (bspw. mittels AES-256 oder höher) verschlüsseln und danach den erzeugten kryptographischen Schlüssel verwerfen. Die Ausbildungsstätte würde dann lediglich die individuell verschlüsselten Datensätze zusammen mit den zugehörigen Zugangsschlüsseln an die nach § 2 Abs. 2 EPPSG zuständige Stelle übermitteln. Dort lägen bis zur Antragstellung nur verschlüsselte Daten der Anspruchsberechtigten vor.

Für die Antragstellung müsste der Antragsberechtigte, anders als bisher in § 10 Abs. 3 EPPSG-VO vorgesehen, nicht nur seinen ihm von der Ausbildungsstätte mitgeteilten Zugangsschlüssel eingeben, sondern auch das dann ebenfalls mitgeteilte dazugehörige Passwort. Das dahinterliegende IT-System würde mittels des Zugangsschlüssels den passenden, zu diesem Zeitpunkt noch verschlüsselten Datensatz selektieren und könnte diesen dann mittels des ebenfalls vom Antragsberechtigten zur Verfügung gestellten Passworts entschlüsseln, um so Zugriff auf die Klartextdaten zu erhalten und das weitere Verwaltungsverfahren zu durchlaufen. Hierfür würde das IT-System aus dem vom Antragsteller zur Verfügung gestellten Passwort ebenfalls (wie bereits der Zugangscode-Generator) mittels bspw. PBKDF2 einen bzw. den richtigen kryptographischen Schlüssel ableiten und könnte so den verschlüsselten Datensatz entschlüsseln.

Denkbar wäre auch, dass man anstatt eines zufällig generierten Passworts die bereits in der EPPSG-VO vorgesehene PIN verwendet. Mittels PBKDF2 könnte auch hieraus ein kryptographischer Schlüssel generiert werden. Allerdings wären dann noch - insbesondere zur Vermeidung von Brute-Force-Angriffen - zusätzliche Vorgaben hinsichtlich der Länge der PIN zu machen und diese PIN dürfte, anders als derzeit noch vorgesehen, nicht an die nach § 2 Abs. 1 EPPSG zuständige Stelle übermittelt werden.

Auch unabhängig von einem gesetzgeberischen Tätigwerden stellt das vorbeschriebene Verfahren eine datenschutzfreundliche Lösung dar, die den Risiken, die sich aus zentralen Datenbeständen für die Rechte und Freiheiten der hiervon betroffenen Personen ergeben, wirksam begegnet. Insofern regen wir an, auch im Falle der Schaffung der notwendigen Rechtsgrundlagen durch den Bundes- oder Landesgesetzgeber sich ergänzend für die oben vorgeschlagene technische Realisierung einzusetzen.

Neben den obigen Ausführungen zur datenschutzrechtlichen Zulässigkeit der Übermittlung der personenbezogenen Daten der Ausbildungsberechtigten, ist aus hiesiger Sicht auch noch offen, wie das Verhältnis zwischen der nach § 2 Abs. 1 EPPSG zuständigen Stelle und dem Betreiber des IT-Systems rechtssicher datenschutzrechtlich ausgestaltet sein wird. Hierzu liegen uns bisher jedoch keine Informationen vor, die eine datenschutzrechtliche Einschätzung erlauben.

Gerne stehen wir für Rückfragen und / oder zusätzliche Erläuterungen zur Verfügung.

Herrn Staatssekretär Benedyczuk leite ich ebenfalls eine Kopie dieses Schreibens zu.

Mit freundlichen Grüßen

Monika Grethel
Landesbeauftragte für Datenschutz
und Informationsfreiheit