Bericht über die Durchführung einer Datenschutzfolgen-Abschätzung (DSFA) nach Art. 35 DSGVO
– Digitale Einreiseanmeldung –

Version 1.2

Verfahrenstätigkeit	Digitale Einreiseanmeldung
Verantwortliche(r) i.S.d. Art. 4 Satz 1 Nr. 7 DSGVO:	Robert-Koch-Institut, vertreten durch den Präsidenten Prof. Dr. L. H. Wieler
Fachliche(r) Verantwortliche(r):	
Technische(r) Verantwortliche(r):	

Datum	Tätigkeit
08.11.2020	Erstellung (Version 1.0)
12.01.2021	Ergänzung und Überarbeitung, insbesondere Double-Opt-In, Content Delivery Network, Adressvervollständigung (Version 1.1)
11.02.2021	Ergänzung und Überarbeitung, insbesondere neue Datenkategorien (negativer Coronavirus-Test, Ausnahmetatbestände), Einwilligung als Rechtsgrundlage, Wegfall der Angabe von Daten für Mitreisende

Version vom	11.02.2021
Stellungnahme DSB	
Freigabe	

I. Inhaltsverzeichnis

1. Überblick und Zweck dieses Berichts[1]

Dieser Bericht dokumentiert eine vom Robert Koch-Institut („RKI“) durchgeführte Datenschutz-Folgenabschätzung („DSFA“) nach Art. 35 DSGVO für die unter Kapitel 4 beschriebene Verarbeitungstätigkeit im Rahmen der Digitalen Einreiseanmeldung („DEA“) (Prüfgegenstand). Die DEA ist ein vom RKI eingerichtetes elektronisches Melde- und Informationssystem für Einreisende aus sog. Risikogebieten nach Deutschland zur Mitteilung bestimmter, für die Infektionsbekämpfung relevanter, personenbezogener Daten. Das System dient der Verhütung und Bekämpfung von Infektionskrankheiten und soll erstmalig im Rahmen der COVID-19-Pandemie ab Anfang November 2020Anwendung finden.

Die DEA ist für die Nutzungsverpflichteten online zugreifbar unter https://www.einreiseanmeldung.de („Website“). Der Prüfgegenstand umfasst nur den Bereich des Gesamtverfahrens, der in der datenschutzrechtlichen Verantwortlichkeit des RKI liegt. Verarbeitungstätigkeiten, die durch andere eigenständige Verantwortliche erfolgen, werden daher nur berücksichtigt, soweit sie für die datenschutzrechtliche Bewertung oder das Verständnis der vom RKI verantworteten Verarbeitungstätigkeiten relevant sind.

2. Erforderlichkeit der DSFA / Schwellwertanalyse

Die Durchführung einer DSFA in Bezug auf das Verarbeitungsverfahren wird aus den folgenden Gründen als erforderlich angesehen:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit („BfDI“) hat nach Art. 35 Abs. 4 DSGVO eine Liste von Verarbeitungsvorgängen des öffentlichen Bereichs erstellt[2], für die eine DSFA zwingend durchzuführen ist („Positiv-Liste“). Die Verarbeitungstätigkeit des RKI erfüllt voraussichtlich jedenfalls die in der Positiv-Liste aufgeführten Merkmale 5 und 7, die die Durchführung einer DSFA erforderlich machen.

Merkmal 5 (*Verarbeitung in großem Umfang*): Es handelt sich voraussichtlich um eine Verarbeitung in großem Umfang. Die Artikel-29-Datenschutzgruppe hat ihrer Stellungnahme WP148, bestätigt vom Europäischen Datenschutzausschuss, unter Bezugnahme auf Erwägungsgrund 91 DSGVO die Zahl der Betroffenen, die verarbeitete Datenmenge, die Dauer oder Dauerhaftigkeit der Datenverarbeitung und das geografische Ausmaß der Datenverarbeitung als Anhaltspunkte für eine umfangreiche Datenverarbeitung benannt.[3] Im Rahmen der DEA sollen personenbezogene Daten aller nach Deutschland aus Risikogebieten einreisendeen n Person verarbeitet werden. Die Zahl der Betroffenen liegt voraussichtlich bei mindestens mehreren zehn- oder hunderttausend Einreisenden pro Monat, so dass von einer Verarbeitung in großem Umfang auszugehen ist.

Merkmal 7 (*Verarbeitung von Daten Schutzbedürftiger*): Die Artikel-29-Datenschutzgruppe fasst in der genannten Stellungnahme unter Schutzbedürftige u.a. Kinder und Bevölkerungsteile mit

---

[1] Zur besseren Lesbarkeit wird in dem DSFA-Bericht auf eine gegenderte Schreibweise verzichtet. Es sind aber jeweils Personen aller Geschlechter gemeint.

[2] Bundesbeauftragter für Datenschutz und Informationsfreiheit, Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes vom 1.10.2019, URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_VerarbeitungsvorgaengeArt35.pdf?__blob=publicationFile&v=5 (Abruf 4.11.2020).

[3] Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01, 2017, S. 11.

besonderem Schutzbedarf (Senioren, Patienten etc.). Im Rahmen der DEA sollen personenbezogene Daten aller Einreisenden aus Risikogebieten verarbeitet werden. Daher sind voraussichtlich (auch) Schutzbedürftige im o.g. Sinne von der Verarbeitung betroffen.

3. Geltungsbereich

Gegenstand der DSFA sind die spezifischen Datenschutzrisiken der Verarbeitung, wie in Kapitel 4 beschrieben.

4. Beschreibung der Verarbeitungstätigkeit (Prüfgegenstand)

Der Prüfgegenstand umfasst nur die Verarbeitung von personenbezogenen Daten der Personen, deren Daten im Rahmen des DEA an das RKI übermittelt werden. Die Verarbeitung von Daten anderer Personen (z.B. Mitarbeiter der Gesundheitsämter) ist nicht vom Prüfgegenstand umfasst, auch wenn diese mit der Verarbeitungstätigkeit einhergehen, da für sie die Voraussetzungen gem. Art. 35 Abs. 4 DSGVO nicht vorliegen.

4.1. Ausgangslage und bisheriges Anmeldeverfahren

Im Zusammenhang mit dem Coronavirus SARS-CoV-2 und der Krankheit COVID 19 gelten weiterhin besondere Bestimmungen für die Einreise nach Deutschland. Bislang werden Einreisende nach Deutschland weitgehend analog bzw. papierbasiert mittels sog. Aussteigekarten erfasst, die von Reisenden aus Risikogebieten nach ihrer Einreise in das Bundesgebiet ausgefüllt werden müssen. Dieser Prozess lässt sich nur teilweise automatisieren. Infolgedessen kommt es - regelmäßig zu kapazitätsbedingten Verzögerungen bei der Übermittlung der Aussteigekarten, so dass die zuständigen Gesundheitsämter ihren zeitkritischen Aufgaben, insbesondere bzgl. der Überwachung der Quarantäne und Kontaktnachverfolgung, nicht bzw. nicht zeitgerecht nachkommen können.

4.2. Neues Verfahren der DEA

Die Erfassung von einreisenden Personen aus Risikogebieten soll fortan weitgehend digital über die DEA erfolgen, wobei die betroffenen Personen im Rahmen der DEA weniger personenbezogene Angaben über sich mitteilen sollen als bisher auf den analogen Aussteigekarten (z.B. werden keine Symptome mehr nachgefragt). Zusätzlich bleibt eine analoge Form der Einreiseanmeldung weiterhin ersatzweise möglich, die nicht Prüfgegenstand dieser DSFA ist. Die DEA soll die Gesundheitsämter bei den ihnen durch das IfSG zugewiesenen Verwaltungsaufgaben im Vorfeld unterstützen und entlasten. Die für eine Kontaktnachverfolgung und Überwachung relevanten personenbezogenen Daten sollen insoweit schneller und zielgerichteter in einem einheitlichen Format an die zuständigen Gesundheitsämter gelangen.

Nach der Verordnung des BMG zum Schutz vor einreisebedingten Infektionsgefahren in Bezug auf das Coronavirus SARS-CoV-2 nach Feststellung einer epidemischen Lage von nationaler Tragweite durch den Deutschen Bundestag vom 13. Januar 2021 („Verordnung“) ist eine nach Deutschland einreisende Person, die sich zu einem beliebigen Zeitpunkt in den letzten 10 Tagen vor der Einreise in einem Gebiet aufgehalten hat, das durch das RKI zum Zeitpunkt der Einreise auf seiner Internetseite (https://www.rki.de/covid-19-risikogebiete) als gefährdetes Gebiet mit erhöhtem Infektionsrisiko in Bezug auf eine Infektion mit dem Coronavirus SARS-CoV-2 eingestuft wurde („Risikogebiet“), grundsätzlich verpflichtet, der zuständigen Behörde vor der Einreise

bestimmte personenbezogene Daten über die DEA mitzuteilen. Zu diesen Daten zählen insbesondere Aufenthaltsorte der einreisenden Person bis zu 10 Tage vor und nach der Einreise und das für die Einreise genutzte Reisemittel.

4.3. Zwecke

Die Zwecke der Verarbeitung im Rahmen des Prüfgegenstands lassen sich wie folgt definieren:

Zweck 1 ist der Betrieb des elektronischen Melde- und Informationssystems (DEA), um informations- und meldepflichtigen Personen die Erfüllung ihrer Pflichten gem. Abschnitt I. Nummer 1 der Anordnungen zu ermöglichen.

Zweck 2 ist die Übermittlung der bei dem Betrieb des elektronischen Melde- und Informationssystems (DEA) von informations- und meldepflichtigen Personen gem. Abschnitt I. Nummer 1 der Anordnungen vor Einreise aus einem Risikogebiet mitgeteilten personenbezogenen Daten an die zuständigen Behörden mit der Möglichkeit, dass diese die Daten im Rahmen ihrer jeweiligen Zuständigkeit verarbeiten können.

4.4. Neues Verfahren im Einzelnen

4.4.1. Aufruf des Einreisenden-Frontends

Die einreisende Person ruft für die Dateneingabe die Website über ihren PC oder ihr Smartphone auf. Dabei werden verschiedene Zugriffsdaten erhoben und in Logdateien gespeichert. Die Verbindung ist dabei über TLS – Transport Layer Security – abgesichert.

4.4.2. Dateneingabe in das Einreisenden-Frontend

Die einreisende Person kann auf der Website die Länder und Regionen, aus denen sie einreist, in ein Online-Formular eingeben, um zu prüfen, ob eine Einstufung als Risikogebiet und insoweit eine Meldepflicht besteht. Die Website stellt dem aufrufenden Browser einen JavaScript Client zur Verfügung, der die aktuelle Liste aller Risikogebiete des RKI enthält. Ferner lädt der JavaScript Client aktuelle redaktionelle Informationen, etwa aktuelle Hinweise oder rechtliche Grundlagen, die von den zuständigen staatlichen Stellen zur Verfügung gestellt werden. Die sodann folgende Eingabe der einreisenden Person – also die Auswahl des relevanten Landes sowie die danach folgende Dateneingabe – erfolgt lokal auf dem Gerät des Betroffenen. Nach der Prüfung des Risikogebiets erscheint eine Meldung auf der Website, die der einreisenden Person entweder die Pflicht zur Übermittlung der Reiseangaben und personenbezogenen Daten anzeigt oder aber mitteilt, dass eine entsprechende Übermittlung an das Gesundheitsamt nicht erforderlich ist. Nur in ersterem Fall erscheint der Button „zur Eingabe“, wonach die einreisende Person auf die eigentliche Dateneingabeseite weitergeleitet wird.

Nach Weiterleitung auf die Dateneingabemaske und Eingabe der persönlichen Daten einschließlich Telefonnummer und E-Mail-Adresse erfolgt eine Validierung der Kontaktdaten. Die einreisenden Personen haben die Möglichkeit zu wählen, ob sie ihre E-Mail Adresse oder Ihre Mobilfunknummer validieren möchten. Anschließend bekommen sie eine TAN an die entsprechende Kontaktadresse geschickt. Diese hinterlegen die Nutzer zur Beendigung des Anmeldeprozesses im Interface. Wenn die einreisende Person die Kontakt-Methode SMS zur Verifikation ausgewählt hat, wird seine Mobilfunknummer mit der TAN an den Message-System Dienstleister Message Mobile GmbH übergeben, der dann die SMS an den Reisenden erzeugt.

Anschließend trägt die einreisende Person ihre Adressdaten ein. Als Unterstützung für die Eingabe der Adresse erfolgt eine Nutzung des als Software as a Service angebotenen Geokodierungsdienstes für Adressen und Geonamen des Bundesamtes für Kartographie und Geodäsie (BKG).

Nachdem die Einreisenden mit der Eingabe des Wohnortes, Straßennamens und der Hausnummer begonnen haben, bekommen sie nach und nach Adressvorschläge und können schließlich die richtige Eingabe auswählen. Bei jedem eingegebenen Zeichen und jeder Auswahl wird ein Request an das bei der Bundesdruckerei betriebene Backend geschickt. Der Backend-Server schickt den Request weiter an den Geokodierungsdienst und reicht die Antwort des Geokodierungsdienstes dann zurück an den Browser der Nutzer*innen. Bei den „Requests“, die an den Geokodierungsdienst geschickt werden, wird also nicht die IP-Adresse der Nutzer*innen mitgeschickt, sondern die IP-Adresse des Backend-Servers.

In der Sicherheitsarchitektur des Dienstleistungszentrums werden die kostenrelevanten Anfragen bei einem nutzungsbezogenen Tarif mit minimalen Angaben geloggt. Die oben genannten Suchparameter gehören nicht dazu. Geloggt werden technische Angaben, die den kostenrelevanten Zugriff belegen: Zeit, IP-Adresse, Nutzeridentifikator beim BKG, Name des aufgerufenen Dienstes, Anzahl der bereitgestellten Objekte. Der Geokodierungsdienst und ebenso die vorgelagerte IT-Infrastruktur des BKG speichern keine an ihn gerichteten Anfragen mit ihren semantischen Parametern, auch nicht temporär. Die Suchparameter und die Ergebnisse der Suche werden nur flüchtig verarbeitet, um die Antwort an den Client zu senden.

Anschließend haben Einreisende die Möglichkeit Angaben über möglicherweise vorliegende Ausnahmetatbestände oder zum Vorliegen eines negative Coronavirus SARS-CoV-2-Tests zu machen. Die Angaben sind freiwillig und als solche gekennzeichnet. Wenn die einreisende Person entsprechende Angaben macht, wird sie zusätzlich aufgefordert, eine entsprechende Einwilligung zur Verarbeitung Ihrer Daten zu erteilen. Dazu setzt sie einen Haken vor der entsprechenden Erklärung. Anderenfalls kann sie nicht „Weiter“ klicken.

4.4.3. Übermittlung an Server der Bundesdruckerei

Nach Abschluss der Eingabe werden die Daten in einem neuen Fenster mit einer jeweils durch einen Button erscheinenden Möglichkeit der Überarbeitung bei möglichen Fehlern angezeigt.

Klickt der Nutzer anschließend auf den Übermittlungsbutton, werden die folgenden Funktionen ausgelöst:

aa) Die digital zusammengefassten Informationen werden § 6 IFG [redacted]

bb) Auf dem lokalen Device des Betroffenen werden die gemachten Angaben als PDF angezeigt und können gespeichert werden. Dieses PDF-Dokument wird nicht per E-Mail versendet, sondern nach erfolgreicher Datenübertragung als Bestätigung auf dem Endgerät der Reisenden generiert.

Es hat vor allem eine Nachweisfunktion für die Betroffenen, die das Dokument direkt auf ihrem Gerät vorzeigen und abspeichern können.

cc) Der Datensatz wird – mit Hilfe von Transport- und Inhaltsverschlüsselung – an die Server der Bundesdruckerei übermittelt.

4.4.4. Übermittlung an das zuständige Gesundheitsamt

Für die Übermittlung der Datensätze an die zuständigen Gesundheitsämter, die nach erfolgter Übermittlung dann das dortige Verwaltungsverfahren eröffnen, gibt es drei unterschiedliche Varianten.

aa) Direkte Anbindung der Gesundheitsämter

§ 6 IFG [redacted] Nach Übermittlung der lokalen verschlüsselten Datensätze von den Devices der Betroffenen an den Server des Auftragsverarbeiters wird dort eine Sortierung der Datensätze nach Postleitzahl vorgenommen.Der Serverstandort ist Deutschland.

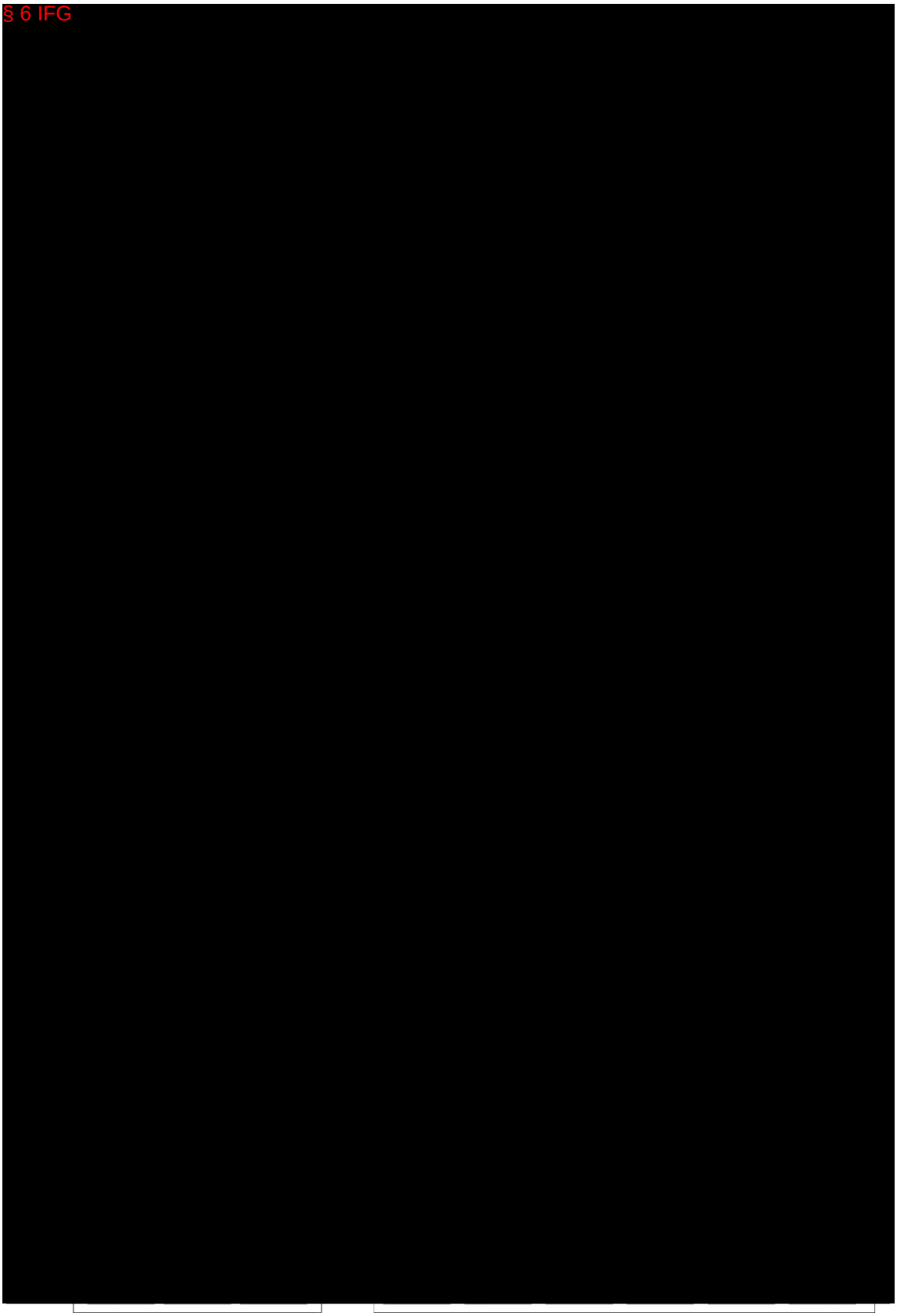
Die von der einreisenden Person eingetragenen personenbezogenen Daten werden zentral abgespeichert und den Gesundheitsämtern über ein eigenes Frontend zugänglich gemacht. Die Gesundheitsämter haben nur Zugriff auf den Teil der gespeicherten Einreiseanmeldungen, der innerhalb ihres örtlichen Zuständigkeitsbereiches liegt. Das Gesundheitsamt wird anhand der Postleitzahl des Zielortes ermittelt. Mit einem gesundheitsamtspezifischen öffentlichen Schlüssel wird das Datenpaket so übermittelt, dass nur dasjenige Gesundheitsamt die Datensätze entschlüsseln kann, das über den passenden Schlüssel verfügt.

Berechtigte Mitarbeiter der Gesundheitsämter verfügen im Gesundheitsamt-Portal über einen Button, der serverseitig den Export der für das jeweilige Gesundheitsamt verfügbaren Daten startet, welche dann im Gesundheitsamt-Client entschlüsselt werden. Hierbei handelt es sich um die Daten, die den jeweiligen Mitarbeitern im Interface zur Verfügung stehen.

Daneben gibt es für die Gesundheitsämter die Möglichkeit, einen sogenannten CSV-Export aus denjenigen Daten zu generieren, die zu ihrem Zuständigkeitsbereich gehören. Angezeigt wird insoweit eine Liste, die – je nach möglicher Datenkategorie in Spalten getrennt – die Daten der letzten 14 Tage vollständig enthält.

bb) Übermittlung durch Deutsche Post

§ 6 IFG



§ 6 IFG

Für einen Übergangszeitraum, solange einige Gesundheitsämter noch nicht an die Systeme der Bundesdruckerei angeschlossen sind, erfolgt in diesen Fällen eine Offenlegung der Datensätze der Betroffenen nicht direkt an das zuständige Gesundheitsamt, sondern an die Deutsche Post. Die Bundesdruckerei lädt dabei die verschlüsselten Daten auf einen Server der Deutschen Post hoch. § 6 IFG

Auch hier erfolgt ein Mapping der angegebenen PLZ auf das zuständige Gesundheitsamt. Die Daten werden dann auf einem FTP-Server in einem zugangsgeschützten Unterordner des jeweils zuständigen Zielgesundheitsamts abgelegt, wo sie via SFTP durch die jeweils zuständigen Gesundheitsämter abgerufen werden.

cc) Übermittlung durch RKI („Clearing Stelle“)

Es hat sich in Tests des Systems gezeigt, dass eine Restmenge von PLZ nicht eindeutig automatisiert einem zuständigen Gesundheitsamt zugeordnet werden kann. Hierfür wird mittels der bestehenden Struktur eine sogenannte Clearing-Stelle beim RKI integriert. Das RKI wird in gleicher Weise wie die zuständigen Gesundheitsämter an die Systeme der Bundesdruckerei angebunden.

Alle PLZ, welche im Frontend des Reisenden keinem GA zugeordnet werden können und für die somit kein öffentlicher Schlüssel zur Verschlüsselung zur Verfügung steht, werden mit dem öffentlichen Schlüssel des RKI verschlüsselt. Das RKI greift § 6 IFG auf den Web-Zugriff zu und kann dort alle nicht zugewiesenen Datensätze vorfinden. Der Verantwortliche ist nun in der Lage anhand der detaillierten Merkmale über die PLZ hinaus eine eindeutige Zuweisung an ein Gesundheitsamt vorzunehmen. Für diese Einzelfälle kann die Clearing-Stelle des Verantwortlichen derzeit einen CSV-Export generieren, welchen sie über einen gesicherten Austausch § 6 IFG an die jeweils zuständigen Gesundheitsämter übertragen können.

5. Datenübermittlung an Drittländer

Greift ein Einreisender auf die Website einreiseanmeldung.de zu, stellt der Webserver eine Datei index.html bereit. Dem Endgerät des Einreisenden werden die in der Datei index.html benannten Web-Ressourcen (Inhalte der Website) mittels eines CDN bereitgestellt. Dazu wird die Anfrage des Reisenden-Clients via DNS an den lokalen Cloudfront Edge-Standort weitergeleitet, der die Anfrage am schnellsten beantworten kann. In der Regel ist dies der dem Endnutzer nächstgelegene Edge-Standort. Wenn die angeforderten Dateien im Cache des Edge-Standorts vorhanden sind, gibt das CDN sie an das anfragende Endgerät weiter. Anderenfalls werden die Dateien zunächst vom Ursprungsserver an den Edge-Standort gesendet und sodann dem Einreisenden von dort bereitgestellt. Die Dateien werden dann im Cache des Edge-Standorts gespeichert, damit sie bei der nächsten Anfrage eines Reisenden sofort zur Verfügung stehen. Bei den über den CDN angefragten Dateien handelt es sich stets um die Inhalte der Website (Grafiken, Texte, notwendige Daten für die jeweiligen Website-Funktionen), die für alle Nutzer gleich angezeigt werden. Sofern der Edge-Standort, von dem die Daten dem Einreisenden zur Verfügung gestellt werden, in einem Drittland liegt, kommt es insoweit zu einer Übermittlung der IP-Adresse des Endgerätes des Einreisenden sowie Metadaten (wie z.B. Browser, Betriebssystem-Version, User Agent, Character Sets) an diesen Edge-Server des CDN. Die von dem Einreisenden eingegebenen Daten werden auf den Endgeräten verschlüsselt und direkt an die Server der Bundesdruckerei übermittelt. Eine Drittlandsübermittlung dieser Daten findet nicht statt.

6. Verarbeitete Daten

Bei Aufruf der Website werden, wie bei jedem Website-Aufruf, aufgrund der HTTP-Prokokollvorgaben folgende Log-Daten automatisch erhoben:

- IP-Adresse
- Datum und Uhrzeit der Anfrage
- Zeitzonendifferenz zur Greenwich-Mean-Time (GMT)
- Inhalt der Anforderung (konkrete Seite)
- Zugriffsstatus / HTTP-Statuscode
- jeweils übertragene Datenmenge
- Website, von der die Anforderung kommt
- Browser
- Betriebssystem und dessen Oberfläche
- Sprache und Version der Browsersoftware

Die folgenden Daten von Einreisenden aus Risikogebieten werden im Rahmen der DEA, je nach Transportmittel (Flugzeug/Bahn/Bus/PKW/LKW/Schiff), abgefragt:

a) Flugzeug

- Beförderungsunternehmen
- Linien-/Flugnummer
- Name der Fluggesellschaft
- Abflugort
- Sitzplatz (optional)
- Ankunftsdatum
- Umstieg (optional)

b) Bahn

- Beförderungsunternehmen
- Zugnummer
- Sitzplatz (optional)
- Ankunftsdatum
- Einsteigeort
- Umstieg (optional)

c) Bus

- Beförderungsunternehmen
- Reservierungsnummer
- Ankunftsdatum

d) PKW

- Abfahrtsort
- Ankunftsdatum

e) LKW

- Unternehmensname
- Abfahrtsort
- Ankunftsdatum

f) Schiff

- Schiffname
- Schiffnummer
- Reisedatum (von / bis)

Darüber hinaus werden folgende Datenkategorien erfasst:

- Nachname (Familienname)
- Vorname
- Geschlecht (weiblich/männlich/divers)
- Geburtsdatum
- Staatsangehörigkeit
- Pass- oder Ausweisnummer (optional)
- Persönliche Mobilnummer
- Weitere Telefonnummern – Arbeit/Privat (optional)
- E-Mail-Adresse
- Anschrift der nächsten 14 beziehungsweise 10 Tage, also der Ort, in dem sich der Betroffene in Quarantäne begibt. Hier werden folgende Informationen erhoben:
    - Hotelname (optional)
    - Straße
    - Hausnummer
    - Wohnungsnummer (optional)
    - Postleitzahl
    - Stadt
    - Bundesland

Ggfs. werden weitere Anschriften des Einreisenden verarbeitet, sollte diese für den Zeitraum der nächsten 14 Tage für eine Kontaktnachverfolgung relevant sein.

Zudem können die Einreisenden folgende Angaben machen:

- Angabe eines Ausnahmetatbestands (beispielsweise, wenn der Aufenthalt im Risikogebiet oder in Deutschland ausschließlich zur Durchreise ohne Zwischenaufenthalt, lediglich für bis zu 24 Stunden oder aus beruflichen oder ausbildungsbedingten Gründen erfolgte)

- Vorliegen eines negativen Ergebnisses eines Coronavirus SARS-CoV-2-Tests

7. Aufbewahrungsdauer und Löschung der Daten

Gemäß Art. 5 Abs. 1 lit. e DSGVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Grundsatz der Speicherbegrenzung). Es gelten folgende Aufbewahrungs- und Löschfristen:

Personenbezogene Daten	Löschung	Zweck
Log-Daten	Speicherung nach Ende der jeweiligen Sitzung bis zu 90 Tage. Session Cookies, die zum Einsatz kommen, verfallen nach dem Ende der Sitzung.	Zur Gewährleistung der Funktionalität von Front- und Backend der „Digitalen Einreiseanmeldung“ sowie zu Analysezwecken im Falle eines Angriffs (Zweck 1)
Verschlüsselte Daten aus ausgefüllten Webformular	14 Tage nach Offenlegung an Gesundheitsamt, Deutsche Post bzw. RKI werden Daten automatisch von den Servern der Bundesdruckerei gelöscht. Die Deutsche Post löscht Daten ebenfalls innerhalb von 14 Tagen.	Übermittlung der bei dem Betrieb des elektronischen Melde- und Informationssystems (DEA) von informations- und meldepflichtigen Personen gem. Abschnitt I. Nummer 1 der Anordnungen vor Einreise aus einem Risikogebiet mitgeteilten personenbezogenen Daten an die zuständigen Behörden (Zweck 2)

8. Bewertung der Notwendigkeit und Verhältnismäßigkeit

In diesem Kapitel werden gemäß Art. 35 Abs. 7 lit. b DSGVO die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungstätigkeit in Bezug auf die Zwecke beschrieben.

8.1. Notwendigkeit

Die Datenverarbeitung im Rahmen der DEA ist notwendig, damit das RKI seine gesetzlichen Aufgaben nach den Anordnungen und dem Infektionsschutzgesetz („IfSG“) erfüllen kann.

Diese Aufgaben bestehen insbesondere darin, das elektronischen Melde- und Informationssystem zu betreiben, um informations- und meldepflichtigen Personen die Erfüllung ihrer Pflichten gem. Abschnitt I. Nummer 1 der Anordnungen zu ermöglichen.

Weiterhin ist es Aufgabe des RKI der bei dem Betrieb des elektronischen Melde- und Informationssystems (DEA) von informations- und meldepflichtigen Personen gem. Abschnitt I. Nummer 1 der Anordnungen vor Einreise aus einem Risikogebiet mitgeteilten personenbezogenen Daten an die zuständigen Behörden mit der Möglichkeit zu übermitteln, dass diese diese Daten im Rahmen ihrer jeweiligen Zuständigkeit verarbeiten können.

8.1.1. Notwendigkeit der verarbeiteten Daten:

Die Einrichtung der DEA sowie der Umfang der in Formularform abgefragten Daten werden in Abschnitt I, Ziffer 1 bzw. Anlage 2 der Anordnungen gesetzlich vorgegeben. Insoweit steht dem RKI kein Gestaltungsspielraum zu. Die Verarbeitung der personenbezogenen Daten in der DEA ist notwendig, damit das RKI die beschriebenen gesetzlichen Aufgaben erfüllen kann.

Gleiches gilt für Daten, die durch den Besuch und die Nutzung der Website bzw. DEA erhoben werden. Die Website und die damit verbundene Datenverarbeitung beim Aufruf ist integraler Bestandteil der DEA. Diese Daten müssen standardmäßig und notwendigerweise bei jedem Websitebesuch verarbeitet werden.

Dies gilt auch für die freiwilligen Angaben des Nutzers, also zum negativen Coronavirus SARS-CoV-2-Test (optional) sowie zum Vorliegen von Ausnahmetatbeständen. Die Angaben sind für die Gesundheitsämter für die Überprüfung der Einhaltung der Quarantäne-Vorschriften erforderlich.

8.1.2. Notwendigkeit der Speicherfrist:

Die Speicherdauer von 14 Tagen ist erforderlich, da nach derzeitigem Forschungsstand die Infektiosität der Betroffenen in der Regel 14 Tage lang besteht und somit die Daten für den der BMG-Anordnung zu Grunde liegenden Zweck, die Kontrolle der Einhaltung der Pflicht zur Quarantäne durch die Gesundheitsämter, für diesen Zeitraum erforderlich sind.

Auf Grundlage von Art. 6 Abs. 1 lit. e DSGVO i.V.m. § 3 BDSG und § 5 BSI-Gesetz ist das RKI die Erhebung und Speicherung der Daten zum Schutz vor Angriffen auf die Internetinfrastruktur des RKI und der Kommunikationstechnik des Bundes auch über den Zeitpunkt des Besuches der Nutzer hinaus gestattet. Die Speicherung dieser Daten für die Dauer von 90 Tagen ist üblich und insoweit als datenschutzrechtlich notwendig anzusehen.

8.1.3. Notwendigkeit der Verarbeitung durch das RKI:

Die Notwendigkeit der Verarbeitung durch das RKI folgt aus den gesetzlichen Aufgaben des RKI gemäß IfSG und den Anordnungen (siehe oben). Diese Aufgaben werden durch die durch das

Dritte Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite vom 28.10.2020 („Gesetzentwurf“) im IfSG eingeführten Änderungen bestätigt und konkretisiert. Das Gesetz sieht nun insbesondere vor, dass das RKI für die Zwecke der Einreiseanmeldung ein Melde- und Informationssystem einrichtet (§ 36 Abs. 9 S. 1 i.V.m. Abs. 8 S. 1 IfSG) und dieses als Verantwortlicher im Sinne des Datenschutzrechts betreibt (§ 14 Abs. 1 S. 2 IfSG).

8.1.4. Notwendigkeit der Auftragsverarbeitung:

Die Beauftragungen der Bundesdruckerei und der Deutsche Post beruht auf verbindlichen Weisungen des BMG an das RKI gem. § 14 Abs. 1 S. 1 IfSG und sind somit für das RKI zur Erfüllung seiner Aufgabe notwendig.

8.2. Verhältnismäßigkeit

Die Verarbeitungstätigkeit des RKI ist verhältnismäßig, da sie (1) einem legitimen Zweck dient, der zur Zweckerreichung (2) geeignet, (3) erforderlich und (4) angemessen ist.

(1) Die Verarbeitung erfolgt zu einem legitimen Zweck, nämlich der pflichtgemäßen Erfüllung der gesetzlichen Aufgaben mit dem Ziel, die vom BMG angeordnete DEA zum Infektionsschutz durchzuführen.

(2) Die Verarbeitung ist zur Zweckerreichung auch geeignet. Die Verarbeitung im Rahmen der DEA entspricht den zweckgebundenen Vorgaben des IfSG und der Anordnungen. Die Bewertung der Eignung der DEA für die vom BMG angestrebten Zwecke ist nicht Aufgabe des RKI und ist für die vorliegende DSFA somit unerheblich.

(3) Die Verarbeitung ist zur Zweckerreichung erforderlich, wenn sie

- keine gleich geeigneten bzw. effektiven, milderen Mittel zur Erreichung des verfolgten Zwecks zur Verfügung stehen,
- wenn sich die Verarbeitung auf diejenigen Daten beschränkt, die geeignet sind, um den verfolgten Zweck zu erreichen und
- mildere Mittel nicht ersichtlich sind.

Es sind keine in gleicher Weise geeigneten, milderen Mittel ersichtlich sind. Die geplante DEA entspricht vollumfänglich den Vorgaben des IfSG und der Anordnungen, ist gleichzeitig aber gerade auf deren enge Grenzen beschränkt. .

(4) Die Verarbeitung ist angemessen, wenn im Rahmen einer Abwägung das zu schützende Rechtsgut dem beeinträchtigten Rechtsgut, in das eingriffen werden soll, überwiegt. Vorliegend kann auch die Angemessenheit bejaht werden: Auf der einen Seite stehen Leib und Leben der Öffentlichkeit als höchste Rechtsgüter, zu deren Schutz die DEA in erheblichem Maße beiträgt, insbesondere für eine spätere Kontaktverfolgung und Verhinderung der Weiterverbreitung des Coronavirus SARS-CoV-2. Auf der anderen Seite steht das Recht auf Datenschutz und eine überwiegend gesetzlich definierte, teilweise freiwillige, vorwiegend auf Kontaktdaten und Daten zur stattgefundenen Reise begrenzte Verarbeitung personenbezogener Daten. Durch die DEA werden die Gesundheitsämter in die Lage versetzt, die in der Regel 14-tägige Quarantäne effektiv zu überwachen, da sie ohne ein digitales System erst nach mehreren Tagen von Personen erfahren, die der Quarantäne-Pflicht unterliegen. Aufgrund des eng umgrenzten Zwecks der Verarbeitung sowie der kurzen Speicherfrist, ist die vorliegende Verarbeitung daher als verhältnismäßig anzusehen.

9. Rechtsgrundlagen

Die spezifischen Rechtsgrundlagen für die Datenverarbeitungen im Rahmen des Prüfgegenstandes sind den folgenden Ausführungen zu entnehmen.

9.1. Daten von sämtlichen Einreisenden

Die gesetzliche Erlaubnis zur Verarbeitung der personenbezogenen Daten durch den bloßen (freiwilligen) Besuch bzw. die bloße Nutzung der Website durch sämtliche Einreisende (auch solche aus Nicht-Risikogebieten) ergibt sich aus Art. 6 Abs. 1 lit. e DSGVO i.V.m. § 3 BDSG und den öffentlichen Aufgaben des RKI aus § 2, 4 BGA-NachfG, insbesondere zur Information der Öffentlichkeit. Wie bei jeder Websitennutzung unvermeidlich, werden in begrenztem Umfang Daten des Nutzers (hier: der einreisenden Person) erhoben. Ohne diese Daten wäre ein Websitebetrieb und die dem zugrundeliegende DEA in der Form nicht möglich.

9.2. Daten von Einreisenden aus Risikogebieten

Personen, die sich zu einem beliebigen Zeitpunkt innerhalb der letzten zehn (10) Tage vor Ihrer Einreise nach Deutschland in einem Risikogebiet aufgehalten haben, sind zur Angabe verschiedener Daten gegenüber dem zuständigen Gesundheitsamt verpflichtet. Darüber hinaus können sie weitere freiwillige Daten angeben, die den Gesundheitsämtern helfen, die Einhaltung der geltenden Regelungen zu prüfen.

Die Pflicht zur Meldung und Auskunft bei dem zuständigen Gesundheitsamt sowie zur Nutzung der vom RKI betriebenen Webanwendung Digitale Einreiseanmeldung ergibt sich aus § 36 Abs. 8, 9 IfSG und der Verordnung des BMG zum Schutz vor einreisebedingten Infektionsgefahren in Bezug auf das Coronavirus SARS-CoV-2 nach Feststellung einer epidemischen Lage von nationaler Tragweite durch den Deutschen Bundestag vom 13. Januar 2021 sowie gegebenenfalls aus den in den Bundesländern geltenden Einreisebestimmungen.

Die Kontaktdaten der einreisenden Personen werden validiert, um dem Gesundheitsamt den Kontakt zu ermöglichen und Fehler bei der Eingabe sowie Falschangaben möglichst zu verhindern. Die Rechtsgrundlage der Verarbeitung zu Validierung der Kontaktdaten der einreisenden Personen ist § 3 BDSG in Verbindung mit Art. 6 Abs. 1 lit. e DSGVO.

9.3. Rechtsgrundlage der Verarbeitung der Angaben der Betroffenen zum Vorliegen eines negativen Testnachweises sowie zum Vorliegen etwaiger Ausnahmetatbestände ist die separat von den Betroffenen erklärte Einwilligung, Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit Art. 9 Abs. 2 lit. a DSGVO. Diese Angaben sind für die Betroffenen ausdrücklich freiwillig.Übermittlung der Daten von Einreisenden aus Risikogebieten an Gesundheitsämter

Gleiches gilt für die Bereitstellung bzw. Übermittlung der personenbezogenen Daten an die für die weitere Verarbeitung zuständigen Gesundheitsämter. § 1 der Verordnung beschreibt den Datenfluss dahingehend, dass die vom RKI erhobenen Daten an die Gesundheitsämter übermittelt werden.

10. An der Datenverarbeitung Beteiligte

Die folgenden Akteure sind an der Datenverarbeitung im Rahmen des DEA unmittelbar beteiligt.

10.1. Betroffene

Betroffene Personen im datenschutzrechtlichen Sinne sind alle Personen, die die Website aufzurufen und Daten im Wege der DEA mitteilen.

10.2. Verantwortlicher

Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die Verarbeitung der personenbezogenen Datender betroffenen Personen ist das RKI. Die vorgeschaltete Abfrage nach den Aufenthaltsorten vor der Einreise zur Unterscheidung zwischen Einreisenden aus Risikogebieten und Nicht-Risikogebieten ist zentraler Bestandteil der DEA und damit der Aufgabenerfüllung. Die Verantwortlichkeit des RKI bezieht sich daher auf sämtliche im Rahmen des Prüfgegenstands verarbeiteten personenbezogenen Daten.

§ 14 Abs. 1 IfSG-E hätte insoweit nur klarstellende Funktion: „*Das Robert Koch-Institut ist der Verantwortliche im Sinne des Datenschutzrechts*“ (§ 14 Abs. 1 S. 2 IfSG-E).

10.3. Keine gemeinsame Verantwortlichkeit von RKI und Gesundheitsämtern

Eine gemeinsame Verantwortlichkeit vom RKI und den (bzw. einzelnen) zuständigen Gesundheitsämtern ist nicht ersichtlich. Beide verfolgen mit Blick auf ihre jeweiligen rechtlichen Pflichten unterschiedliche Zwecke für die Verarbeitung. Nach Ansicht der deutschen Aufsichtsbehörden muss bei verschiedenen Zwecken, die von den jeweiligen Beteiligten verfolgt werden, eine Zweckverfolgung im Rahmen dieser konkreten Datenverarbeitung nicht ohne die andere möglich ist.[4] Ein solcher Zusammenhang zwischen den Zwecken ist nicht ersichtlich. Zwar vereinfacht die Verarbeitung durch das RKI die nachfolgende Verarbeitung durch die Gesundheitsämter. Eine gegenseitige Abhängigkeit beider Zwecke folgt daraus aber nicht. Auch der Europäische Datenschutzausschuss betont, dass die Nutzung gemeinsamer Datenverarbeitungssysteme nicht automatisch zu einer gemeinsamen Verantwortlichkeit führt.[5] Zudem haben die zuständigen Gesundheitsämter keinen Einfluss auf die Festlegung der Mittel und Zwecke des DEA. Vielmehr werden die Gesundheitsämter durch das BMG zur Nutzung des DEA verpflichtet.

10.4. Auftragsverarbeiter

Bezüglich der Verarbeitung personenbezogener Daten durch die Bundesdruckerei GmbH ist sie Auftragsverarbeiter der personenbezogenen Daten i.S.d. Art. 4 Nr. 8 DSGVO und erbringt Leistungen auf Grundlage einer Vereinbarung zur Auftragsverarbeitung in Bezug auf den Service, Weiterentwicklung / Pflege und den Betrieb der DEA.

---

[4] DSK, Kurzpapier Nr. 16, Gemeinsam für die Verarbeitung Verantwortliche vom 19.03.2018, S. 2.

[5] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version1.0, adopted on 02 September 2020, S. 20.

Von der Bundesdruckerei eingesetzte Sub-Dienstleister sind Amazon Webservices, Inc., Message Mobile GmbH sowie das Bundesamt für Kartographie und Geodäsie. Mit diesen hat die Bundesdruckerei jeweils Auftragsverarbeitungsverträge abgeschlossen.

Bezüglich der Daten aus der Digitalen Einreiseanmeldung, die durch die Bundesdruckerei an die Deutsche Post E-Post Solutions GmbH übergeben werden, ist diese Auftragsverarbeiter des RKI und erbringt Leistungen ebenfalls auf Grundlage einer Vereinbarung zur Auftragsverarbeitung.

11. Wahrung der Betroffenenrechte

Zur Wahrnehmung ihrer Datenschutzrechte gem. Art. 12 ff DSGVO können sich betroffene Personen an die durch das RKI veröffentlichten Kontaktdaten richten. Darüber hinaus steht u.a. auch der direkte Kontakt zum Datenschutzbeauftragten des RKI offen.

11.1. Information des Betroffenen (Art. 12 ff. DSGVO)

Die Informationen gem. Art. 12 ff DSGVO werden den betroffenen Personen auf der Website zur Verfügung gestellt. Da das RKI als Verantwortlicher die Daten bei der betroffenen Person erhebt, richtet sich die Informationspflicht nach Art. 13 Abs. 1 DSGVO. Die Datenschutzerklärung enthält die insoweit geforderten Informationen.

11.2. Auskunftsrecht (Art. 15 DSGVO)

Da dem RKI personenbezogene Daten aufgrund der grundsätzlichen Verschlüsselung der Daten des Betroffenen nicht bekannt sind, werden Auskunftsanfragen an das zuständige Gesundheitsamt oder die Deutsche Post weitergeleitet. Soweit Daten durch das RKI als Clearing Stelle verarbeitet werden, müssen Auskunftsersuchen im Einzelfall geprüft werden.

11.3. Recht auf Berichtigung (Art. 16 DSGVO)

Die betroffenen Personen haben jederzeit die Möglichkeit, die Berichtigung ihrer personenbezogenen Daten durch das RKI zu verlangen.

Ein Recht auf Berichtigung personenbezogener Daten gegenüber dem RKI wird in der Regel nicht bestehen. Wie der EuGH festgestellt hat, ist das Recht auf Berichtigung “im Hinblick auf den Zweck zu beurteilen [...], für den die Daten erhoben wurden” (EuGH, Urt. v. 20 Dezember 2017, Rs. C-434/16, Rn. 53). Dieser Zweck besteht hier in der Übermittlung der personenbezogenen Daten an die zuständigen Gesundheitsämter, wie sie von dem Einreisenden “vor der Einreise in die Bundesrepublik” (§ 1 S. 1 der Verordnug) angegeben wurden.

Sollten im Einzelfall ein Anspruch auf Berichtigung bestehen, etwa weil Daten missbräuchlich durch Dritte eingegeben wurden, ist eine Berichtigung durch das zuständige Gesundheitsamt möglich. Die Mitarbeiter des Gesundheitsamts können Daten über das Webinterface der Bundesdruckerei berichtigen. Soweit Daten durch das RKI als Clearing Stelle verarbeitet werden, muss das Recht auf Berichtigung im Einzelfall geprüft werden.

11.4. Recht auf Löschung (Art. 17 DSGVO)

Die betroffene Person hat jederzeit die Möglichkeit, die Löschung ihrer personenbezogenen Daten zu verlangen.

Ein Recht auf Löschung personenbezogener Daten durch das RKI wird in der Regel nicht bestehen, da Zweck der Verarbeitung in der Übermittlung von personenbezogenen Daten an die zuständigen Gesundheitsämter besteht, wie sie von der einreisenden Person “vor Einreise in die Bundesrepublik” angegeben wurden.

Sollten im Einzelfall ein Löschanspruch bestehen, etwa weil Daten missbräuchlich durch Dritte eingegeben wurden oder die Einwilligung widerrufen wird, ist eine Löschung durch das zuständige Gesundheitsamt möglich. Die Mitarbeiter des Gesundheitsamts können Daten über das Webinterface der Bundesdruckerei löschen. Soweit Daten durch das RKI als Clearing Stelle verarbeitet werden, muss das Recht auf Löschung im Einzelfall geprüft werden.

11.5. Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Die betroffenen Personen haben jederzeit die Möglichkeit, die Einschränkung der Verarbeitung ihrer Daten im Einzelfall zu verlangen. Sollten im Einzelfall ein Recht auf Einschränkung der Verarbeitung bestehen, ist eine Einschränkung durch das zuständige Gesundheitsamt möglich. Die Mitarbeiter des Gesundheitsamts können Daten über das Webinterface der Bundesdruckerei löschen. Soweit Daten durch das RKI als Clearing Stelle verarbeitet werden, muss das Recht auf Einschränkung der Verarbeitung im Einzelfall geprüft werden.

11.6. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Die betroffene Person hat jederzeit die Möglichkeit, ihr Recht auf Datenübertragbarkeit geltend zu machen hinsichtlich der Verarbeitung, die auf ihrer Einwilligung beruht.

11.7. Widerspruchsrecht (Art. 21 DSGVO)

Das Recht auf Widerspruch besteht nicht. Die erhobenen personenbezogenen Daten werden weder auf Grundlage von Art. 6 Abs. 1 lit.e) DSGVO noch auf Grundlage von Art. 6 Abs. 1 lit. f) DSGVO verarbeitet.

12. Bewertung der potenziellen Risiken des Verfahrens

Im Folgenden werden gemäß Art. 35 Abs. 7 lit. c und d DSGVO die potenziellen spezifischen Risiken des Prüfgegenstands für die Rechte und Freiheiten der betroffenen Personen dargestellt, die sich aus der Art der Verarbeitung, insbesondere aus der Speicherung und Übermittlung der Daten, ergeben und die zur Bewältigung der Risiken getroffenen Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Vorgaben der DSGVO eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

12.1. Gewährleistungsziele

Erforderlich ist nach der Methodik des SDM die Sicherung des Verarbeitungsverfahrens in Bezug folgende Gewährleistungsziele:

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Transparenz
- Nichtverkettung
- Intervenierbarkeit

12.2. Risiko-Analyse

Die Dokumentation und Bewertung der identifizierten Risiken für die Rechte und Freiheiten der betroffenen Personen sowie ggf. der getroffenen Maßnahmen zur Risikobehandlung (Abhilfemaßnahmen) erfolgt in tabellarischer Form als Begleitdokument und ist Bestandteil des vorliegenden DSFA-Berichts. Die Risiko-Analyse basiert auf Zuarbeit von Dienstleistern, die eine eigene Risikobewertung für die Verarbeitung in ihrem Zuständigkeitsbereich vorgenommen haben.

12.3. Verfahren zur Risikobewertung

Die Darstellung des Risikos erfolgt anhand einer vierstufigen Risikomatrix (siehe folgende Tabelle) Die Risikomatrix berücksichtigt die Faktoren Schadenshöhe und Eintrittswahrscheinlichkeit des Risikos. Jede Farbe ist einem Risikowert nach DSGVO – geringes Risiko, (mittleres) Risiko, hohes Risiko – zugeordnet (siehe unten Tabelle 4).

Schadenshöhe					
	Sehr hoch	Hoch	Hoch	Sehr hoch	Sehr hoch
	Hoch	Hoch	Hoch	Hoch	Sehr hoch
	Mittel	Mittel	Mittel	Hoch	Hoch
	Gering	Gering	Mittel	Hoch	Hoch
		Gering	**Mittel**	**Hoch**	**Sehr hoch**
		Eintrittswahrscheinlichkeit			

Tabelle 1: Matrix zur Risikobewertung

Schadenshöhe:

Schadenshöhe	Erläuterung
Sehr hoch	Die Schadensauswirkungen können ein existenzbedrohendes, katastrophales Ausmaß erreichen.
Hoch	Die Schadensauswirkungen können beträchtlich sein.
Mittel	Die Schadensauswirkungen sind begrenzt und überschaubar
Gering	Die Schadensauswirkungen sind gering und können vernachlässigt werden.

Tabelle 2: Schadenshöhe

Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit	Erläuterung
Gering	Ereignis tritt seltener als alle 5 Jahre auf
Mittel	Ereignis tritt einmal alle 5 Jahre bis einmal in 6 Monaten auf
Hoch	Ereignis tritt einmal in 6 Monaten bis einmal im Monat auf
Sehr hoch	Ereignis tritt mehrmals im Monat auf

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
1.	Unverständnis über die Datenverarbeitung i.V.m. der „Digitalen Einreiseanmeldung“	Reisender/ Dritte	Verantwortlicher	Materielle und immaterielle Schäden	Transparenz	Mittel	Hoch	Hoch	Datenschutzinformation auf dem Reisenden-Frontend zur Information der betroffenen nach Art. 13, 14 DSGVO, die den Ansprüchen aus Art. 12 DSGVO entspricht (transparent, präzise, leicht zugänglich, verständlich, in klarer und einfacher Sprache verfasst).	Gering
2.	Reisende können das Formular nicht lesen (Fremdsprache nötig)	Reisender/ Dritte	Verantwortlicher / IT-Dienstleister	Materielle und immaterielle Schäden	Transparenz	Mittel	Hoch	Hoch	Notwendige Informationen/Formular sind in verschiedenen Sprachen vorhanden.	Gering
3.	Reisende haben kein mobiles Endgerät oder Internet	Reisender/ Dritte	Verantwortlicher / IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit	Mittel	Hoch	Hoch	Für einen Übergangszeitraum steht die analoge Aussteigekarte zur Verfügung, um den Meldepflichten bei Einreise aus einem Risikogebiet trotzdem nachkommen zu können. Die näheren Umstände werden durch den Gesetz- bzw. Verordnungs-/Anordnungsgeber bestimmt. Dem Risiko wird jedoch allgemein dadurch Rechnung getragen und soweit wie möglich abgeholfen, dass eine weitestgehende technische Kompatibilität angestrebt wird (Technologieneutralität), allgemein gebräuchliche Web-Standards (und keine native App, die eine bestimmte Systemumgebung benötigt) zum Einsatz kommt und somit z.B. auch die Nutzung in einem Internet-Café, einem Hotel, auf einem Kiosk-Terminal oder einem Gerät Dritter grundsätzlich möglich ist.	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
4.	Reisende wissen nicht, ob Herkunftsland ein Risikogebiet ist	Reisender/ Dritte	Verantwortlicher / IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Mittel	Hoch	Hoch	Abfrage vorab möglich – durch die geführte Benutzersteuerung (GUI) im Sinne eines Dialogs wird ein veralteter Informationsstand der reisenden Person(en) vermieden; regelmäßige Aktualisierung der Liste der Risikogebiete vom RKI, zukünftig mittels API. Die Daten sollen eine digitale Signatur erhalten, die nachträgliche Änderungen sichtbar macht. Weitere Informationsmöglichkeiten sind leicht auffindbar und kommuniziert (z.B. auf der Website des RKI).	Gering
5.	Reisende kennen Ansprechpartner zur Wahrnehmung der Betroffenenrechte nicht	Reisender/ Dritte	Verantwortlicher	Materielle und immaterielle Schäden	Transparenz und Intervenierbarkeit	Gering	Hoch	Hoch	Datenschutzinformation auf dem Reisenden-Frontend zur Information der Betroffenen nach Art. 13, 14 DS-GVO; klare und eindeutige Kennzeichnung der Verantwortlichkeit (z.B. Impressum, Datenschutzinformation), Bekanntgabe der Kontaktmöglichkeiten (z.B. des zuständigen Datenschutzbeauftragten), der datenschutzrechtlichen Zuständigkeit und der Möglichkeit zur Beschwerde bei der zuständigen, benannten Datenschutzaufsichtsbehörde.	Gering
6.	Reisende werden nicht über Datenschutz-Verletzungen informiert	Reisender/ Dritte	Verantwortlicher für die Datenverarbeitung	Materielle und immaterielle Schäden	Transparenz und Intervenierbarkeit	Mittel	Hoch	Hoch	Sensibilisierung der Beteiligten zu Verfahren nach Art. 33, 34 DS-GVO.	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
7.	Bewusste Falschangaben	Unbeteiligter Dritter	Reisender/ Dritter		Integrität	Sehr hoch	Hoch	Sehr hoch	Textuelle Klarstellung, dass bewusst getätigte Falschangaben einen Bußgeld-Tatbestand erfüllen können, gegenwärtig z.B. nach § 111 OWiG i.V.m. der RGebEinRTestPflV in der jeweils gültigen Fassung – analog zur papierbehafteten Aussteigekarte („Falschangaben können als Ordnungswidrigkeit mit einer Geldbuße bis zu 25.000 EURO verfolgt werden“), bei der ebenso Falschangaben möglich und per se nicht auszuschließen sind, die sich grds. erst im Dialog mit dem zuständigen Gesundheitsamt aufklären lassen werden. Das Risiko unbewusster Falschangaben (z.B. durch eine unleserliche Handschrift) wird durch die digitale Verarbeitung deutlich vermindert.	Mittel
8.	Fehlende Identifizierung und Authentisierung	Ggf. unbeteiligter Dritter	Reisender		Integrität	Hoch	Mittel	Hoch	Siehe Nr. 7.	Mittel
9.	Fehlende Validierung eingegebener Daten	Reisender/ ggf. unbeteiligter Dritter	Reisender	Materielle und immaterielle Schäden	Integrität und Richtigkeit der Daten	Mittel	Gering	Gering	Es erfolgt eine Adressvalidierung, so dass das Risiko einer unbewusst falschen Zuordnung zu einem nicht zuständigen Gesundheitsamt (z.B. über Tippfehler in der Postleitzahl) so weit wie möglich reduziert wird.	Gering
10.	Einspielen von Schadcode auf	Reisender/ Dritter	Unbeteiligter Dritter	Materielle und	Integrität	Hoch	Hoch	Hoch	Es ist nicht zu verhindern, dass Schadcode auf anderem Wege auf ein benutztes Endgerät gelangt oder	N/A

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
	dem Client-Gerät			immaterielle Schäden					sich bereits auf diesem befindet. Für die Sicherheit des Endgerätes hat der Nutzer (z.B. durch den clientseitigen Einsatz von Virenscannern) wie bei jeder anderen Verarbeitung in einer Client-Server Konstellation selber Sorge zu tragen, da ihm nicht anders abgeholfen werden kann. Daher wird dieses Risiko hier nicht bewertet. Die Gesamtheit der Sicherheitsmaßnahmen, die im IT-Sicherheitskonzept detailliert beschrieben sind, sollte jedoch eine Kompromittierung durch an der Verarbeitung beteiligte Systeme verhindern. Ferner ist die Verarbeitung bewusst als Website und nicht als App ausgestaltet. Diese kann somit z.B. im Kontext einer Sandbox oder virtuellen Maschine laufen, um das Risiko weiter zu reduzieren.	
11.	Ein Angreifer spielt maliziösen Code ein (z.B. SQL Injection, XSS etc.)	Reisender/ Dritter	Unbeteiligter Dritter	Materielle und immaterielle Schäden	Integrität	Gering	Hoch	Hoch	Gesamtheit der IT-Sicherheitsmaßnahmen in Betrieb und Entwicklung. Die Eingaben werden [redacted] sodass der Schadcode, XSS etc. nicht auf den Clients der GA ausgeführt wird.	Gering
12.	Denial-of-Service Angriffe	Reisender/ Dritter	Unbeteiligter Dritter	Materielle und immaterielle Schäden	Verfügbarkeit	Mittel	Hoch	Hoch	Bereit- und Sicherstellung einer Hochverfügbarkeitsumgebung für den Dienst.	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									Alternative besteht zumindest in der Übergangszeit die Möglichkeit, ersatzweise auf die papierbehaftete Aussteigekarte auszuweichen.	
13.	Unsichere Datenübertragung zum Backend – Schadprogramme. Die im Frontend eingegebenen Daten können nicht auf Malware gescannt werden, bevor sie in die Datenbank im Backend geschrieben werden. Ein Aufbrechen der Verbindung ist aus Vertraulichkeitsaspekten nicht gewünscht.	Reisender/ Dritter	Ggf. unbeteiligter Dritter	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Gering	Hoch	Hoch	Die Eingaben werden [redacted] geprüft, sodass der Schadcode, XSS etc. nicht auf den Clients der Gesundheitsämter ausgeführt wird.	Gering
14.	Unbefugter Zugriff auf bestehende Sessions (des Vorbenutzers bei Flughafen-Terminals)	Reisender/ Dritter	Unbeteiligte Dritte	Materielle un-d immaterielle Schäden	Vertraulichkeit und Integrität	Hoch	Hoch	Hoch	Sensibilisierung der Betroffenen durch Hinweise vor Eingabe der Daten bei Nutzung eines öffentlichen Terminals/Clients; automatisches Verwerfen der Eingabe bei längerer Untätigkeit (Timeout).	Mittel

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
15.	Fehlerhafte Übermittlung von Daten über Risikogebiete	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Gering	Mittel	Mittel	Der Abruf der Risikogebiete durch die Bundesdruckerei beim RKI soll zukünftig § 6 IFG erfolgen. Die Daten sollten dabei eine digitale Signatur beinhalten, die nachträgliche Änderungen sichtbar macht. § 6 IFG [redacted]	Gering
16.	Manipulation der Daten über Risikogebiete	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Mittel	Mittel	Mittel	Der Abruf der Risikogebiete durch die Bundesdruckerei beim RKI soll zukünftig mittels API erfolgen.	Gering
17.	Unsicherer Betrieb – Ausfall von Geräten oder Systemen	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit	Gering	Hoch	Hoch	§ 6 IFG [redacted] Betriebskonzept ist Teil des IT-Sicherheitskonzeptes.	Gering
18.	Ausfall oder Störung der Stromversorgung	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit	Gering	Hoch	Hoch	Die Geräte werden in Räumen untergebracht, die speziell für den Betrieb von (verfügbarkeitskritischen) IT-Systemen vorgesehen und ausgestattet sind (RZ-Räume bzw. spezielle IT-Technikräume). Am zentralen Standort der Bundesdruckerei ist per Sicherheitsrichtlinie für alle aktiven Netzkomponenten, die als Sicherheitsgateways fungieren, eine RZ-Unterbringung vorgeschrieben. Anschlüsse an die Spannungsversorgung mit USV- und NEA-Absicherung gehören zu den	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									Ausstattungsmerkmalen solcher Räume: Die RZ-Räume am zentralen Standort der Bundesdruckerei wurden als Trusted Site Infrastructure (TSI) vom TÜV zertifiziert. Besonders erhöhte und wirksame Maßnahmen bzgl. durchgängiger Energieversorgung sind ein Prüfschwerpunkt der TSI-Kriterienkataloge. Als IT-Systeme mit sehr hohem Schutzbedarf bzgl. Verfügbarkeit erhalten alle Firewalls entsprechend ausgelegte Anschlüsse an die Spannungsversorgung.	
19.	Unsicherer Betrieb – Fehlfunktion von Geräten oder Systemen	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Gering	Hoch	Hoch	§ 6 IFG [redacted] verkürzte Backup-Zyklen kann das Risiko minimieren.	Gering
20.	Daten werden nicht gemäß der definierten Löschfristen gelöscht	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Datenminimierung	Gering	Mittel	Mittel	Automatisierte Löschung erfolgt fristbasiert und ohne Notwendigkeit manueller Schritte. Klar definierte Löschintervalle ermöglichen Sicherstellung ordnungsgemäßer Funktion bereits in der Entwicklung.	Gering
21.	Betroffenenrechte können technisch nicht erfüllt werden	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Transparenz und Intervenierbarkeit	Gering	Hoch	Hoch	Soweit das RKI personenbezogene Daten in der Funktion als Clearing-Stelle verarbeitet, können die Anträge von betroffenen Personen zur Wahrnehmung ihrer Betroffenenrechte umgesetzt werden. Im Übrigen besteht durch das RKI kein Zugriff auf die Daten. Die zuständigen Gesundheitsämter	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									können Betroffenenrechte über das ihnen zur Verfügung stehende Web-Interface umsetzen. Die Gesundheitsämter werden über die Anträge zur Wahrnehmung von Betroffenenrechten durch das RKI in Kenntnis gesetzt.	
22.	Zugriff der Gesundheitsämter auf Daten, die nicht innerhalb ihres Zuständigkeitsbereiches liegen	Reisender/ Dritter	IT-Dienstleister und Gesundheitsamts	Materielle und immaterielle Schäden	Vertraulichkeit	Gering	Mittel	Mittel	[redacted]	Gering
23.	Unbefugter Zugriff auf IT-Systeme	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit	Mittel	Hoch	Hoch	Die Gesamtheit der mehrschichtigen Maßnahmen der Bundesdruckerei zur Gewährleistung der Informationssicherheit (defense-in-depth) dient der Sicherstellung der Schutzziele. Diese sind im Detail im IT-Sicherheitskonzept dargestellt, werden fortlaufend mit Blick auf den aktuellen Stand der Technik	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									evaluiert und angepasst sowie fortgeschrieben.	
24.	Unzureichende Dimensionierung	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit	Mittel	Hoch	Hoch	§ 6 IFG [redacted] Ausreichende Dimensionierung, SPOF-Vermeidung, Fallback/Redundanz und Loadbalancing können, soweit technisch möglich, die Verfügbarkeit gewährleisten und insofern als mitigierende Maßnahmen einen entscheidenden Beitrag leisten. Leistungsspitzen sind jedoch gänzlich nie auszuschließen.	Mittel
25.	Unbefugter Zutritt zu Datenverarbeitungsanlagen	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Mittel	Hoch	Hoch	Zutrittsregelungen als Teil des ganzheitlichen Sicherheitskonzepts. Zutritts-, Zugangs- und Zugriffskontrolle auf den Kreis des notwendigen Betriebs- und Wartungspersonals beschränkt wie im IT-Sicherheitskonzept beschrieben.	Gering
26.	Unbefugter Zugriff auf Daten in der Datenbank	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Gering	Hoch	Hoch	§ 6 IFG [redacted] Zugriff auf die Datenbankserver sowie die Datenbank selbst ist auf	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									den absolut notwendigen Kreis beschränkt. Zusätzlich liegen die personenbezogenen Daten in der Datenbank ausschließlich in verschlüsselter Form vor.	
27.	Verlust der Daten durch Löschen oder Zerstörung	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit und Wiederherstellbarkeit	Gering	Hoch	Hoch	Im Rahmen der Verfügbarkeitskontrolle kommen eine Vielzahl an Einzelmaßnahmen ergänzend zur Geltung, die im IT-Sicherheitskonzept beschrieben sind. Dies beinhaltet, erschöpft sich aber nicht in: Viren- und Malwareschutz, organistorischen Maßnahmen (Notfallhandbuch, ständig besetze Notfallrufnummer, Notfallübungen) und technischen Vorkehrungen (regelmäßige Backups, sichere Aufbewahrung in separaten Brandabschnitten, ausreichend dimensionierte IT-Infrastruktur, etc.).	Gering
28.	Verlust der Daten durch Löschen/Verlust der Datenbank-Schlüssel für Entschlüsselung	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit/Wiederherstellbarkeit	Gering	Hoch	Hoch	§ 6 IFG [redacted] Für das Key Management kommen Standard-Prozesse der Bundesdruckerei weitestgehend zum Einsatz. § 6 IFG	Mittel

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									§ 6 IFG [redacted]	
29.	Unsichere Datenübertragung	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Gering	Hoch	Hoch	Verbindung zu entfernten Systemen erfolgt ausschließlich verschlüsselt ([redacted] § 6 IFG [redacted]	Gering
30.	Unbefugter Zugriff auf Daten der Datenbank (das Backend-System)	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Gering	Hoch	Hoch	Durch eine Zugriffskontrolle nach dem „Need-To-Know“-Prinzip (Minimalberechtigung), kann eine Verarbeitung von Daten durch berechtigte Mitarbeiter*innen gewährleistet werden. Siehe Nr. 26.	Gering
31.	Verlust der Daten durch Löschen oder Zerstörung	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Gering	Hoch	Hoch	Integritätskontrollen korrespondierend zum Schutzbedarf eingerichtet. Dies betrifft sämtliche Ebenen im Rahmen eines ganzheitlichen Sicherheitskonzeptes (z.B. die regelmäßige Überprüfung von Benutzerrechten sowie den Fortbestand derer Notwendigkeit durch die Abteilung ID-Management), aber auch technische Maßnahmen. Durch die Verschlüsselung wird ebenfalls eine Integritätsprüfung umgesetzt, durch die Integritätsverletzungen sofort erkannt würden ([redacted] § 6 IFG [redacted]	Gering
32.	Manipulation von Hard- und Software - Eine Veränderung der Daten, die im CDN ausgelagert	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Gering	Hoch	Hoch	§ [redacted] 6 [redacted] IFG [redacted]	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
	worden sind, könnten zu Funktionsfehlern der Applikation auf den Clients der Einreisenden führen. Des Weiteren kann mit der Veränderung des JavaScripts eine Umleitung der Daten erfolgen und die Verschlüsselung verändert werden.								§ 6 IFG [redacted]	
33.	Keine ausreichende Trennung der Daten	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Trennungsgebot	Gering	Mittel	Mittel	Implementierte Mandantentrennung stellt sicher, dass die Daten jeweils nur von den berechtigen Mitarbeitern der zuständigen Gesundheitsämter gelesen werden können. § 6 IFG [redacted]	Gering
34.	Kein Zugang/Zugriff für die Gesundheitsämter. Die Anbindung der Gesundheitsä	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Verfügbarkeit	Hoch	Hoch	Hoch	Zur Minimierung des Risikos können folgende Maßnahmen dienen: 1. Einsatz einheitlicher VPN-Endpunkte bei den Gesundheitsämtern	Mittel

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
	mter ist nicht einheitlich geregelt. Inkompatibilität der VPN Gateways der GÄ mit dem VPN Endpunkt der Bundesdruckerei können gegeben sein, da jedes Gesundheitsamt ein eigenes VPN-Gateway verwenden kann.								§ [redacted] 6 [redacted] 3. Beratung der Gesundheitsämter und deren EDV-Dienstleistern durch Support-Mitarbeiter der Bundesdruckerei (soweit gewünscht).	
35.	Unbefugte Modifikation der Datensätze	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Gering	Hoch	Hoch	Inhaltsverschlüsselung stellt sicher, dass eine Datenveränderung durch nicht autorisierte Nutzer sofort auffallen würde. Mandantentrennung und Benutzerverwaltung der Fachanwender § 6 IFG stellen sicher, dass nur berechtigte User hierauf Zugriff haben und somit eine unbefugte Modifikation unterbunden wird.	Gering
36.	Denial-of-Service Angriffe	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Mittel	Hoch	Hoch	Bereit- und Sicherstellung einer Hochverfügbarkeitsumgebung für den Dienst. (siehe Nr. 12). Anders als in der Reisenden-Perspektive besteht hier jedoch nicht die Möglichkeit auf ein analoges Äquivalent auszuweichen.	Mittel

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
37.	Ein Angreifer spielt maliziösen Code ein (Web-Zugriff)	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Integrität	Gering	Hoch	Hoch	Gesamtheit der IT-Sicherheitsmaßnahmen in Betrieb und Entwicklung. (siehe Nr. 11). § [redacted]	Gering
38.	Unbefugter Zugang/Zugriff auf Systeme/Daten	Reisender/ Dritter	IT-Dienstleister, ggf. unbeteiligte Dritte	Materielle und immaterielle Schäden	Integrität und Vertraulichkeit	Gering	Hoch	Hoch	Analog zu Nr. 26 und 30 erfolgt die Absicherung der Daten und Systeme.	Gering
39.	Unbefugter Zugriff auf Daten bei Datenübertragung an Gesundheitsämter	Reisender/ Dritter	IT-Dienstleister; ggf. unbeteiligte Dritte	Materielle und immaterielle Schäden	Integrität und Vertraulichkeit	Gering	Hoch	Hoch	Analog zu Nr. 26 und 30 erfolg die Absicherung der Datenübermittlung. § 6 IFG [redacted]	Gering
40.	Keine Behandlung von Datenschutzverletzungen	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Transparenz und Intervenierbarkeit	Gering	Hoch	Hoch	Sensibilisierung; etablierte Prozesse zu Data Breaches der Bundesdruckerei stellen ordnungsgemäße und fristgerechte Behandlung sicher.	Gering
41.	Keine organisatorischen Mittel zur Erfüllung von Betroffenenrechte (Auskunft, Korrektur, Löschung etc.)	Reisender/ Dritter	IT-Dienstleister	Materielle und immaterielle Schäden	Transparenz und Intervenierbarkeit	Gering	Hoch	Hoch	Soweit das RKI personenbezogene Daten in der Funktion als Clearing-Stelle verarbeitet, können die Anträge von betroffenen Personen zur Wahrnehmung ihrer Betroffenenrechte umgesetzt werden. Im Übrigen besteht durch das RKI kein Zugriff auf die Daten. Die zuständigen Gesundheitsämter können Betroffenenrechte über das	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									ihnen zur Verfügung stehende Web-Interface umsetzen. Die Gesundheitsämter werden über die Anträge zur Wahrnehmung von Betroffenenrechten durch das RKI in Kenntnis gesetzt.	
42.	Unsicherer Betrieb – Ausfall von Geräten oder Systemen	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Verfügbarkeit	Gering	Hoch	Hoch	Einsatz von Firewall, Virenschutz, Notfallhandbuch, ständig besetzte Natfallrufnummer, Notfallübungen, regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt), USV, virtualisierte Infrastruktur, ausreichend dimensionierte Infrastruktur.	Gering
43.	Ausfall oder Störung der Stromversorgung	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Verfügbarkeit	Gering	Hoch	Hoch	Einsatz von Firewall, Virenschutz, Notfallhandbuch, ständig besetzte Natfallrufnummer, Notfallübungen, regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt), USV, virtualisierte Infrastruktur, ausreichend dimensionierte Infrastruktur.	Gering
44.	Unsicherer Betrieb – Fehlfunktion von Geräten oder Systemen	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Verfügbarkeit und Integrität	Gering	Hoch	Hoch	Einsatz von Firewall, Virenschutz, Notfallhandbuch, ständig besetzte Natfallrufnummer, Notfallübungen, regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt), USV, virtualisierte Infrastruktur, ausreichend dimensionierte Infrastruktur.	Gering
45.	Daten werden nicht gemäß der definierten Löschfristen gelöscht.	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Datenminimierung	Gering	Mittel	Mittel	Die Daten werden nach Ablauf von 14 Tagen gelöscht werden.	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
46.	Betroffenenrechte können technisch nicht erfüllt werden.	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Transparenz und Intervenierbarkeit	Gering	Hoch	Hoch	Soweit das RKI personenbezogene Daten in der Funktion als Clearing-Stelle verarbeitet, können die Anträge von betroffenen Personen zur Wahrnehmung ihrer Betroffenenrechte umgesetzt werden. Im Übrigen besteht durch das RKI kein Zugriff auf die Daten. Die Post wird über Anträge beim RKI in Kenntnis gesetzt.	Gering
47.	Unbefugte Verkettung der Daten	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Nichtverkettung	Mittel	Hoch	Hoch	Es erfolgt eine logische Trennung von Systemen, getrennte Ablage in verschlüsselten Ordnern. Ein sachgerechtes Rollen- und Berechtigungskonzept ist umgesetzt, um zu verhindern, dass Mitarbeiter der Deutsche Post die Daten mit anderen Daten zusammenführen.	Gering
48.	Unbefugter Zutritt zu Datenverarbeitungsanlagen	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Vertraulichkeit und Integrität	Mittel	Hoch	Hoch	Es gibt elektronische Zutrittskontrallen an allen Standorten sowie zusätzlich innerhalb der Standorte für verschiedene Schutzzonen, Zutritt für Dienstleister nur nach Authentisierung, Verpflichtung und Begleitung durch Mitarbeiter der Deutsche Post, Einbruchmeldeanlagen sowie optische Zutrittskontrollen, Erteilung von Zutrittsgenehmigungen nur durch Leitungskräfte über eine entsprechende Berechtigungsmatrix, Verpflichtung auf Vertraulichkeit	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
49.	Manipulation von Hard- und Software	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Integrität	Mittel	Hoch	Hoch	Ablage in verschlüsselten Dateien, Einsatz von Firewall, Virenschutz, Notfallhandbuch, ständig besetzte Notfallrufnummer, Notfallübungen, regelmäßige Backups,, Zutrittskontrollen	Gering
50.	Kein Zugang/Zugriff für die Gesundheitsämter	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Verfügbarkeit	Gering	Mittel	Mittel	Die folgenden Maßnahmen kommen zum Einsatz: Firewall, Virenschutz, Notfallhandbuch, ständig besetzte Notfallrufnummer, Notfallübungen, regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt), USV, virtualisierte Infrastruktur, ausreichend dimensionierte Infrastruktur.	Gering
51.	Verlust der Daten durch Löschen/Verlust der Datenbank-Schlüssel für Entschlüsselung	Reisender/ Dritter	Deutsche Post	Materielle und immaterielle Schäden	Verfügbarkeit/Integrität	Mittel	Hoch	Hoch	Die folgenden Maßnahmen kommen zum Einsatz: Firewall, Virenschutz, Notfallhandbuch, ständig besetzte Notfallrufnummer, Notfallübungen, regelmäßige Backups, sichere Aufbewahrung (separater Brandabschnitt), USV, virtualisierte Infrastruktur, ausreichend dimensionierte Infrastruktur.	Gering
52.	Keine ausreichende Trennung der Daten	Reisende/ Dritte	Deutsche Post	Materielle und immaterielle Schäden	Trennungsgebot	Mittel	Hoch	Hoch	Es erfolgt eine logische Trennung von Systemen, getrennte Ablage in verschlüsselten Ordnern.	Gering
53.	Identifizierung anhand der eingetragenen Anschrift	Reisende	BKG/Dritte	Immaterielle Schäden	Vertraulichkeit	Gering	Gering	Gering	Die Anschrift (ohne Hausnummer) ist nur in sehr seltenen Fällen geeignet, eine Person zu identifizieren. Die an das BKG übermittelten Daten enthalten außer der Anschrift keine die reisende Person identifizierende Information. Die Anschrift wird durch das BKG nicht gespeichert.	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
54.	Verlust/Missbrauch der durch das RKI im Rahmen des DOI erhobenen Kontaktdaten (E-Mail/Telefonnummer)	Reisende	Dritte	Immaterielle Schäden	Vertraulichkeit	Gering	Gering	Gering	Das RKI/Dienstleister erhalten außer der vom Reisenden § 6 IFG [redacted] gewählten Kontaktdaten keine unverschlüsselten Informationen. Die Daten werden nicht dauerhaft gespeichert.	
55.	DEA-Dienst kann aufgrund von Latenzen im außereuropäischen Ausland nicht oder nur eingeschränkt genutzt werden. Rechtspflicht zur Abgabe einer Einreiseanmeldung kann nicht nachgekommen werden.	Reisender/ Dritter	-	Materielle und immaterielle Schäden	Verfügbarkeit	Mittel	Hoch	Hoch	§ 6 IFG [redacted]	Gering
56.	Weltweite Systemverfügbarkeit von 99,8% mit bis zu 600.000 Reisendenanmeldungen pro Tag kann nicht gewährleistet werden.	Reisender/ Dritter	-	Materielle und immaterielle Schäden	Verfügbarkeit	Hoch	Hoch	Hoch	§ 6 IFG [redacted]	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
	Rechtspflicht zur Abgabe einer Einreiseanmeldung kann nicht nachgekommen werden									
57.	Drittlandsübermittlung: Reisendendaten werden von Dritten (bspw. Geheimdiensten) abgegriffen bzw. vom CDN-Anbieter AWS gesetzlich/rechtlich angefordert Einem Angreifer könnte hierdurch bekannt werden, dass eine ggf. bestimmbare Person (nicht jede Person ist zweifelsohne einer IP-Adresse zuzuordnen, sofern	Reisender/ Dritter	Dritte/ Geheimdienste/ Regierungen	Materielle und immaterielle Schäden	Vertraulichkeit	Hoch	Hoch	Hoch	- § 6 IFG [redacted] - Abschluss von Standardvertragsklauseln - § 6 IFG [redacted]	Gering

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
	Netzkomponenten wie Proxies, entsprechende NAT-Devices oder Gateways zum Einsatz kommen) plant nach Deutschland zu reisen, da sie die Website einreiseanmeldung.de aufgerufen hat.								§ 6 IFG [redacted] Unter Risikoaspekten muss zusammenfassend davon ausgegangen werden, dass es sich im Zweifelsfall um einen unsicheren Drittstaat handelt, in dem ausreichende Garantien für ein angemessenes Schutzniveau nicht vorliegen. Dieser Aspekt war darüber hinaus ein wesentliches Kriterium bei der Auswahl des Anbieters (vertraglich definierte hohe bis sehr hohe Anforderungen an die Verfügbarkeit des Dienstes; verbunden hiermit die Notwendig einer hohen Resilienz	

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									gegen (D)DOS-Angriffe, einer geringen Latenz, da die Anwendung auf dem Reisenden-Device ausgeführt wird und dorthin übertragen werden muss und der expliziten Anforderung auch eine steigende Nutzerzahl bei Einhaltung der Schutzziele abdecken zu können). § 6 IFG [redacted]	

Nr	Beschreibung des Szenarios - Gefahr	Betroffene Person	Angreifer	möglicher Schaden	Betroffene Gewährleistungsziele	Eintritts-wahrscheinlichkeit	Schadens-höhe	Gesamt-risiko	Maßnahmen	Rest-risiko
									§ 6 IFG [redacted]	
58.	Fehlende Freiwilligkeit der eingeholten Einwilligung	Reisender	Verantwortlicher	Immaterieller Schaden	Rechtmäßigkeit	Mittel	Gering	Mittel	Auf die Freiwilligkeit der betroffenen Angaben (negativer Coronavirus Test und Ausnahmtetatbestände) wird in den Überschriften deutlich hingewiesen.	Mittel
59.	Intransparenz der eingeholten Einwilligung	Reisender	Verantwortlicher	Immaterieller Schaden	Rechtmäßigkeit, Transparenz	Mittel	Gering	Mittel	Die Einwilligung benennt die betroffenen Datenkategorien ausdrücklich. Die Zwecke werden ebenfalls beschrieben. Die Einwilligung muss aktiv erklärt werden, sofern der	Mittel

13. **Gesamtrisiko**

Unter Berücksichtigung der geplanten technischen und organisatorischen Maßnahmen wird das datenschutzrechtliche Risiko in Bezug auf den Prüfgegenstand wie folgt bewertet (maßgeblich ist der höchste festgestellte Risikowert in Bezug auf das jeweilige Gewährleistungsziel):

Es besteht kein hohes, sondern lediglich ein geringes bis mittleres Restrisiko für die Rechte und Freiheiten natürlicher Personen. Das identifizierte Restrisiko, welches bei dem geplanten Verfahren zur digitalen Einreise-Anmeldung vom RKI zu verantworten ist, kann durch die geplanten Maßnahmen auf ein angemessenen Maß reduziert werden. Diese Bewertung beruht insbesondere auf folgenden Erwägungen:

- Es wurde berücksichtigt, dass es sich um ein zeitkritisches Verfahren handelt, das in Teilen nur eine Zwischenlösung sein (z.B. mit Blick auf die Einbindung der Deutschen Post), aber aus dem Grund implementiert werden soll, um die Restrisiken der Vorgängerlösung zur Erfassung von Einreisendendaten (sog. mit Blick auf die Einbindung der Deutsche Post), aber aus dem Grund implementiert werden soll, um die Restrisiken der Vorgängerlösung zur Erfassung von Einreisendendaten (sog. Scanlösung) schnellstmöglich nochmals zu reduzieren.
- Es wurde ferner berücksichtigt, dass im Rahmen der digitalen Einreise-Anmeldung keine Gesundheits- oder andere sensiblen Daten im Sinne von Art. 9 DSGVO verarbeitet werden, so dass die Erforderlichkeit von Maßnahmen zur Gewährleistung eines ausreichenden Schutzniveaus entsprechend angepasst werden können.

In Bezug auf die einzelnen Gewährleistungsziele sind die Risiken wie folgt zu bewerten:

Nr.	SDM-Gewährleistungsziel	Geringes Risiko	(normales) Risiko	Hohes Risiko
1	Datenminimierung	x		
2	Verfügbarkeit		x	
3	Integrität		x	
4	Vertraulichkeit		x	
5	Nichtverkettung	x		
6	Transparenz	x		
7	Intervenierbarkeit	x		

14. Stellungnahme des Datenschutzbeauftragten

Die Vorgehensweise zum Vorhaben wurde mit den Projektteilnehmern sowie der Datenschutzaufsichtsbehörde (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit - BfDI) diskutiert, die Anregungen aufgegriffen und von der Projektleitung entsprechend umgesetzt.

Es gibt keine datenschutzrechtlichen Bedenken gegen die Durchführung des Vorhabens in der beschriebenen Weise.

Da im Rahmen des Vorhabens personenbezogene Daten verarbeitet werden, müssen Angaben im Verzeichnis der Verarbeitungstätigkeiten des RKI hinterlegt werden.

15. Abschließendes Ergebnis

Unter Berücksichtigung der Stellungnahme des Datenschutzbeauftragten kann die DSFA mit folgendem Ergebnis abgeschlossen werden:

15.1. Bewertung

Das Gremium der DSFA kommt zu folgendem Ergebnis:

☒ Die DSFA, einschließlich Risikoanalyse, verlief **positiv**. Die Verarbeitungstätigkeit geht unter Umsetzung der technisch-organisatorischen Maßnahmen in die Nutzung über.

☐ Die DSFA, einschließlich Risikoanalyse, verlief **negativ**. Die Verarbeitungstätigkeit geht nicht in die Nutzung über. Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung sind notwendig.

☐ Die DSFA, einschließlich Risikoanalyse, verlief **negativ**. Die Verarbeitungstätigkeit geht nicht in die Nutzung über. Eine Nach-Folgenabschätzung und erneute Maßnahmenfestlegung ist nicht möglich.

15.2. Entscheidung bzgl. Information Aufsichtsbehörde

Die Einbeziehung der Aufsichtsbehörde

☐ ist auf Grund des Ergebnisses der DSFA und der Tatsache, dass die Verarbeitungstätigkeit trotz des Ergebnisses durchgeführt werden soll, notwendig.

☐ ist nicht notwendig, da die Verarbeitungstätigkeit auf Grund des Ergebnisses der DSFA nicht durchgeführt wird.

☒ ist nicht notwendig, weil kein hohes Restrisiko identifiziert wurde oder ausreichende Maßnahmen zur Eindämmung des Restrisikos getroffen wurden.

16. **Nächster Prüfungstermin**

Die DSFA muss wiederholt bzw. aktualisiert werden, sofern und sobald sich Begleitumstände, die eine erneute DSFA erforderlich erscheinen lassen, ändern.

Davon ist zwingend auszugehen, sofern und sobald mindestens einer der folgenden Fälle eintritt:

- Änderung der Rechtslage, insbesondere durch neue BMG-Verordnung betreffend die Einreiseanmeldung oder entsprechende Gesetzesvorhaben
- Sobald erkannt wird, dass die der Risikoanalyse zugrunde gelegten TOM und Abhilfenahmen wahrscheinlich nicht oder nicht vollständig umgesetzt werden können