Datenschutz-Folgenabschätzung (DSFA)

Verfahrensbezeichnung: Online-Antragstellung EPPSG-Einmal-zahlung im Antragsverfahren

Version:

Bearbeiter/in	Organisationseinheit	Datum

Inhalt

1 Prüfung der Erforderlichkeit einer DSFA

Erforderlichkeit nach Art. 35 Abs. 3 DSGVO, Beispielliste (bitte ankreuzen)

☐ Verarbeitung personenbezogener Daten zum Zwecke des Profilings[1] oder des Scorings[2]

☐ umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 DSGVO[3] oder Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO[4]

☐ Verarbeitung personenbezogener Daten zum Zwecke einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche

☒ DSFA ist nach der Liste von Verarbeitungsvorgängen des LfD Sachsen-Anhalt nicht erforderlich.[5] Die dort aufgeführten Tatbestände liegen nicht vor. Eine Pflicht zur Durchführung einer DSFA folgt auch nicht aus Art. 35 Abs. 3 DSGVO. Diese Regelbeispiele liegen ebenfalls nicht vor. Gleichwohl sprechen hier gute Gründe dafür, dass eine DSFA aufgrund von Art. 35 Abs. 1 DSGVO erforderlich ist, weil voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit der Datenverarbeitung einhergeht.

Ergebnis

- Trifft eine der genannten Möglichkeiten zu, ist eine DSFA durchzuführen. Die Datenschutzbeauftragte des Verantwortlichen ist zu informieren und beratend einzubeziehen. Bitte fortfahren unter Punkt 2 des Vordrucks.

- Trifft keine der Möglichkeiten zu, bitte fortfahren mit der Schwellwertanalyse unter Punkt 1.2. (Seite 3)

[1] **Profiling** bezeichnet die Erstellung, Aktualisierung und Verwendung von Profilen durch Sammlung von gewonnenen Daten sowie deren anschließende Analyse und Auswertung.

[2] Beim **Scoring** werden anhand von gesammelten Erfahrungen aus der Vergangenheit möglichst zuverlässige Prognosen für die Zukunft erstellt.

[3] pb Informationen über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische, biometrische und Gesundheitsdaten, zum Sexualleben oder der sexuellen Orientierung

[4] pb Informationen über Taten und Strafen nach den strafgesetzlichen Bestimmungen; offen bleibt bisher, ob auch mögliche oder nur vermutete Straftaten und Strafen darunterfallen sollen.

[5] Liste von Verarbeitungsvorgängen gem. Art. 35 Abs. 4 DSGVO für öffentliche Stellen, für die im Zuständigkeitsbereich des Landesbeauftragter für den Datenschutz Sachsen-Anhalt eine DSFA durchzuführen ist: Auf der Internet-Seite des LfD abrufbar.

2 Durchführung der DSFA

2.1 Welche Arten personenbezogener Daten werden verarbeitet? (bitte ankreuzen)

- ☒ personenbezogene Daten einfach[6]
- ☐ personenbezogene Daten sensibel[7]
- ☐ besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO[8]

2.2 Zweck der Verarbeitung

Der „Online-Antrag EPPSG-Einmalzahlung“ unter der Verantwortung des Ministeriums für Infrastruktur und Digitales Sachsen-Anhalt (MID) dient der Assistenz bei der Eingabe der Antragsdaten (Antragsassistent), der Registrierung, der Identifizierung und Authentifizierung der antragsberechtigten Studierenden, (Berufs-) Fachschülerinnen und Fachschülern nach dem Studierenden-Energiepreispauschalengesetz (EPPSG) sowie der Übermittlung der Antragsdaten in die Fachverfahren der Länder bzw. an die zuständigen Stellen der Bundesländer zur Antragsbearbeitung und Einleitung eines Verwaltungsverfahrens. Die Fachverfahren sind ebenfalls Teil der Gesamtplattform. Der Antragsassistent dient der Kanalisierung der Anträge in einer zentralen Stelle, die auf diese Weise eine überlange Verfahrensdauer und Unübersichtlichkeit über die zuständigen Stellen in den Ländern verhindern soll.

Zusammengefasst besteht die Plattform aus Antragsassistenten, über den die Berechtigten ihren Antrag auf Auszahlung der Energiepreispauschale ausfüllen können und den Fachverfahren der Länder, in denen die Antragsprüfung und die Erstellung der Bescheide erfolgt. Der Versand der Bescheide erfolgt per E-Mail an die im Antragssystem angegebene E-Mailadresse der Antragsberechtigten. Die Datenverarbeitung in den Fachverfahren ist nicht Gegenstand dieser DSFA.

Für die Antragstellung erfolgt die Anmeldung mit einem BUND-ID Konto und einem Zugangscode und optional zusätzlich einer PIN, die von den Ausbildungsstätten bereitgestellt werden.

---

[6] personenbezogene (pb) Informationen, deren Schutzbedarf als normal hoch anzusehen ist

[7] pb Informationen, die zwar nicht unter den abschließenden Katalog der besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO fallen, gleichwohl einen erhöhten Schutzbedarf haben, z.B. bei unbefugtem Gebrauch besonders schützenswerte Lebensbereiche betreffen, gravierenden Auswirkungen auf das Ansehen/die Reputation, die finanzielle Situation, die körperliche Unversehrtheit, Diskriminierung/Stigmatisierung haben können

[8] pb Informationen über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische, biometrische und Gesundheitsdaten, zum Sexualleben oder der sexuellen Orientierung

Die Kombination aus Zugangscode und PIN erlaubt es der berechtigten Person, ohne die Onlinefunktion des Personalausweises oder das Elster-Zertifikat, Zugang zum Antrag zu erhalten. Personen mit Zugangscode und PIN benötigen lediglich eine gültige E-Mailadresse. Mit der E-Mailadresse müssen sie sich ein BundID-Konto anlegen, um anschließend den Antrag stellen zu können.

Nutzer mit Zugangscode ohne PIN müssen ihre Identität mit einem BundID-Konto mit hohem Vertrauensniveau (Online-Ausweisfunktion oder persönliches ELSTER-Zertifikat) nachweisen. Die hierbei erfassten und gespeicherten personenbezogenen Daten gewährleisten einen Schutz vor nichtberechtigten Antragstellern.

Darüber hinaus erfolgen das Erfassen und Speichern personenbezogener Daten bereits beim Besuch der Webseite www.einmalzahlung200.de und der Nutzung des Antragsassistenten zur Gewährleistung der Funktionalität sowie zu Analysezwecken im Falle von Angriffen auf die verwendete Kommunikationstechnik. Im Antragsassistenten werden die Antragstellenden aufgefordert, weitere Daten zu ergänzen, die ggf. nicht aus dem bund.id-Benutzerkonto übernommen werden können (wie z.B. Kontodaten oder Kontaktdaten), die aber für den weiteren Verlauf der Antragstellung, insbesondere zur Kontaktaufnahme, benötigt werden. Nach Abschluss der fachlichen Prüfung im Fachverfahren können die zuständigen Stellen der Bundesländer die Bescheide per E-Mail an die im Antragssystem angegebene E-Mailadresse der antragberechtigten Person übermitteln. Bei einer solchen „Kettenverarbeitung“, wenn also verschiedene Akteure, hier das MID Sachsen-Anhalt und die zuständigen Stellen der Länder, nacheinander die gleichen personenbezogenen Daten verarbeiten, liegt keine gemeinsame Verantwortlichkeit vor, vielmehr sind das MID Sachsen-Anhalt und die zuständigen Stellen der Länder dann aufeinanderfolgende, voneinander unabhängige Verantwortliche.

2.3 Rechtsgrundlage(n) für die Verarbeitung

- Besuch der Website: Art. 6 Abs. 1 lit. e DSGVO i. V. m. i.V.m. § 9 Abs. 3 EGovG LSA i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA; § 25 Abs. 2 Nr. 2 TTDSG
- CDN/Waiting Room: Art. 6 Abs. 1 lit. e DSGVO i. V. m. i.V.m. § 9 Abs. 3 EGovG LSA i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA; § 25 Abs. 2 Nr. 2 TTDSG
- Registrierung mittels Zugangscodes ohne PIN: § 8 Abs. 5 S. 1, 2 OZG, Art. 6 Abs. 1 lit. e DS-GVO i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA, teilweise i.V.m. § 3 Abs. 4 VwV-EPPSG

- Registrierung per Zugangscode und PIN: § 8 Abs. 5 S. 1, 2 OZG, Art. 6 Abs. 1 lit. e DS-GVO i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA, teilweise i.V.m. § 3 Abs. 4 VwV-EPPSG
- Verifizierung der E-Mail-Adresse: Art. 6 Abs. 1 lit. e DS-GVO i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA
- Anmeldung: Art. 6 Abs. 1 lit. e DS-GVO i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA
- Kontaktformular: Art. 6 Abs. 1 lit. e DSGVO i. V. m. i.V.m. § 9 Abs. 3 EGovG LSA i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA; § 25 Abs. 2 Nr. 2 TTDSG
- Online-Antragsassistent: Art. 6 Abs. 1 lit. e DS-GVO i.V.m. § 4 S. 1 Nr. 2 1. HS DSAG-LSA

2.4 Geplantes Verarbeitungsverfahren

Durch Nutzung des Antragsassistenten soll es Antragsberechtigten erleichtert werden, die EPPSG-Einmalzahlung zu beantragen.

Zur weiteren Bearbeitung durch die zuständigen Stellen der Länder werden die Antragsdaten über eine Datenschnittstelle direkt an die Fachverfahren des Bundeslandes der zuständigen Stelle verteilt.

Die Sachbearbeitung der Anträge in den zuständigen Stellen der Länder erfolgt dann im Fachverfahren. Die Bearbeitung der Anträge erfolgt in datenschutzrechtlicher Verantwortlichkeit der zuständigen Stellen der teilnehmenden Länder, die nicht Teil der hier beschriebenen reinen Unterstützung der Antragstellung durch den Online-Assistenten ist.

Für die Antragstellung ist eine Registrierung/ Identifizierung durch die Antragsberechtigten im eigenen Namen erforderlich, die auf folgenden Wegen möglich ist, unter Angabe des Bundeslandes der Ausbildungsstätte:

Zugangscode ohne PIN:

Die Registrierung erfolgt über das Nutzerkonto Bund (oder auch „bund.id“). Sofern noch keine bund.id vorhanden ist, muss eine Registrierung zunächst dort erfolgen. Für die Identifizierung im „EPPSG-Portal“ über die bund.id werden die im dortigen Konto verarbeiteten Daten zweckändernd verwendet. Dafür übermittelt das Bundesministerium des Innern und für Heimat (BMI) die dort hinterlegten

Registrierungsdaten an das MID Sachsen-Anhalt, damit mithilfe dieser Daten die Identifizierung für die Antragstellung im „EPPSG-Portal“ durchgeführt werden kann. Im Anschluss werden die bund.id-Registrierungsdaten in den Onlineantrag, der Teil des Antragssystems ist, übernommen und gespeichert.

Zugangscode und PIN:

Die Registrierung erfolgt ebenfalls unter Verwendung der bund.id, jedoch ohne dass innerhalb der bund.id eine Authentifizierung über eID/ELSTER zwingend erforderlich ist. In dieser Variante sind nur eine gültige E-Mail-Adresse und ein selbst gewähltes Passwort erforderlich, es kann aber auch Ausweis oder ELSTER Zertifikat genutzt werden.

Zum Abschluss des Registrierungsprozesses werden die Antragstellenden aufgefordert, weitere Daten (z.B. E-Mail-Adresse) zu ergänzen, die ggf. nicht aus dem bund.id-Benutzerkonto übernommen werden können, die aber für den weiteren Verlauf der Antragstellung, insbesondere zur Kontaktaufnahme, benötigt werden. Zur Verifizierung der E-Mail-Adresse wird ihnen eine E-Mail mit einem Aktivierungslink zugesendet. Durch den Klick auf den Link ist der Registrierungsprozess abgeschlossen. Es steht nun ein portalspezifisches Benutzerkonto (im Folgenden: Antragskonto) zur Verfügung.

Anmeldung

Nach erfolgreich abgeschlossener Registrierung können sich die Antragsstellenden im „EPPSG-Portal “ erneut anmelden. Jede neue Anmeldung erfordert eine Authentifizierung mit dem bund.id-Benutzerkonto, je nach gewählter Variante der Authentifizierung ggf. einschließlich PIN.

Antrag EPPSG-Einmalzahlung auf Energiepreispauschale

Antragsberechtigte:

Antragsberechtigt sind Studierende, (Berufs-) Fachschülerinnen und Fachschülern gemäß §1 EPPSG.

Umfang der EPPSG-Einmalzahlung Energiepreispauschale

Wegen der stark gestiegenen Lebenshaltungskosten und Energiepreise sollen Studierende sowie Fachschüler und Fachschülerinnen eine einmalige Energiepreispauschale in Höhe von 200 Euro erhalten. Die Energiepreispauschale kann erhalten, wer am 1. Dezember 2022 an einer in Deutschland gelegenen Ausbildungsstätte immatrikuliert ist. Somit umfasst das Gesetz auch ausländische Studierende, die ihren Wohnsitz oder gewöhnlichen Aufenthalt in Deutschland haben. Ausgenommen von der Einmalzahlung sind allerdings Gaststudierende.

Antragsvorbereitung

Die Infowebseite (www.einmalzahlung200.de) informiert über die Möglichkeiten zur Antragstellung zur Einmalzahlung, u.a. mit Informationen zu Anspruchsvoraussetzungen und Antworten auf häufige Fragen. Beim Besuch der Websites werden während einer laufenden Verbindung über den Internetbrowser des Nutzers und mit Hilfe von technisch notwendigen sog. Session-Cookies Daten erhoben. Diese Daten beziehen sich lediglich auf die IP-Adresse, Datum und Uhrzeit des Aufrufs der Website, verwendete Webbrowser und verwendetes Betriebssystem und den Namen des verwendeten Internet-Providers. Außerdem werden bei jedem Zugriff auf die Website bzw. bei jedem Abruf einer Datei Daten über diesen Vorgang vorübergehend in einer Protokolldatei erfasst und gespeichert. Die sind im Einzelnen folgende Daten: das Datum und die Uhrzeit des Aufrufs der Website, verwendete Webbrowser und verwendetes Betriebssystem, die vollständige IP-Adresse des anfordernden Rechners, der Name und die URL der abgerufenen Datei, die Webseite, von der aus der Zugriff erfolgt, der Name des verwendeten Internet-Providers (sog. Kommunikationsmetadaten). Alle die beim Besuch der Website erhobenen Daten werden nach maximal sieben Tagen gelöscht.

Dateneingabe im Antragsassistenten

Die Antragsdaten können digital in eine Eingabemaske im Antragsassistenten eingegeben werden. Eine Registrierung bzw. Identifizierung ist wie oben dargestellt erforderlich.

Im Einzelnen handelt es sich dabei um die folgenden Daten bzw. Datenkategorien:

- Stammdaten (Vorname, Familienname)
- Zugangscode und optional PIN
- Bankverbindung
- E-Mail-Adresse

- Geburtsdatum/-ort
- optional Anschrift und Telefonnummer

Nach Abschluss der Eingabe der Daten im Antragsassistenten werden die Antragsdaten über eine Schnittstelle an die Fachverfahren der zuständigen Stellen der Länder übermittelt. Ab dem Zeitpunkt der Übermittlung sind die zuständigen Stellen der Länder datenschutzrechtlich verantwortlich. Diese nutzen die personenbezogenen Daten zur Bearbeitung des Antrags; erst nach Eingang der Antragsdaten beginnt das Verwaltungsverfahren.

Validierung der Daten und Absenden des Antrags

Da die Antragstellung nicht an die Schriftform gebunden ist, muss der Antrag nicht unterschrieben werden. Die Antragstellung erfolgt durch einfaches „Absenden“ im Antragsassistenten.

Der Antrag kann jedoch nur versendet werden, wenn die Daten der Bankverbindung syntaktisch oder semantisch richtig sind und alle Pflichtangaben im Antragssystem ausgefüllt wurden: Die eingegebenen Daten, z.B. die IBAN, werden nach jedem Drücken der Schaltfläche „Jetzt Antrag einreichen“ über eine Schnittstelle gegen den Dienst iban.com validiert. Hierfür wird ausschließlich die IBAN an den Dienstleister „iban.com“ übermittelt. Dieser prüft die IBAN und meldet zurück, ob die IBAN validiert werden konnte. Ist dies nicht der Fall, erfolgt über eine Schnittstelle/REST API eine Fehlermeldung an das Antragssystem, wo wiederum der Antragsteller über den Fehler informiert wird. Es erfolgt somit eine Übergabe der IBAN an iban.com und als Ergebnis kommt "Erfolg" oder "Fehler" zurück.

Es handelt sich hierbei um eine Prüfung der Vollständigkeit, die als reine Service-Leistung erfolgt, die jedoch noch keine inhaltliche Prüfung darstellt.

Sind die Antragsdaten nicht vollständig oder die IBAN syntaktisch oder semantisch falsch, so erfolgt eine Fehlermeldung mit der Bezeichnung des konkreten Fehlers. Ergeben sich hingegen bei der Validierung keine Fehler, so wird der Antrag abgesendet. Die Antragstellenden erhalten eine Bestätigung im Browser, dass der Antrag erfolgreich abgesendet wurde.

Die Antragsdaten werden nach Absenden des Antrags im Antragskonto gespeichert. Sie sollen dort bis zum Ende des Antragszeitraums (mind. Ende Septem-

ber 2023) gespeichert bleiben, damit sich NutzerInnen zu einem späteren Zeitpunkt nochmals einloggen können, um ihren Antrag einzusehen und dessen Status zu prüfen. Nach Abschluss des Antragszeitraums sollen die portalspezifischen Benutzerkonten automatisch gelöscht werden. Hierüber werden die NutzerInnen per E-Mail zuvor informiert.

Technische Umsetzung des Antragsassistenten

Der Antragsassistent ist auf Basis der bereits erprobten Software umgesetzt. Die Kommunikation vom Nutzer zum Antragsassistenten erfolgt verschlüsselt nach der vom BSI empfohlenen Cypher-Suite der Klasse TLS 1.1-1.3. mit HTTPS.

Hosting und Betrieb des Antragsassistenten erfolgen im Auftrag des MID Sachsen-Anhalt von der Firma]init[AG im BSI-zertifizierten Rechenzentrum. Die Betriebsumgebung (technische Infrastruktur) wurde als so genannte logisch getrennte Drei-Schichten-Architektur umgesetzt und besteht aus Web-Servern, Applikations-Servern und Datenbank-Servern. Um die Kommunikationsverbindungen auf das minimale notwendige Maß zu reduzieren, sind die IT-Systeme des Antragsassistenten in dedizierten, nach Funktionalität der Systeme geordneten Netzwerkzonen aufgestellt. Die Netzzonen sind durch Firewalls voneinander getrennt und es können nur explizit erlaubte (Whitelisting) Kommunikationsverbindungen zwischen den Systemen aufgebaut werden. Horizontale Kommunikationsverbindungen zwischen zwei Systemen der gleichen Netz-Zone sind möglich. Die Server selbst haben ebenfalls eine eigenständige Firewall und ergänzenden Schutz der Server in einem Netz.

Übermittlung an Dritte – Funktion Schnittstelle zum Fachverfahren

Nach Abschluss der Eingabe der Daten im Antragsassistenten werden die Antragsdaten über eine technische Schnittstelle elektronisch an das jeweilige der 16 nach Bundesland getrennten IT-Systeme (Fachverfahren) übermittelt. Die Zuordnung des jeweiligen Antrags zur je nach Bundesland zuständigen Stelle erfolgt anhand des Zugangscodes. Im Antragssystem wird diese Zuordnung automatisch geprüft und der Antrag dem entsprechenden Fachverfahren zugeleitet.

Das Antragssystem und die Fachverfahren werden auf zwei getrennten Arten von Applikationsserver-Instanzen betrieben. Antragssystem und Fachverfahren speichern ihre jeweiligen Daten in separaten Datenbankschemata. Ein Zugriff aus einem

Fachverfahren auf die Daten aus dem Antragssystem und umgekehrt ist über eine Schnittstelle (REST API) möglich.

Auf den Fachverfahren der einzelnen Bundesländer läuft ein Prozess, der dann regelmäßig prüft, ob neue Anträge für das Bundesland vorliegen.

Antragsbearbeitung in den zuständigen Stellen der Länder

Die Sachbearbeitung, durch die je nach Bundesland zuständigen Stellen der Länder, erfolgt im jeweiligen IT-System des Fachverfahrens, welches die Bearbeitung führt und unterstützt, aber technisch getrennt erfolgt und somit nicht Teil des hier beschriebenen Verfahrens ist.

2.5 Empfänger der Daten (bitte benennen)

☐ anderer (gemeinsam) Verantwortlicher:

☒ andere Behörde: zuständigen Stellen der Bundesländer

☒ Auftragsverarbeiter: mit der]init[AG für digitale Kommunikation, Köpenicker Straße 9, 10997 Berlin (Entwicklung, Installation, Hosting, Betrieb) ist ein entsprechender Vertrag nach Art. 28 DSGVO abgeschlossen; als Subunternehmer und weitere Auftragsverarbeiter der]init[AG:

1. Cloudflare Inc. (CDN/Waiting Room)
2. iban.com GW Solutions LTD (IBAN-Validierung)
3. BP Mediawork GmbH (Servicedesk)
4. Blue Rose Technologies GmbH (Entwicklung, 2nd Level Support)
5. Greenfield Technology AG (QA, 2nd Level Support)
6. Pega (Entwicklung, 2nd und 3rd Level Support)

2.6 Wie viele Personen haben Zugriff auf die Daten? (bitte ankreuzen und ergänzen)

☐ …… Personen

☐ ungefähr …… Personen

☐ mindestens ……. aber sicher nicht mehr als ……. Personen

☒ Anzahl steht bisher noch nicht fest

2.7 Kann auf eine bereits vorliegende DSFA zurückgegriffen werden? (bitte ankreuzen und ergänzen)

☐ DSFA aus dem Jahre …… liegt vor

Beschreibung:

☐ DSFA zu einem ähnlichen Verarbeitungsverfahren liegt vor

Beschreibung:

☒ Nein

2.8 Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung in Bezug auf den Zweck

Die geplanten und vorstehend unter 2.4 beschrieben Verarbeitungsvorgänge werden ausgehend von den mit ihnen verfolgten Zwecken daraufhin bewertet, ob der durch sie bewirkte Eingriff in die Rechte und Freiheiten der Betroffenen im Verhältnis zu den angestrebten Zwecken steht, ob sie zum Erreichen der Zwecke tatsächlich notwendig sind oder ob alternative Vorgehensweisen zur Verfügung stehen, die in die Rechte und Freiheiten der Betroffenen weniger stark eingreifen.

Der Antragsassistent in Verantwortung des MID Sachsen-Anhalt ist notwendig, um die Anträge zentral in einer Stelle zu kanalisieren. Dies ist wiederum geboten, um einerseits eine überlange Verfahrensdauer zu verhindern. In der gegenwärtigen Lage gibt es potenziell 2,95 Millionen Studierende und etwa 450.000 Fachschülerinnen und Fachschüler, die antragsberechtigt sind. Anderseits soll eine Unübersichtlichkeit über die zuständigen Stellen in den Ländern verhindert werden. Die schnelle und zügige Bearbeitung der Anträge ist wegen der stark gestiegenen Lebenshaltungskosten und Energiepreise von nationaler Tragweite im Interesse der Schüler*innen und Studierenden dringend notwendig. Schließlich würde eine verzögerte Bearbeitung über Monate hinweg viele Schüler*innen und Studierende in Zahlungsnot bringen.

Die mit der Bereitstellung des Antragsassistenten (einschließlich des Webseite-Betriebs) erfolgenden konkreten Datenverarbeitungen sind notwendig und verhältnismäßig. Sie werden auf das absolut notwendige Maß beschränkt und erweisen sich mit

Blick auf den überragend wichtigen Zweck des Schutzes der Anspruchsberechtigten als nicht übermäßig belastend für die Rechte und Freiheiten der betroffenen Personen.

Mildere, die Rechte und Freiheiten der betroffenen Personen weniger intensiv einschränkende Datenverarbeitungen sind nicht ersichtlich. Eine Antragstellung für die betroffenen Antragsberechtigten ist ohne die Angaben der Antragsdaten denklogisch nicht möglich. Sämtliche verarbeiteten personenbezogenen Antragsdaten werden zur Bearbeitung der Anträge bei den zuständigen Behörden auf Landesebene benötigt, um den Antrag zu bescheiden. Dafür ist es auch erforderlich, dass Bankdaten der Antragsteller als Teil der Anträge verarbeitet werden.

Ihre Speicherung und Übermittlung sind angesichts der stark gestiegenen Lebenshaltungskosten und Energiepreise und der damit einhergehenden besonderen Eilbedürftigkeit der Sachbearbeitung erforderlich.

Die im Zuge der Nutzung der Website verarbeiteten personenbezogenen Daten sind ebenfalls – teilweise schon technisch – zwingend notwendig, um ein funktionsfähiges und benutzerfreundliches Online-Antragsverfahren zur Verfügung zu stellen. Die damit einhergehende Eingriffsintensität in die Rechte und Freiheiten der betroffenen Personen ist gering.

Die übrigen Grundätze der DSGVO werden ebenfalls eingehalten. Die Nutzer werden im Rahmen der Datenschutzerklärung über die Verarbeitung der Daten entsprechend der Vorgaben gemäß Art. 13 Abs. 1, 2 DS-GVO informiert. Sie kann auf der Website aufgerufen werden, bevor bzw. ohne, dass der Nutzer sich bereits für oder gegen die Nutzung des Antragsassistenten entschieden haben muss. Die Daten werden nur zu den unter 2. 2 verarbeiteten Zwecken gemäß Art. 5 Abs. 1 lit. b DSGVO genutzt. Weiterhin werden die Nutzer insb. über das Recht auf Berichtigung und Löschung informiert gem. der Art. 16 ff. DS-GVO.

2.9 Mögliche Folgen für betroffene Personen bei Datenschutzverletzungen (nach ErwG Nr. 75 DSGVO)[9] (bitte ankreuzen)

- ☐ Gefahr für Leib oder Leben
- ☐ Rufschädigung/gesellschaftliche Nachteile
- ☐ Diskriminierung
- ☒ wirtschaftliche Nachteile/finanzielle Verluste
- ☐ Ausschluss oder Einschränkung von Grundrechten, insb. des Grundrechts auf informationelle Selbstbestimmung
- ☐ Erschwerung der Rechtsausübung oder Kontrollverlust
- ☐ anderer immaterieller Schaden (bitte benennen)

[9] Die Verletzungsfolgen sind vor Berücksichtigung von risikominimierenden technischen und organisatorischen Maßnahmen (TOM) zu betrachten.

3 Risikoermittlung und -bewertung

3.1 Vorbemerkung

Durch die Datenschutz-Folgenabschätzung sind vor Beginn einer Verarbeitung mögliche Risiken zu identifizieren, zu bewerten und Maßnahmen aufzuzeigen, mit denen diese Risiken auf ein akzeptiertes Maß gesenkt werden. Die Pflege der Risikoanalyse, -bewertung und -behandlung erfolgt regelmäßig im Rahmen der Aktualisierung des Datenschutzkonzepts und überprüft die Umsetzung der empfohlenen Maßnahmen.

3.2 Vorgehen

Die Höhe des Risikos hängt sowohl von der Eintrittswahrscheinlichkeit (Eintrittseinschätzung) der Gefährdung als auch von der Höhe des Schadens ab. Die Beurteilung des resultierenden Schadens erfolgt aus der Perspektive des Betroffenen. Beim Eintritt einer Gefährdung müssen die Art des Schadens und mögliche Folgeschäden eingeschätzt werden. Eine mögliche Berücksichtigung schließt ein, ob und wie ein Schaden zu beheben ist.

(1) **Datenminimierung**

Es werden nur die Daten verarbeitet, die absolut notwendig sind, um den jeweiligen Zweck –Beantragung und Bewilligung - EPPSG-Einmalzahlung zu erzielen. Ohne die erforderlichen Angaben können keine Anträge gestellt und keine Auszahlungen erfolgen.

(2) **Verfügbarkeit**

Die personenbezogenen Daten sind für eine fachgerechte Verarbeitung verfügbar. Es ist gewährleistet, dass die zuständigen Stellen der Länder durch ausreichend Speicherplatz auf die Antragsdaten zugreifen können und diese nicht unkontrolliert verschwinden oder vernichtet werden. Die von stark gestiegenen Lebenshaltungskosten und Energiepreise betroffenen Schüler*innen und Studierende benötigen möglichst schnell eine Entlastung. Stünden die Systeme zur Antragsstellung oder Antragsbearbeitung für einen längeren Zeitraum nicht zur Verfügung, könnten Anträge nicht gestellt werden und der erhoffte Effekt der EPPSG-Einmalzahlung würde nicht eintreten.

(3) **Integrität**

Daten werden vor unberechtigten Änderungen geschützt. Sofern Modifikationen durchgeführt werden, sind diese nachvollziehbar dokumentiert, um Manipulationen zu verhindern. Es ist wichtig, dass die Zahlungen nur an die beantragenden

und berechtigten Schüler*innen und Studierende erfolgen. Es ist zudem von einem hohen öffentlichen Interesse an dem Projekt auszugehen.

(4) **Vertraulichkeit**

Durch Berechtigungskonzepte wird gewährleistet, dass nur diejenigen Mitarbeiter und Sachbearbeiter der zuständigen Stellen der Länder Zugriff auf gespeicherte Daten haben, die direkt für die Antragsstellung und Bearbeitung erforderlich sind. Mit der Antragstellung übermitteln die Antragsberechtigten im eigenen Namen personenbezogene Daten. Damit diese personenbezogenen Daten von Dritten nicht zum Nachteil der Antragsberechtigten verwendet werden, müssen diese vertraulich behandelt werden. Entsprechende Berechtigungskonzepte, Verpflichtungen auf Vertraulichkeiten und Datenschutzschulungen gewährleisten die entsprechende Vertraulichkeit.

(5) **Nichtverkettung**

Daten, die für einen bestimmten Zweck erhoben worden sind, werden nicht für andere Zwecke verarbeitet. Das Antragssystem und die Fachverfahren werden auf zwei getrennten Arten von Applikationsserver-Instanzen betrieben. Antragssystem und Fachverfahren speichern ihre jeweiligen Daten in separaten Datenbankschemata. Ein Zugriff aus einem Fachverfahren auf die Daten aus dem Antragssystem und umgekehrt ist nicht möglich.

(6) **Transparenz**

Es ist dokumentiert, zu welchen Zwecken eine Datenverarbeitung erfolgt. Zum einen steht hier den Betroffenen neben Informationen und der Datenschutzerklärung einschließlich der Betroffenenrechte auf der Website zur Verfügung, zum anderen besteht ein Datenschutzkonzept.

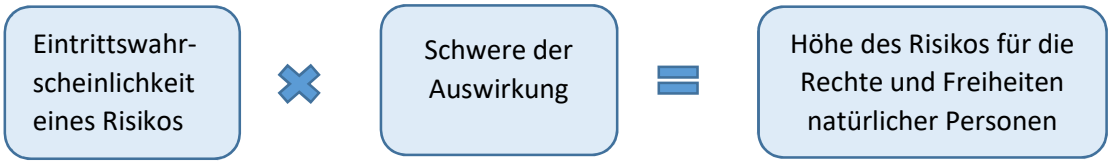
(7) **Intervenierbarkeit**

Betroffene können ihre Rechte an ihren Daten wahrnehmen. Die Betroffenenrechte sind in der Datenschutzerklärung auf der Website dargelegt. Datenverarbeitungsprozesse sind so gestaltet, dass Betroffenenrechte wahrgenommen werden können: Die Betroffenen erhalten über ihre gespeicherten Daten Auskunft, sie können Korrekturen vornehmen, sie sperren oder löschen lassen.

3.3 Schadensbewertung

Die Schutzbedarfsfeststellung nach Bewertung der Höhe des Schadens und Risikoermittlung unter Zugrundelegung der Eintrittswahrscheinlichkeit wird nachfolgend in diesem Dokument DSFA abgebildet.

Zugrunde gelegt wird für die Berechnung der Bewertung von Datenschutzrisiken nachfolgende Formel:



Die Schutzbedarfskategorien bzw. die Risiken sind wie folgt definiert[10]:

Gering, wenn die Schadensauswirkungen begrenzt und überschaubar sind
Mittel, wenn die Schadensauswirkungen beträchtlich sind und
Hoch, wenn die Schadensauswirkungen ein existentiell bedrohliches, katastrophales Ausmaß erreichen

Mögliche Risiken/ Schwachstellen	Risikoquelle	Möglicher Schaden	Eintrittswahrscheinlichkeit/ Schutzbedarf
Missbrauch von Betroffenendaten/Datenverarbeitung in großem Umfang (**es werden ca. 3,5 Mio. Anträge erwartet**) gemäß Art. 35 Abs. 1 DSGVO.	Software Online-Antragsassistent EPPSG-Einmalzahlung, Antragsteller, Auftragsverarbeiter	Eine missbräuchliche Verwendung der personenbezogenen Daten, kann wirtschaftliche Nachteile auf Seiten des Betroffenen als auch Beeinträchtigung der staatlichen Aufgabenerfüllung und längere Verfahrensdauer mit sich bringen.	**Hoch**, DSFA erforderlich, da Datenverarbeitung in großem Umfang per se ein potenziell hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
Missbrauch von **schutzbedürftigen** Betroffenendaten gemäß Art. 35 Abs. 1 DSGVO, da unter den Antragsberechtigten voraussichtlich auch Minderjährige sind.	Software Online-Antragsassistent EPPSG-Einmalzahlung, Antragsteller, Auftragsverarbeiter	Eine missbräuchliche Verwendung der personenbezogenen Daten, kann persönliche Nachteile auf Seiten des Betroffenen mit sich bringen.	**Hoch**, DSFA erforderlich, da die Datenverarbeitung von schutzbedürftigen Personen per se ein potenziell hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt.
Unsachgemäße/ fehlerhafte Eingabe der Registrierungs- bzw. Anmeldedatendaten	Antragsteller	Verzögerung der Auszahlung, wirtschaftlicher Schaden für den Antragsteller	**Gering.** Bei einer Falscheingabe der Registrierung- bzw. An-

[10] Karg in Simitis/Hornung/Spiecker Art. 35 Rn 25, Kommentar zum Datenschutzrecht 2019

			meldedaten erfolgt sofortige Mitteilung. D. h. der Antragsteller e kann sich erneut anmelden/ registrieren. Es handelt sich daher nur um eine kurzfristige Verzögerung.
Unsachgemäße/ fehlerhafte Eingabe der Antragsdaten	Antragsteller	Verzögerung der Auszahlung, wirtschaftlicher Schaden für den Antragsteller	**Gering**. Schüler bzw. Studierende sind es gewohnt, Daten in Formulare einzutragen, z.B. Anmeldung, Immatrikulation. Gleichwohl kann ein „menschliches Versagen“ nicht ganz ausgeschlossen werden. Eine solche Fehlerquelle lässt sich niemals ausschließen, weder analog noch digital.
Manipulation von Informationen eines/vieler Antragsteller	Antragsteller	Unberechtigte Auszahlung an den Antragsteller, wirtschaftlicher Schaden des Staates	**Gering**. Ein Antragsteller könnte die gegenüber den Behörden zu machenden Daten manipulieren. Die Bewilligung der EPPSG-Einmalzahlung wird von entsprechenden Sachbearbeitern in den zuständigen Stellen der Länder geprüft. Es wurden sogenannte Prüf-Kriterien festgelegt. Diese Kriterien ermitteln automatisch, ob ein Antrag möglicherweise falsche Angaben enthalten könnte. Gleichwohl kann es im Einzelfall zu unerkannten Manipulationen kommen.
Unbefugtes Eindringen in IT-Systeme	Dritte	Unbefugter Zugriff auf Daten durch Dritte, z. B. Hacker. Gefahr gesellschaftlicher und wirtschaftlicher Nachteile auf Seiten des Betroffenen, Beeinträchtigung	**Gering/ Mittel.** Das BSI zertifizierte Rechenzentrum der]init[AG hat entsprechenden Schutz vor Angriffen Dritter durch Firewalls etc. Die Zertifizierung des]Init[Rechenzentrums stellt

		der staatlichen Aufgabenerfüllung und längere Verfahrensdauern.	nach anerkannten Kriterien sicher, dass die Informationen des Verfahrens durch Techniken und Methoden nach dem Stand der Technik abgesichert werden. Ein Eindringen Unbefugter ist damit maximal erschwert, eine hundertprozentige Sicherheit kann aufgrund der Materie aber nicht gewährleistet werden.
Software-Schwachstellen oder –Fehler	IT-Systeme (]init[AG)	1. Unberechtigte Auszahlung an den Antragsteller, wirtschaftlicher Schaden des Staates 2. Verzögerung der Auszahlung, wirtschaftlicher Schaden für den Antragsteller	**Zu 1. Gering.** Softwareschwachstellen oder Fehler, die z. B. eine unvollständige Antragstellung zulassen, würden auffallen. Eine unberechtigte Auszahlung ist kaum wahrscheinlich. Zudem würden die zuständigen Stellen der Länder entsprechende Schwachstellen an die]init[AG melden. Software- Schwachstellen oder Fehler könnten schnell behoben werden. **Zu 2. Gering/ Mittel.** Softwareschwachstellen oder Fehler, die z. B. eine unvollständige Antragstellung zulassen, würden auffallen. Es ist jedoch nicht abzusehen, wie lange eine Bewilligungsbearbeitung tatsächlich dauert. Ggf. verzögert sich die Nachforderung von Angaben und die Prüfung der Bewilligung. Die Verzögerung dürfte jedoch nicht erheblich sein.
Verstoß gegen Gesetze oder Regelungen	1. Antragsteller, 2.]init[AG,	Unberechtigte Auszahlung an den Antragsteller, wirtschaftlicher Schaden des Staates	**Zu 1: Gering.** Siehe oben bei „Manipulation von Informationen eines/vieler Antragsteller“

		Datenverkauf an Dritte	**Zu 2: Gering.** Ein Verstoß gegen Gesetze und Regelungen wäre stark Ruf schädigend. Zudem ist nicht ersichtlich, wie ein]init[-MA die Software so manipulieren könnte, dass er unberechtigte Auszahlungen erhält oder mit einem Antragsberechtigten unberechtigte Auszahlungen „teilt". Alle]init[MA sind auf Vertraulichkeit verpflichtet und wissen um die Strafbarkeit bei Verstoß gegen das Datenschutzrecht.
Unberechtigte Nutzung oder Administration von Geräten und Systemen	MA der]init[AG	Ggf. können dadurch Anträge nicht gestellt werden. Verzögerung der Auszahlung, wirtschaftlicher Schaden für den Antragsteller	**Gering.** Nur ein kleiner Kreis von]init[MA hat Zugriff auf Geräte und Systeme. Es gibt ein Berechtigungskonzept und entsprechende Verpflichtung auf Vertraulichkeit und IT-Sicherheit.]init[MA sind darauf geschult, Datenschutz und IT-Sicherheit einzuhalten.
Fehlerhafte Nutzung oder Administration von Geräten und Systemen	MA der]init[AG	Ggf. können dadurch Anträge nicht gestellt werden. Verzögerung der Auszahlung, wirtschaftlicher Schaden für den Antragsteller	**Gering.** Nur ein kleiner Kreis von]init[MA hat Zugriff auf Geräte und Systeme. Fehlerhafte Nutzung würde ohne große zeitliche Verzögerung bemerkt. Es gibt ein Berechtigungskonzept und entsprechende Verpflichtung auf Vertraulichkeit und IT-Sicherheit.]init[MA sind darauf geschult, Datenschutz und IT-Sicherheit einzuhalten.
Missbrauch von Berechtigungen	Service-Desk-/Admin-MA der]init[AG	Datenverkauf an Dritte,	**Gering.** Vgl. oben „Verstoß gegen Gesetze oder Regelungen"

		Unberechtigte Auszahlung an den Antragsteller, wirtschaftlicher Schaden des Staates	
Identitätsdiebstahl	Dritte	Unberechtigte Auszahlung an den Antragsteller, wirtschaftlicher Schaden des Staates	**Gering.** Anträge können nur über Zugangscode bzw. Zugangscode mit PIN eingereicht werden. Dazu wurde die PIN-Vergabe an gewisse Hürden geknüpft.
Missbrauch personenbezogener Daten, Schadprogramme	Dritte	Unberechtigter Zugriff auf Bankkonten, wirtschaftlicher Schaden Verkauf an Dritte für Werbespams etc.	**Gering/ Mittel.** Das BSI zertifizierte Rechenzentrum der]init[AG hat entsprechenden Schutz vor Angriffen Dritter durch Firewalls etc. Die BSI Zertifizierung des]init[Rechenzentrums stellt nach anerkannten Kriterien sicher, dass die Informationen des Verfahrens durch Techniken und Methoden nach dem Stand der Technik abgesichert werden. Ein Eindringen Unbefugter ist damit maximal erschwert. Dennoch ist kein IT-System vor Angriffen Dritter (Hacker) sicher.

3.4 Maßnahmen zur Risikominimierung

Um die Risiken / Schwachstellen zu minimieren sind nachfolgend folgende Maßnahmen umgesetzt:

Mögliche Risiken/ Schwachstellen	Eintritts-wahrschein-lichkeit/ Schutzbedarf	Maßnahmen (TOM) zur Risikomin-imierung	Ermitteltes Risiko nach Maßnahmenergreifung
Die Datenverarbeitung in großem Umfang (**es werden ca. 3,5 Mio. Anträge erwartet**) und die Datenverarbeitung von **schutzbedürftigen Betroffenen** stellen per se ein potenziell hohes Risiko für die Rechte und Freiheiten der betroffenen Personen dar. Mögliche Gefahrenquellen sind hierbei: • **unerlaubter Zugriff von außen,** • **unerlaubter Zugriff eines Innentäters sowie** • **Datenverlust**	**Hoch**	Die Datenverarbeitungssysteme befinden sich in einer Betriebsinfrastruktur, die nach den Kriterien des BSI IT-Grundschutzkatalogs eingerichtet und auditiert ist. Der administrative Zugriff auf die Systeme ist nur durch befugtes Personal des Auftragnehmers möglich, die Berechtigungen werden auf Basis von internen Prozessen vergeben und dokumentiert. Für die Passwörter besteht eine Richtlinie für den Account (Passwortkomplexität, Passworterneuerung, automatische Sperrmechanismen). Für die Administratoren ist eine Verschlüsselung der Übertragungswege vorgesehen. Zugänge zu den redaktionellen Schnittstellen sind über erweiterte Zugangskontrollsysteme gesichert. Die Systeme befinden sich in einem nach SAGA in Sicherheitszonen strukturierten Netzwerk. Ein mehrstufiges Sicherheitsgateway regelt den Datenfluss zwischen den Systemen nach dem Minimalprinzip. Durch die Zugangsregelung ist bereits gewährleistet, dass nur autorisiertes und sicherheitsüberprüftes Personal Zugriff auf die Datenverarbeitungssysteme hat. Dabei handelt es sich ausschließlich um das Wartungspersonal im eigenen Haus. Die Zugriffsregelung reduziert den Zugriff auf das für den Betrieb notwendigste Maß. Die Arbeitsplätze der autorisierten Personen unterliegen organisatorischen Richtlinien für Account (Passwortkomplexität und Passworterneuerung) sowie Autologoff bei Inaktivität, so dass das Risiko durch Missbrauch stark verringert ist.	**Mittel/ Gering** Durch die ergriffenen Maßnahmen kann ein unerlaubter Zugriff von außen, ein unerlaubter Zugriff eines Innentäters sowie Datenverlust deutlich erschwert und reduziert werden. Das Risiko kann nicht gänzlich auf „Null“ reduziert werden, da die Vergangenheit gezeigt hat, dass auch sicher geglaubte Server vor Cyber-/ Hackerangriffen nicht geschützt werden können. Das Risiko ist jedoch durch die ergriffenen TOM auf ein Mindestmaß eingegrenzt.

		Die Zugriffskontrolle ist mittels eines Berechtigungskonzeptes festgelegt und erfolgt nach dem Minimalprinzip, so dass nur die benötigten Mitarbeiter Zugriff auf die Systeme erhalten. Zugriffe auf die Systeme werden protokoliert. Die ordnungsgemäße Vernichtung von Datenträgern und ggf. zugehörigen Akten ist durch einen zertifizierten Dienstleister sichergestellt, der die Vernichtung protokolliert. Näheres ist im Betriebskonzept und in den IT-Sicherheitsrichtlinien festgehalten. Alle]init[Mitarbeiter sind auf Vertraulichkeit verpflichtet. Es finden regelmäßig Datenschutz und IT-Sicherheitsschulungen statt. Die Teilnahme solcher Überprüfungen ist verpflichtend. Daten und Systeme sind in mehrfacher Hinsicht vor dem Risiko des Verlustes geschützt: Unterbringung in einem Rechenzentrum, das gegen Risiken durch Brand, Klima, Strom, Sabotage entsprechend ausgerüstet ist. Tägliche Datensicherung gewährleistet den Schutz der Daten im Generellen. Die Daten werden aus dem Rechenzentrum täglich in einem anderen Brandabschnitt gesichert. Die Datensicherung unterliegt einem dokumentierten Datensicherungskonzept. Es existiert ein Notfallplan für die Wiederherstellung von Daten. Diese wird mittels regelmäßig durchgeführter Wiederherstellungstests auf Basis der täglichen Datensicherung sichergestellt.	

3.5 Bestätigung der Wirksamkeit der Maßnahmen

Aufgrund der vorgesehenen technisch-organisatorischen Maßnahmen können die Schwere der Schäden und Risiken für Rechte und Freiheiten der betroffenen Personen begrenzt und die jeweilige Eintrittswahrscheinlichkeit reduziert werden. Die erfolgten Maßnahmen sind durchgehend angemessen und verhältnismäßig und reduzieren die bestehenden Risiken auf ein akzeptables Maß.

4 Abschließende Bewertung

Zusammenfassende Beurteilung für die Rechte und Freiheiten betroffener Personen (bitte erläutern):

Es ergibt sich vor Ergreifen der geplanten Abhilfemaßnahmen ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen. Aufgrund der vorgesehenen technisch-organisatorischen Maßnahmen können die Schwere der Schäden an den Rechten und Freiheiten der betroffenen Personen und die jeweilige Eintrittswahrscheinlichkeit reduziert werden. Die erfolgten Maßnahmen leisten mithin einen Beitrag zur Reduzierung der bestehenden Risiken.

Verbleibt ein hohes Risiko unter
Berücksichtigung der risikominimierenden Maßnahmen (TOM)? (bitte ankreuzen)

☐ Ja ➔ die Aufsichtsbehörde (LfD) ist zu informieren

☒ Nein ➔ Verfahren kann entsprechend durchgeführt werden