Datenschutzfolgenabschätzung nach Art. 35 DS-GVO

Bezeichnung der Verarbeitungstätigkeit:

Bezahldienst SocialCard

Zu Blatt-Nr.:

Von der Verzeichnisführenden Stelle auszufüllen!

1.	**Information zur Datenschutzfolgenabschätzung:**	
1.1	Name des Bearbeiters:	Vorname, Nachname einfügen
1.2	Name des Datenschutzbeauftragten:	Vorname, Nachname einfügen
1.3	Bearbeitungsdatum:	

2.	**Grundlegende Informationen:**	
2.1	Welche Verarbeitung ist geplant?	Die Daten von Asylsuchenden werden im Fachverfahren Fachverfahren einfügen aufgenommen und der Leistungsanspruch nach dem AsylbLG ermittelt. Die Leistungen nach dem AsylbLG werden ab dem auf die sogenannte SocialCard (=Bezahldienst: Produkt der Bietergemeinschaft aus Publk GmbH und Secupay AG) als normale Überweisung ausgezahlt. Damit eine Überweisung aus Fachverfahren einfügen über das Buchhaltungssystem der entsprechend einfügen vorgenommen werden kann, wird Asylsuchenden eine SocialCard mit einer IBAN zugewiesen. Die für die Zahlung benötigten Stammdaten der Asylsuchenden werden dazu manuell in das Portal des Bezahl-dienstes übertragen, so dass eine personenbezogene IBAN erzeugt wird, die für künftige Zahlungen von Leistungsansprüchen nach dem AsylbLG zur Verfügung steht. Die IBAN muss dazu in Fachverfahren einfügen manuell übernommen werden. In der Folge einer normalen Anordnung wird die Auszahlung über die auszahlende Stelle einfügen ausgelöst.
2.2	Welche Zuständigkeiten bestehen für die Verarbeitung?	1. Behörde einfügen ist für die Erhebung und Übertragung der Daten für Leistungsempfänger nach dem AsylbLG verantwortlich. 2. Die Behörde einfügen ist für den Buchhaltungs- und Auszahlungsprozess der Leistungen nach dem AsylbLG auf die IBAN des Leistungsempfängers zuständig
2.3	Gibt es Normen oder Standards für die Verarbeitung?	Normen, die die Verarbeitung tragen: § 4 LSDG (BW) i.V.m. Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e DS-GVO

3.	**Daten, Prozesse und Unterstützung**	
3.1	Welche Daten werden verarbeitet?	Personenbezogene Daten Personendaten (Name, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Kontaktdaten (Adresse, E-Mail-Adresse, Telefonnummer)

		Legitimationsdaten (Ausweis- und Meldedaten); Aktenzeichen Fachverfahren einfügen; Verfügungsrahmen als Schieberegler, IBAN - (vgl. Art. 4 Nr. 1 DS-GVO) - Mitarbeiterdaten (Vorname, Nachname und dienstliche E-Mail-Adresse)
3.2	Wie verläuft der Lebenszyklus von Daten und Prozessen?	Die Daten werden 10 Jahre ab dem Tag der letzten Nutzung der SocialCard aufbewahrt (bei Secupay/Publk und Software zur Zahlungsabwicklung einfügen). Erst danach dürfen sie gem. Vorgabe der BaFin gelöscht werden (Vorgaben der Behörde einfügen vgl. Bestimmungen zur LHO bzw. GemHVO auswählen)
3.3	Mit Hilfe welcher Mittel erfolgt die Datenverarbeitung?	- Webportal des Bezahldienstes (Publk) - IP der Anwender müssen durch IT-Dienstleister einfügen und den Bezahldienst freigeschaltet werden.

4. Verhältnismäßigkeit und Notwendigkeit		
4.1	Sind die Verarbeitungszwecke eindeutig definiert und rechtmäßig?	Ja, die Nutzung der Daten dient ausschließlich der Auszahlung von Leistungen nach dem AsylbLG/und in bestimmten Fällen der Sperrung der Karte auf Verlangen
4.2	Aufgrund welcher Rechtsgrundlage erfolgt die Verarbeitung?	§ 4 LSDG (BW) i.V.m. Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e DS-GVO i.V.m. dem AsylbLG
4.3	Sind die erhobenen Daten erforderlich, relevant und auf das für die Datenverarbeitung Notwendige beschränkt?	Ja, es werden nur die für die Leistungsgewährung und Kartenausstellung erforderlichen Daten verarbeitet, entsprechend den erforderlichen Angaben nach dem AsylbLG und der BaFin, z.B. Vorname, Nachname, Geburtsdatum, Staatsangehörigkeit etc.
4.4	Sind die Daten korrekt und auf dem neuesten Stand?	Ja, die Daten werden unmittelbar nach der Registrierung in der Erstaufnahme in XX / Aufnahme in XX für die in der Folge zu tätigende Auszahlung der Leistung nach dem AsylbLG erhoben und im Webportal zur Generierung der IBAN hinterlegt.
4.5	Welche Speicherdauer haben die Daten?	10 Jahre nach Vorgabe der BaFin

5. Maßnahmen zu Schutz der Persönlichkeitsrechte der betroffenen Personen		
5.1	Wie werden die betroffenen Personen über die Verarbeitung informiert?	1. Auf der Seite des Bezahldienstes 2. Nach erfolgreicher Ausgabe der SocialCard erhält der Kartennutzer die Anwenderinformationen und den Nutzungsvertrag. Die Datenschutzerklärung der beteiligten Firmen sind hier zu finden: SocialCard - Datenschutz und https://secupay.com/datenschutz Die Behörde einfügen informiert die betroffenen Beschäftigten darüber, welche Daten an den Dienstleister weitergegeben werden.
5.2	Wenn anwendbar: wie wird die Einwilligung der betroffenen Personen eingeholt?	Nach erfolgreicher Ausgabe der SocialCard erhält der Kartennutzer die Anwenderinformationen und schließt einen Nutzungsvertrag mit den Firmen (Publik/Secupay) ab. Eine Einwilligung wird nicht eingeholt.

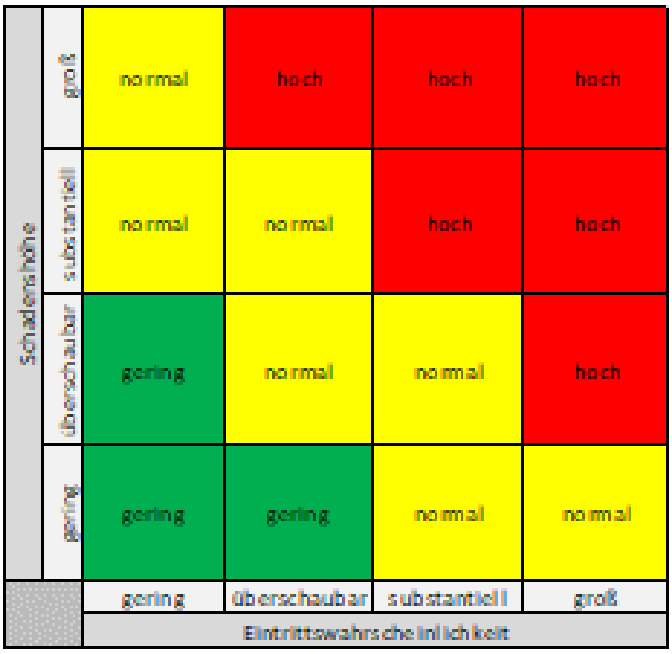
5.3	Wie können Betroffene ihre Rechte auf Auskunft und Datenübertragbarkeit ausüben?	Auf das Auskunftsrecht weisen Publik und Secupay auf ihren Internetseiten zum Datenschutz hin. Die Behörde einfügen informiert in ihren behördlichen Datenschutzhinweisen über den Ansprechpartner zur Entgegennahme von Auskunftsanträgen. Im Übrigen verweist sie für Auskunftsanträge gegenüber Secupay auf die Internetseite des Bezahldienstes (Art 13 Absatz 1 lit. e DS-GVO) Ein Recht auf Datenübertragbarkeit liegt mangels Einwilligung nicht vor.
5.4	Wie können betroffene Personen ihre Rechte auf Berichtigung und Löschung (Recht auf Vergessenwerden) ausüben?	/ siehe 5.3
5.5	Wie können betroffene Personen ihre Rechte auf Einschränkung oder Widerspruch der Verarbeitung ausüben?	/siehe 5.3.
5.6	Sind die Verpflichtungen der Auftragsverarbeiter klar definiert und vertraglich geregelt?	/ siehe 5.3.
5.7	Soweit Datenübermittlungen in Länder außerhalb der EU stattfinden, werden die Daten angemessen geschützt?	entfällt

6. Geplante oder bestehende Maßnahmen		
6.1	Dokumentation	☒ ja, Aktenführung durch Behörde einfügen, Fachverfahren einfügen, Dokumentation der Zahlläufe in der Software zur Zahlungsabwicklung einfügen ☐ nein
6.2	Protokollierung	☒ ja, der Bezahldienst speichert die personenbezogenen Daten ☐ nein
6.3	Mandantentrennung	☒ ja ☐ nein
6.4	Verschlüsseln	☒ ja, Nutzende (Mitarbeitende der Behörde einfügen) (Client/Webbrowser) verbinden sich über eine Hypertext Transfer Protocol Secure (HTTPS) gesicherte Verbindung über das Internet mit dem Webportal (Webserver). Serverseitig wird ausschließlich eine HTTPS Verbindung zugelassen. ☐ nein
6.5	Testen	☒ ja, die grundsätzlichen Funktionen wurden von der (kassenrechtlich!) verantwortlichen Stelle in der Behörde einfügen getestet ☐ nein
6.6	Betriebsvereinbarung	☐ ja ☒ nein
6.7	Datenschutz-Erklärung	☒ ja, ☐ nein
6.8	Policies	☒ ja ☐ nein Es gelten die üblichen einschlägigen Policies aus den Feldern des Datenschutzes und der Informationssicherheit
6.9	Datenschutzmanagement	☐ ja

		☒ nein
6.10	Löschen	☒ ja, die Löschung der elektronischen personenbezogenen Daten erfolgt nach einer 10jährigen Aufbewahrungsfrist. ☐ nein
6.11	Anonymisieren	☐ ja ☒ nein, nicht relevant
6.12	Backup	☒ ja, der Bezahldienst sichert seine Daten ☐ nein
6.13	Weitere:	Klicken Sie hier, um Text einzugeben.

7. Risiken und zu gewährleistende Schutzziele

Zur Bewertung und Eindämmung der Risiken für die Rechte und Freiheiten Betroffener durch Nutzung der Anwendung werden die beschriebenen Verarbeitungsvorgänge aus der zentralen Risikoperspektive der Betroffenen betrachtet. Es gilt zu prüfen, ob durch die Verarbeitung der pbD trotz der implementierten geeigneten Vorkehrungen und wirkungsvollen Abhilfemaßnahmen weiterhin ein hohes Risiko besteht. Ausgehend von den erkannten Risikoquellen werden, zugeordnet zu den verschiedenen Gewährleistungszielen, **nachfolgend unterschiedliche Angriffs- / Schadensszenarien** betrachtet. Unter Berücksichtigung der eingerichteten Sicherheitsmaßnahmen wird jeweils das entsprechende Risiko – entsprechend der folgenden **Risikomatrix-Grafik** - bewertet.



Bei der hier empfohlenen Risikobewertung werden die Eintrittswahrscheinlichkeit und die Schwere/der Schaden wie folgt abgestuft[1]:

Möglicher Grad der Eintrittswahrscheinlichkeit:

Grad	Bezeichnung des Grads	Eintrittswahrscheinlichkeit	
		Beschreibung	**Beispiel**
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware aus-gestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.

[1] Der Bayerische Landesbeauftragte für den Datenschutz, Risikoanalyse und Datenschutz-Folgenabschätzung, Stand 01.05.2022, III. 3 Risikoanalyse der SDM-Datensicherheitsziele, S. 23.

3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware aus-gestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Um-stände möglich und sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

Möglicher Grad der Schwere/des Schadens:

Grad	Bezeichnung des Grads	Schwere der Folgen / möglicher Schaden	
		Beschreibung	**Beispiel**
1	geringfügig	Betroffene erleiden eventuell Unannehm-lichkeiten, die sie aber mit einigen Proble-men überwinden können.	immateriell: leichte Verärgerung materiell: Zeitverlust physisch: vorübergehende Kopfschmerzen"
2	überschaubar	Betroffene erleiden eventuell signifkante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwin-den können.	immateriell: geringe, aber objektiv nachweisbare psychi-sche Beschwerden materiell: deutlich spürbarer Verlust an privatem Komfort physisch: minderschwere körperliche Schäden (z. B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifkante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	immateriell: schwere psychische Beschwerden materiell: finanzielle Schwierigkeiten physisch: schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifkante o-der sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	immateriell: dauerhafte, schwere psychische Beschwer-den materiell: erhebliche Schulden physisch: dauerhafte, schwere körperliche Beschwerden

7.1	**Risiko: Unrechtmäßiger Zugriff auf die Daten** **Schutzziel: Vertraulichkeit**	
7.1.1	Was könnten die wesentlichen Auswirkun-gen für die betroffenen Personen sein, wenn das Risiko eintritt?	Unberechtigte könnten Informationen über die Identitäten erlangen. Die Daten könnten im Falle ei-nes unrechtmäßigen Zugriffs Dritter für alle denk-baren nicht bestimmungsgemäßen Zwecke ver-wendet werden (Werbung, Verkäufe). Auch könn-ten die Daten etwa im Internet veröffentlicht werden und hierbei die Betroffenen als Asylsuchende bloß-gestellt werden. Die unbefugte Offenlegung des Umstands des Empfangs von Asylleistungen kann für die Betroffenen schambesetzt und stigmatisie-rend sein. Die mögliche Fremdbestimmung über die eigenen Daten verletzt zudem das informatio-nelle Selbstbestimmungsrecht und kann bei den Betroffenen insb. immaterielle Schäden hervorru-fen. Auch finanzielle bzw. wirtschaftliche Nachteile (etwa durch Identitätsdiebstahl, betrügerische Inter-neteinkäufe zu ihren Lasten durch unbefugte Dritte) könnten die mittelbare Folge sein. Die mögliche unbefugte Fremdbestimmung über die eigenen personenbezogenen Daten verletzt in erheblicher Weise zudem die datenschutzrechtliche Integrität der Betroffenen, deren grundrechtlich ge-schütztes informationelles Selbstbestimmungsrecht (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG) sowie das europarechtliche Grundrecht zum Schutz perso-nenbezogener Daten aus Art. 8 GRCh.
7.1.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	- Vertraulichkeitsbruch - Kompromittierung im Rechenzentrum des Bezahl-dienstes Die Daten könnten insbesondere auf den digitalen Übermittlungswegen

		- von Behörde einfügen ins Rechenzentrum des Bezahldienstes - von der Behörde einfügen mittels Fachverfahren einfügen zur Software zur Zahlungsabwicklung einfügen und von dort zur Auszahlung an die Bundesbank und/oder im Rahmen der internen Verarbeitung (Innentäter) - bei Behörde ggf. Kasse einfügen - beim Bezahldienst unbefugten Personen offengelegt bzw. sich von Seiten Unbefugter angeeignet werden.
7.1.3	Was sind die Risikoquellen?	- Das Abfangen und die Entschlüsselung der Antragsdaten auf dem Weg zwischen dem Webportal und Secupay - Missbräuchliche Verwendung der Daten in der Behörde ggf. Kasse einfügen
7.1.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	- Sicherheitskonzept des Bezahldienstes betrieben in einem Rechenzentrum in Deutschland mit einer BSI-Zertifizierung nach ISO 27001) - Serverseitig zur Bearbeitung ausschließlich HTTPS Verbindungen akzeptiert - Zugang nur nach Freischaltung der IP Adressen durch IT-Dienstleister einfügen und durch den Bezahldienst - Nutzerkonten mit individuellen Passwörtern gesichert - Berechtigungskonzept ist vorhanden
7.1.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.1.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☐ geringfügig ☐ überschaubar ☒ substantiell ☐ groß Beschreibung: Die unter Ziffer 7.1.1 beschriebenen möglichen Auswirkungen beim Eintritt des Risikos führen aufgrund der Sensitivität der verarbeiteten Daten zu einer substantiellen Schadenshöhe. Denn Betroffene erleiden eventuell signifikante Konsequenzen (z.B. auch in den Heimatländern), die sie nur mit ernsthaften Schwierigkeiten überwinden können. Die unter Ziffer 7.1.4 beschriebenen, sehr umfänglichen Sicherheitsmaßnahmen (TOMs) können an der Schadenshöhe im Falle des Eintritts des Risikos nichts Wesentliches ändern, wenn unbefugte Personen durch einen Angriff von außen (Hacker) oder von innen (Innentäter) an die Daten gelangen und diese für eigene (und i.d.R. kriminelle) Zwecke verwenden.

		Siehe die datenschutzrechtliche Schutzbedarfsfeststellung.
7.1.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Durch den Einsatz der zuvor beschriebenen Verschlüsselungstechnik und interner Kontroll- und Sicherungsmaßnahmen ist die Eintrittswahrscheinlichkeit als überschaubar anzusehen. Dies gilt sowohl für das Risiko der Offenlegung durch unbefugte Dritte an Übergabepunkten als auch für einen unbefugten internen Zugriff innerhalb der Behörde einfügen. Ein Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein. Vgl. hierzu die obige Tabelle in Ziffer 7 „Möglicher Grad der Eintrittswahrscheinlichkeit“. Dies gilt sowohl für das Risiko der Offenlegung und unzulässigen Verwendung durch unbefugte Dritte insbesondere an Übergabepunkten, als auch für einen unbefugten internen Zugriff innerhalb der Behörde einfügen oder innerhalb des Rechenzentrums des Bezahldienstes.
7.1.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben, Ziffer 7)?	Risikobewertung: normal (Ergebnis aus Risikomatrix aus Risikoschweregrad: substanziell, Eintrittswahrscheinlichkeit: überschaubar) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko als normal anzusehen und somit vertretbar ist.
7.2	**Risiko: Unerwünschte Veränderung von Daten** **Schutzziel: Integrität**	
7.2.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Es könnte zur falschen Höhe der Auszahlung von Leistungen nach dem AsylbLG kommen, sollte der übermittelte Datensatz korrumpiert und so Grundlage der Verarbeitung werden.
7.2.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Die Daten können auf den Servern/Arbeitsrechnern verfälscht werden. Das Risiko kann eintreten, sofern insbesondere die folgenden denkbaren Szenarien eintreten: Manuelle Fehleingaben der Sachbearbeitung, Man-in-the-middle attack (MITM-Angriff) oder - Datenverluste im Rechenzentrum (Platten-Crash, Brand, Wassereintritt o.ä.).

7.2.3	Was sind die Risikoquellen?	- Innentäter - Hacker - technische Fehler
7.2.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	- Sicherheitskonzept des Bezahldienstes betriebenen in einem Rechenzentrum in Deutschland mit einer BSI-Zertifizierung nach ISO 27001) - Serverseitig zur Bearbeitung ausschließlich HTTPS Verbindungen akzeptiert - Zugang nur nach Freischaltung der IP Adressen durch IT-Dienstleister einfügen und durch den Bezahldienst - Nutzerkonten mit individuellen Passwörtern gesichert - Wiederherstellungsmöglichkeiten und redundante Datensicherung im RZ des Bezahldienstes
7.2.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.2.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Der Risikoschweregrad und das damit verbundene Schadensausmaß im Fall der Verletzung der Datenintegrität erscheint unter Berücksichtigung der geplanten technischen und organisatorischen Maßnahmen als überschaubar. Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können. Spätestens beim Wiedervorsprechen in der Behörde einfügen würden fehlerhafte Datensätze auffallen.
7.2.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☒ geringfügig ☐ überschaubar ☐ substantiell ☐ groß Beschreibung: Durch den Einsatz der zuvor beschriebenen Verschlüsselungstechnik und interner Kontroll- und Sicherungsmaßnahmen ist die Eintrittswahrscheinlichkeit als geringfügig anzusehen.
7.2.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben)?	Risikobewertung: gering (Risikoschweregrad: überschaubar, Eintrittswahrscheinlichkeit: gering) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko gering und somit vertretbar ist.

7.3	**Risiko: Datenverlust** **Schutzziel: Verfügbarkeit**	
7.3.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Die Möglichkeit zur Nutzung des Webportals in der Behörde einfügen und durch die Kartennutzer wird zeitweise unterbrochen. Dennoch können Leistungen weiterhin in Ausnahmefällen in anderer Weise erbracht werden.
7.3.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Ausfälle technischer Natur wären möglich, wenn: - Ausfall IT-Dienstleister ergänzen / durch Behörde ergänzen - Ausfall Webportal
7.3.3	Was sind die Risikoquellen?	- Fehler im Serverbetrieb - Wartungsarbeiten - Stromausfall - Menschliches Versagen
7.3.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	- Betriebs- und Sicherheitskonzept des Bezahldienstes - Mehr-Augen-Prinzip bei der Sachbearbeitung - Belehrung über Pflichten des Arbeitnehmers (Verhaltenskodex) - Kleiner Kreis an zugriffberechtigten Personen - Möglichkeit zur Auszahlung von Bargeld besteht weiterhin
7.3.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.3.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Angesichts der zuvor beschriebenen Maßnahmen, welche die vorhergenannten Risiken helfen zu bewältigen, kann ein überschaubarer Risikoschweregrad für Betroffene in Bezug auf das Schutzziel Verfügbarkeit festgestellt werden.
7.3.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Die Eintrittswahrscheinlichkeit wird in Ermangelung entgegenstehender Erkenntnisse und in Ansehung grundsätzlich ausreichender und funktionierender systemischer Gewährleistung des Schutzziels der Verfügbarkeit für überschaubar gehalten. Ein Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände und der technischen und organisatorischen

		Maßnahmen scheint der Eintritt aber unwahrscheinlich zu sein.
7.3.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben)?	Risikobewertung: gering (Risikoschweregrad: überschaubar, Eintrittswahrscheinlichkeit: überschaubar) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko vertretbar ist.
7.4	**Risiko: lange Zugriffsmöglichkeit auf personenbezogene Daten** **Schutzziel: Datenminimierung**	
7.4.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Die Auswirkungen für die Betroffenen sind bei einer Verletzung des Schutzziels der Datenminimierung zumeist nicht unmittelbar spürbar bzw. festzustellen. Die Betroffenen wissen hiervon zumeist gar nichts, da sie von der unterbliebenen Löschung in der Regel nichts mitbekommen. Nichtsdestotrotz stellt eine zu lange Speicherung der für die Sachbearbeitung benötigten personenbezogenen Daten von Antragstellern und/oder Leistungsempfängern einen Verstoß gegen Art. 17 Abs. 1 lit. a DS-GVO dar. Hiernach hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Die personenbezogenen Daten der betroffenen Personen wären infolgedessen unnötig lange den übrigen Risiken wie der unerwünschten Veränderung von Daten, dem Datenverlust, der Zweckentfremdung der Daten und der Verletzung des Rechts auf informationelle Selbstbestimmung ausgesetzt. Auch würde das Recht der Betroffenen auf sofortige Löschung aus Art. 17 Abs. 1 lit. a DS-GVO, sobald ihre personenbezogenen Daten nicht mehr für den Zweck der Aktion benötigt werden, verletzt. Des Weiteren würde der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DS-GVO durch eine nicht erforderliche längere Speicherung und Verwendung verletzt.
7.4.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Dauerhaftes Speichern der erhobenen Daten wegen technischem oder menschlichem Versagen, Unterbleiben der festgelegten Aufbewahrungsdauer im Bezahldienst bzw. in den behördlichen Anwendungen.
7.4.3	Was sind die Risikoquellen?	Die erhobenen Daten könnten ggf. aus technischen Gründen (Softwareprobleme, Hardwareprobleme) vorübergehend nicht gelöscht werden.

		Des Weiteren könnte die Löschung aufgrund von Verstößen der beteiligten Mitarbeiterinnen und Mitarbeiter gegen die festgelegten Löschanordnungen unterbleiben.
7.4.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Bezahldienst: Während der Nutzung des Bezahldienstes (Webportal zur Generierung der IBAN und Zuordnung einer Bezahlkarte) werden die Daten im Serverspeicher abgelegt. Nach erfolgreicher Beendigung, Abbruch oder Zwischenspeicherung der Anwendung werden sowohl die Datensätze verworfen. Dies wird technisch durch entsprechende Programmierung sichergestellt. Behörde einfügen: Die Erhebung der personenbezogenen Daten erfolgt im vorgelagerten Prozess in Kombination mit der Fachanwendung Fachverfahren einfügen. Im Webportal werden lediglich die für die Ausgabe und Auszahlung über die SocialCard benötigten Daten übertragen. Es wird geprüft, ob eine kassenrechtliche Dienstanweisung zur Bezahlkarte erforderlich ist.
7.4.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.4.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒ geringfügig ☐ überschaubar ☐ substantiell ☐ groß Beschreibung: Der Risikoschweregrad erscheint als gering, insbesondere in Ansehung der o.g. Maßnahmen. Insbesondere unvorhersehbare technische Ursachen können möglicherweise dazu führen, dass sich die Löschung der Daten verzögert. Angesichts der Sicherungsmechanismen dürfte dies aber allenfalls ein überschaubarer Zeitraum sein und der ganze Vorgang eng überwacht werden. Für die Betroffenen bestehen eher abstrakte Risiken für ihr Recht auf Vergessenwerden, wie oben bereits erwähnt.
7.4.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Die Wahrscheinlichkeit des Eintritts des o.g. Risikos wird angesichts bewährter technischer und organisatorischer Abläufe beim Bezahldienst und der sehr beherrschbaren Datenminimierung beim Übertrag der Beschäftigten als überschaubar angesehen. Ein Schaden kann zwar eintreten, aus bislang

		gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände und technischen und organisatorischen Maßnahmen scheint der Eintritt aber unwahrscheinlich zu sein.
7.4.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben)?	Risikobewertung: gering (Risikoschweregrad: gering, Eintrittswahrscheinlichkeit: überschaubar) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko vertretbar ist.
7.5	**Risiko: Zweckentfremdung der Daten** **Schutzziel: Nichtverkettung**	
7.5.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Realistische Szenarien für eine unzulässige zweckändernde behördliche Verarbeitung sind im Rahmen des begrenzten Scopes des Bezahldienst SocialCard nicht ersichtlich.
7.5.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Siehe Ziffer 7.5.1
7.5.3	Was sind die Risikoquellen?	Siehe Ziffer 7.5.1
7.5.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Siehe Ziffer 7.5.1
7.5.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Siehe Ziffer 7.5.1
7.5.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒ geringfügig ☐ überschaubar ☐ substantiell ☐ groß Beschreibung: Siehe Ziffer 7.5.1
7.5.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☒ geringfügig ☐ überschaubar ☐ substantiell ☐ groß Beschreibung: Siehe Ziffer 7.5.1
7.5.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben)?	Risikobewertung: gering (Risikoschweregrad: gering, Eintrittswahrscheinlichkeit: gering) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko vertretbar ist.

7.6	**Risiko: Verschleierung des Datenflusses** **Schutzziel: Transparenz**	
7.6.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Hier ist insbesondere auf die Folgen mangelnder Transparenz hinsichtlich der Zuständigkeiten, der Herkunft und des Verwendungszwecks der Daten abzustellen. Der betroffene Personenkreis (also die Asylsuchenden) könnte bei Eintritt des Risikos, also einer Verletzung der Transparenzpflichten, nicht über die betroffenen Rechte und über den Zweck der Datenerhebung, z.B. dass die Daten auch über Dritte weiterverarbeitet werden, informiert sein. Eine Verschleierung des Datenflusses ist nicht gegeben. Die betroffenen Personen sind grundsätzlich darüber informiert, dass Daten durch die Behörde einfügen, vgl. Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e DS-GVO und dem AsylblG verarbeitet werden mit dem Ziel: - Feststellungen treffen und Leistungen gewähren zu können - die mit der Leistungserbringung verbundenen gesetzlichen Aufgaben durchführen zu können - Bereits getroffene Feststellungen in Verfahren von Amts wegen überprüfen zu können
7.6.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Fehlende oder unklare Information der betroffenen Personen über die Aktion und die damit verbundene Datenverarbeitung. Verletzung der Informationspflichten nach Art. 13 und Art. 14 DS-GVO und der Transparenzvorgaben des Art. 12 DS-GVO.
7.6.3	Was sind die Risikoquellen?	Beim Ausstellen der Unterlagen wird die nach Art. 13 und Art. 14 DS-GVO bei einer Datenerhebung vorgeschriebene Information versäumt oder aufgrund technischer Probleme im Druckablauf nicht vorgenommen. Es können weitere Verarbeitungsschritte notwendig werden, die in der übermittelten Information nicht berücksichtigt wurden.
7.6.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Betroffene Personen werden durch die in Punkt 5.1 beschriebenen Maßnahmen, insb. durch entsprechende Informationsschreiben oder Merkblätter über die Datenverarbeitung nach Maßgabe der Informationspflichten aus Art. 13 und 14 DS-GVO in Kenntnis gesetzt.
7.6.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.6.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒ geringfügig ☐ überschaubar ☐ substantiell ☐ groß Beschreibung:

		Das Risiko wird aufgrund der o.g. Begründung als geringfügig eingeschätzt. Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
7.6.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Durch die Erfüllung der Informationspflichten nach Art. 13 und 14 DS-GVO wird die Eintrittswahrscheinlichkeit als geringfügig überschaubar betrachtet. Ein Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.
7.6.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben)?	Risikobewertung: gering (Risikoschweregrad: gering, Eintrittswahrscheinlichkeit: überschaubar) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko vertretbar ist.
7.7	**Risiko: Verletzung des Rechts auf informationelle Selbstbestimmung** **Schutzziel: Intervenierbarkeit**	
7.7.1	Was könnten die wesentlichen Auswirkungen für die betroffenen Personen sein, wenn das Risiko eintritt?	Die Verletzung des Schutzziels der Intervenierbarkeit wäre insbesondere dann gegeben, wenn die Betroffenen ihre Rechte (insb. Löschung, Berichtigung, Einschränkung der Verarbeitung, Widerspruch) nicht effektiv gegenüber dem Verantwortlichen (Behörde einfügen) geltend machen könnten.
7.7.2	Was sind die Hauptbedrohungen, die zu dem Risiko führen könnten?	Das o.g. Risiko wird insbesondere durch mangelnde Transparenz, den Verstoß gegen die Informationspflichten aus Art. 13 und Art. 14 DS-GVO, die mangelnde verbindliche und effiziente Regelung über Zuständigkeiten zur Bearbeitung von Anliegen zur Wahrnehmung der Betroffenenrechte, fehlende interne Dokumentation und den damit verbundenen Verstoß gegen die Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO realisiert. Auch mangelnde technische Umsetzungsmöglichkeiten (z.B. hinsichtlich der Umsetzung der Löschung nach Art. 17 Abs. 1 lit. a DS-GVO) zur Realisierung der Betroffenenrechte führen zu einem entsprechenden Risiko.
7.7.3	Was sind die Risikoquellen?	Siehe 7.6.3. Risiken können sich durch fehleranfällige Prozesse im Zusammenhang zur Gewährleistung von Betroffenenrechten ergeben. Daten könnten z.B. nicht vollständig beauskunftet oder gelöscht werden.

7.7.4	Welche identifizierten Maßnahmen tragen zur Bewältigung des Risikos bei?	Dem o.g. Risiko wird durch die Erfüllung der Informationspflichten sowie durch für Betroffenenrechte zuständige und als solches klar ersichtliche und auch erreichbare Stellen vorgebeugt. Datenschutzerklärung
7.7.5	Müssen ergänzende Maßnahmen zur Bewältigung des Risikos ergriffen werden?	Nein.
7.7.6	Wie schätzen Sie den Risikoschweregrad ein, insbesondere hinsichtlich der möglichen Auswirkungen und geplanten Maßnahmen?	☒ geringfügig ☐ überschaubar ☐ substantiell ☐ groß Beschreibung: Angesichts der geplanten Maßnahmen ist nur von einem geringfügigen Risikoschweregrad bzw. Schadensausmaß auszugehen. Die Betroffenen werden infolge der oben und unter 7.6. beschriebenen Maßnahmen zur Erfüllung der Informationspflichten hinreichend informiert. Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können.
7.7.7	Wie schätzen Sie die Eintrittswahrscheinlichkeit des Risikos ein, insbesondere hinsichtlich der Bedrohungen, Risikoquellen und geplanten Maßnahmen?	☐ geringfügig ☒ überschaubar ☐ substantiell ☐ groß Beschreibung: Die Eintrittswahrscheinlichkeit wird angesichts der geplanten Maßnahmen, insb. der Sicherstellung der Beifügung eines Informationsblatts nach Art. 13 und Art. 14 DS-GVO, als überschaubar angesehen. Ein Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.
7.7.8	Zu welcher Risikobewertung kommen Sie unter Berücksichtigung des festgestellten Risikoschweregrads (Schadenshöhe) und der Eintrittswahrscheinlichkeit (s. Risikomatrix oben)?	Risikobewertung: gering (Risikoschweregrad: gering, Eintrittswahrscheinlichkeit; überschaubar) Durch die o.g. Abhilfe- und Sicherheitsmaßnahmen sind geeignete Vorkehrungen getroffen worden, so dass das Risiko vertretbar ist.

8.	**Stellungnahme des Datenschutzbeauftragten:** ☒ Die Verarbeitung kann so umgesetzt werden. ☐ Die Verarbeitung sollte nicht umgesetzt werden. ☐ Begründung: