Datenschutz-Folgenabschätzung

für das Register der SoHO-Einrichtungen und das Frequenzregister gemäß SoHO-Gesetz (SoHOG) und Verordnung (EU) 2024/1938 (SoHO-Verordnung).

SYSTEMATISCHE BESCHREIBUNG
der geplanten Verarbeitungsvorgänge, Zwecke sowie berechtigten Interessen.

Die Beschreibung hat nach ErwGr. 90 sowie Art. 35 Abs. 7 lit. a und Abs. 8 DSGVO sowie den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) der Artikel-29-Datenschutzgruppe (WP 248) die Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", zu enthalten.

Art der Verarbeitung: (ErwGr. 90 DSGVO)	Die vorliegende Datenschutz-Folgeabschätzung behandelt zwei Register, die aufgrund der SoHO-Verordnung und des SoHOG eingerichtet werden. Es handelt sich um das: • Register der SoHO-Einrichtungen gemäß § 55 SoHOG und Art. 16 Abs. 1 SoHO-Verordnung („Einrichtungsregister") sowie das • Register zur Prüfung der Spendefrequenz gemäß § 56 SoHOG und Art. 53 Abs. 1 lit. i iVm Abs. 3 SoHO-Verordnung („Frequenzregister") Die Verarbeitung erfolgt jeweils elektronisch im Rahmen einer Webanwendung. Das Bundesamt für Sicherheit im Gesundheitswesen ist datenschutzrechtlich Verantwortlicher des Einrichtungsregisters, während der für das Gesundheitswesen zuständige Bundesminister datenschutzrechtlich Verantwortlicher des Frequenzregisters ist. Aus Gründen der Datensicherheit gemäß Art. 32 DSGVO unterbleibt an dieser Stelle eine genaue Beschreibung der technischen Umsetzung, um potentielle Angreifer/innen nicht mit wertvollen Informationen über potentielle Schwachstellen (Art-29-Datenschutzgruppe, WP 248 Rev.01, 8) zu versorgen. **Die Anforderung „Beschreibung der Art der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Umfang der Verarbeitung: (ErwGr. 90 DSGVO)	Einrichtungsregister: Betroffen sind alle in Österreich tätigen SoHO-Einrichtungen sowie deren verantwortliche Personen (Art. 36 der Verordnung [EU] 2024/1938 und § 8 SoHOG) sowie benannte Personen (§ 9 SoHOG). Darüber hinaus werden Daten von Einrichtungen erfasst, die SoHO autolog im Rahmen kosmetischer oder medizinischer Behandlungen beim Menschen verwenden (§ 60 Abs. 5 SoHOG). Erfasst werden insbesondere Daten zur Identifikation der (SoHO-)Einrichtungen und die Identitäts- und Kontaktdaten der verantwortlichen Person (der benannten Person). Die Verarbeitung erfolgt dauerhaft (laufende Aktualisierung bei Änderungen). Die geografische Ausdehnung umfasst das österreichische Bundesgebiet. Die Daten werden soweit erforderlich an die SoHO-Plattform der EU übermittelt (siehe Art. 17 Abs. 2 der Verordnung [EU] 2024/1938). Frequenzregister: Betroffen sind alle lebenden SoHO-Spender, die Vollblut oder Blutbestandteile spenden. Die Zahl der betroffenen Personen wird mehrere zehntausend Personen pro Jahr umfassen.

	Erfasst werden insbesondere Daten zur Spende, also Datum und entnommene Menge. Nähere medizinische Angaben, etwa zu Ausschlussgründen, werden nicht verarbeitet. Die Verarbeitung erfolgt dauerhaft und fortlaufend. Die geografische Ausdehnung umfasst SoHO-Einrichtungen im österreichischen Bundesgebiet. **Die Anforderung „Beschreibung des Umfangs der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Kontext der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21)	Einrichtungsregister: Die Verarbeitung erfolgt im Kontext der Art. 6 Abs. 1 lit. c und e DSGVO. Die rechtliche Verpflichtung, das Einrichtungsregister zu betreiben, ergibt sich unmittelbar aus der SoHO-Verordnung und dem SoHOG. Bereits bisher wurden durch das Bundesamt für Sicherheit im Gesundheitswesen entsprechende Einrichtungen gemäß dem BSG 1999 und dem GSG erfasst. Zukünftig werden auch andere SoHO-Einrichtungen erfasst, etwa im Bereich der Humanmilch oder humanen Mikrobiota. Frequenzregister: Die Verarbeitung erfolgt im Kontext des Art. 9 Abs. 2 lit. i DSGVO (öffentlichen Interesses im Bereich der öffentlichen Gesundheit). Die Daten werden zum Schutz der Gesundheit der lebenden SoHO-Spender erhoben. Ein entsprechendes nationales Register besteht bislang nicht. **Die Anforderung „Beschreibung des Kontexts der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Zweck der Verarbeitung: (Art. 35 Abs. 7 lit. a DSGVO)	Einrichtungsregister: Zweck der Verarbeitung ist, alle in Österreich tätigen SoHO-Einrichtungen zu erfassen und behördliche Aufsicht und Kontrolle gemäß den Anforderungen der SoHO-Verordnung und des SoHOG zu ermöglichen. Die verarbeiteten Daten dienen insbesondere der Durchführung von Inspektionen, der Kommunikation mit den SoHO-Einrichtungen und der Veröffentlichung auf der SoHO-Plattform der EU. Eine Weiterverwendung für andere Zwecke ist nicht vorgesehen. Frequenzregister: Die Verarbeitung dient dem Gesundheitsschutz lebender SoHO-Spender. Diese sollen nicht häufiger spenden, als dies in den einschlägigen technischen Leitlinien vorgesehen ist. Die verarbeiteten Daten dienen ausschließlich dem Gesundheitsschutz der lebenden SoHO-Spender. Eine Verwendung für andere Zwecke ist ausgeschlossen, wobei eine anonyme, statistische Auswertung der Daten erfolgen kann. **Die Anforderung „Beschreibung des Zwecks der Verarbeitung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Personenbezogene Daten: (WP 248 Rev.01, 21 und 28)	Es werden folgende personenbezogene Daten (Datenkategorien) verarbeitet: Einrichtungsregister: • Daten gemäß Art. 35 Abs. 3 SoHO-Verordnung, • Daten gemäß § 7 Abs. 2 zur verantwortlichen Person (Art. 36 der Verordnung [EU] 2024/1938) und zur benannten Person (§ 9), und • Daten der Meldung gemäß § 60 Abs. 5. Frequenzregister: • bereichsspezifisches Personenkennzeichen Gesundheit (bPK-GH) und Geschlecht der lebenden SoHO-Spender,

	• Datumsangaben zu Spenden von SoHO einschließlich der Art der SoHO (Vollblut oder Blutbestandteile) und gegebenenfalls der Menge, • Information, ob von der vorgesehenen Spendefrequenz aufgrund einer ärztlich begründeten Ausnahme abgegangen wurde, und • Angaben zur SoHO-Einrichtung Für die Erstellung des bPK-GH dürfen außerdem Name und Geburtsdatum der lebenden SoHO-Spender verarbeitet werden. Zur Identitätsfeststellung erfolgt ein Abgleich mit dem zentralen Melderegister. Nähere Informationen zum Gesundheitszustand der lebenden SoHO-Spender werden im Sinne der Datenminimierung **nicht** erfasst. **Die Anforderung „Beschreibung der personenbezogenen Daten" ist aufgrund der gesetzlichen Determinierung in der SoHO-Verordnung und dem SoHOG als erfüllt anzusehen.**
Empfänger/innen: (Art-29-Datenschutzgruppe, WP 248, 21)	Einrichtungsregister: Das Bundesamt für Sicherheit im Gesundheitswesen verarbeitet die Daten im Register. Der für das Gesundheitswesen zuständige Bundesminister kann die vorhandenen Daten ebenfalls verarbeiten, soweit dies für den Betrieb des Frequenzregisters und des Versorgungssicherheitsregisters notwendig ist. Die Daten sind gemäß Art. 16 Abs. 2 SoHO-Verordnung außerdem an die SoHO-Plattform der EU zu übermitteln. Frequenzregister: Die Daten werden vom für das Gesundheitswesen zuständigen Bundesminister verarbeitet. Der Zugriff von SoHO-Einrichtungen ist auf das unbedingt erforderliche Ausmaß beschränkt: Es kann stets nur auf jene Daten zugegriffen werden, die zur Prüfung der Spendefrequenz im Einzelfall notwendig sind. Als Ergebnis der Abfrage wird nur die Zulässigkeit bzw. Unzulässigkeit der SoHO-Spende angezeigt. **Die Anforderung „Beschreibung der Empfänger/innen" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Speicherdauer: (Art-29-Datenschutzgruppe, WP 248, 21)	Einrichtungsregister: Da die Datenverarbeitung im Einrichtungsregister dauerhaft angelegt ist, sind die verarbeiteten Daten erst zu löschen, wenn diese nicht mehr für die Vollziehung der SoHO-Verordnung oder des SoHOG erforderlich sind. In diesem Sinne wird auch in der Durchführungsverordnung (EU) 2025/1467 der Kommission vom 18. Juli 2025 mit Durchführungsbestimmungen zur SoHO-Verordnung des Europäischen Parlaments und des Rates hinsichtlich der technischen Spezifikationen für die SoHO-Plattform der EU für den Informationsaustausch über zur Verwendung beim Menschen bestimmte Substanzen menschlichen Ursprungs, ABl. Nr. L 1467 vom 21.07.2025 S. 1, die Speicherfrist der Daten der verantwortlichen Person festgelegt: Gemäß Anhang II Z 1 sind die Daten der verantwortlichen Person solange in der SoHO-Plattform der EU zu speichern, als diese die Funktion für die SoHO-Einrichtung innehat. Eine darüberhinausgehende feste Löschfrist, etwa für SoHO-Einrichtungen nach Betriebseinstellungen, erscheint nicht angemessen. Auch nach Betriebseinstellung können für diese SoHO-Einrichtung zugelassene SoHO-Präparate noch im Umlauf sein. Die im Zusammenhang mit der registrierten Einrichtung vorhandenen Informationen können daher weiterhin relevant sein.

	Frequenzregister: Die Daten sind spätestens nach Ablauf von zehn Jahren ab der letzten SoHO-Spende zu löschen. **Die Anforderung „Beschreibung der Speicherdauer“ ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Funktionelle Beschreibung der Verarbeitung: (Art. 35 Abs. 7 lit. a DSGVO)	Einrichtungsregister: • Registrierung von SoHO-Einrichtungen: SoHO-Einrichtungen haben sich gemäß Art. 35 SoHO-Verordnung zu registrieren, bevor sie SoHO-Tätigkeiten aufnehmen. Dazu haben die nationalen SoHO-Behörden ein Register für das jeweilige Hoheitsgebiet zur Verfügung zu stellen, soweit im Sinne des Art. 16 Abs. 2 SoHO-Verordnung nicht die SoHO-Plattform der EU genutzt wird. Das vom Bundesamt für Sicherheit im Gesundheitswesen betriebene Einrichtungsregister ermöglicht einen gesamtheitlichen Überblick aller im Bundesgebiet tätigen SoHO-Einrichtungen. Diese haben sich über eine Applikation zu registrieren, die vom Bundesamt für Sicherheit im Gesundheitswesen auf dessen Homepage zur Verfügung gestellt wird. Die SoHO-Einrichtungen registrieren sich dabei über die eService-Applikation des Bundesamtes für Sicherheit im Gesundheitswesen, die zentral auf der Homepage unter „eservices.basg.gv.at“ zur Verfügung gestellt wird. Diese Plattform wird von der Österreichischen Agentur für Gesundheit und Ernährungssicherheit GmbH (AGES) für das Bundesamt für Sicherheit im Gesundheitswesen betrieben und ist bereits für eine Vielzahl bestehender Meldewege (u.a. nach AMG, TAMG, MPG, BSG, GSG) im produktiven Einsatz. Die SoHO-Einrichtungsregistrierung wird als zusätzlicher Fachprozess in diese bestehende Infrastruktur integriert. Erstregistrierung der Organisation: Jede SoHO-Einrichtung registriert sich einmalig über die zentrale Registrierungsapplikation (kundenregistrierung.basg.gv.at) als Organisation. Die erstmals registrierende Person erhält dabei eine Administrator-Berechtigung für die Organisation. Voraussetzung für die Freischaltung ist die Vorlage einer Vollmacht der Geschäftsführung („Letter of Authorisation", LoA) sowie eines aktuellen Firmenbuchauszuges (oder eines entsprechenden ausländischen Äquivalents). Über die Administrator-Funktion können weitere Benutzer der Organisation angelegt und mit fachlichen Berechtigungen ausgestattet werden. Authentifizierung: Die Anmeldung am eService-Portal erfolgt nach dem aktuellen Stand der Technik mittels Zwei-Faktor-Authentifizierung (2FA). Neben Benutzername und Passwort ist ein zeitlich befristetes Einmalpasswort einzugeben, das durch eine standardkonforme Authenticator-Anwendung (TOTP) auf einem mobilen Endgerät des Benutzers erzeugt wird. Fachliche Datenerfassung: Nach erfolgter Anmeldung steht den berechtigten Benutzern der SoHO-Einrichtung im eService-Portal ein gesonderter Fachprozess für die Registrierung zur Verfügung. Erfasst werden die in der SoHO-Verordnung sowie in § 7 Abs. 2 SoHOG genannten Daten der Einrichtung, der verantwortlichen Person (Art. 36 der Verordnung [EU] 2024/1938 und § 8 SoHOG) und der benannten Person (§ 9 SoHOG). Änderungen an den Stammdaten der Einrichtung sind durch die Einrichtung selbst über dieselbe Applikation laufend zu pflegen.

	Persistenz und Protokollierung im Bundesamt für Sicherheit im Gesundheitswesen: Die im Rahmen der Registrierung und Meldung erhobenen Daten werden in einer zugangsgeschützten Datenbank im Verantwortungsbereich des Bundesamtes für Sicherheit im Gesundheitswesen persistiert. Sämtliche Verarbeitungsvorgänge (Eintragungen, Änderungen, Abfragen, Übermittlungen und Löschungen) werden revisionssicher protokolliert. • Meldung von Einrichtungen, die autologe SoHO im Rahmen einer kosmetischen oder medizinischen Behandlung verwenden. Werden autologe SoHO vor ihrer Verwendung beim Menschen weder verarbeitet, noch gelagert, sind sie vom Anwendungsbereich der SoHO-Verordnung ausgenommen (Art. 2 Abs. 5 der Verordnung [EU] 2024/1938). Einrichtungen, die autologe SoHO im Rahmen einer kosmetischen oder medizinischen Behandlung ohne Verarbeitung oder Lagerungen verwenden, werden sich aus diesem Grund in der Regel nicht als SoHO-Einrichtung registrieren müssen. Mit der verpflichtenden Meldung gemäß § 60 Abs. 5 SoHOG soll ungeachtet dessen ein Überblick über diese Einrichtungen geschaffen werden, um dem Bundesamt für Sicherheit im Gesundheitswesen eine nähere Prüfung der vorgenommenen Tätigkeiten zu ermöglichen. Die Einrichtungen haben sich über die Applikation auf der Homepage des Bundesamtes für Sicherheit im Gesundheitswesen zu melden, wobei die Meldung technisch der Registrierung von SoHO-Einrichtungen nachgebildet ist (siehe auch die Ausführungen oben). <u>Frequenzregister:</u> In Fällen, in denen SoHO wiederholt gespendet werden können und eine häufige Spende die Gesundheit des lebenden SoHO-Spenders negativ beeinflussen kann, haben SoHO-Einrichtungen gemäß Art. 53 Abs. 1 lit. i iVm Abs. 3 SoHO-Verordnung anhand von Registern zu überprüfen, dass lebende SoHO-Spender nicht zu häufig spenden. Dazu haben sie lebende SoHO-Spender (soweit vorhanden) in nationalen Registern zu registrieren. Vor diesem Hintergrund haben SoHO-Einrichtungen lebende SoHO-Spender von Vollblut und Blutbestandteilen im Frequenzregister zu registrieren (siehe auch § 39 Abs. 3 SoHOG). Anhand des Frequenzregisters haben SoHO-Einrichtungen zu prüfen, ob lebende SoHO-Spender (Art. 3 Z 7 der Verordnung [EU] 2024/1938) häufiger spenden, als in den einschlägigen technischen Leitlinien vorgesehen. Vor jeder Spende muss abgefragt werden, ob die zulässige Spendefrequenz eingehalten wird. Wird die zulässige Frequenz überschritten, ist für die SoHO-Einrichtung eine entsprechende Meldung ersichtlich. Um die Identifizierung der Spender zu ermöglichen, wird das zentrale Melderegister zur Ermittlung eines bPK-GH herangezogen. Der für das Gesundheitswesen zuständige Bundesminister hat SoHO-Einrichtungen den Zugriff auf das Frequenzregister über eine elektronische Schnittstelle zu gewähren. Die einzelnen lebenden SoHO-Spender können auf ihre Daten unter Verwendung der ID-Austria durch eine Bürgeranwendung zugreifen. **Die Anforderung „Funktionelle Beschreibung der Verarbeitung“ ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Beschreibung der Anlagen (Hard- und Software bzw. sonstige Infrastruktur): (Art-29-Datenschutzgruppe, WP 248, 21)	Da die konkret zum Einsatz kommende Hard- und Software nicht gesetzlich geregelt werden, ist an dieser Stelle die Beschreibung der Maßnahmen gemäß Art. 25 DSGVO maßgebend und auch ausreichend.

	Einrichtungsregister: Das Bundesamt für Sicherheit im Gesundheitswesen hat als datenschutzrechtlich Verantwortlicher sicherzustellen, dass jeder Zugriff auf das Einrichtungsregister nur unter Nachweis der eindeutigen Identität (§ 2 Z 2 E-GovG) und der Authentizität (§ 2 Z 5 E-GovG) möglich ist. Es muss sicherstellen, dass geeignete, dem jeweiligen Stand der Technik entsprechende Vorkehrungen getroffen werden, um eine Vernichtung, Veränderung oder Abfrage der Daten des Registers durch unberechtigte Benutzer oder Systeme zu verhindern, und dass alle durchgeführten Verwendungsvorgänge, wie insbesondere Eintragungen, Änderungen, Abfragen und Übermittlungen, protokolliert werden. Frequenzregister: Der für das Gesundheitswesen zuständige Bundesminister hat als datenschutzrechtlich Verantwortlicher sicherzustellen, dass jeder Zugriff auf das Frequenzregister nur unter Nachweis der eindeutigen Identität (§ 2 Z 2 E-GovG) und der Authentizität (§ 2 Z 5 E-GovG) möglich ist. Er muss sicherstellen, dass geeignete, dem jeweiligen Stand der Technik entsprechende Vorkehrungen getroffen werden, um eine Vernichtung, Veränderung oder Abfrage der Daten des Registers durch unberechtigte Benutzer oder Systeme zu verhindern, und dass alle durchgeführten Verwendungsvorgänge, wie insbesondere Eintragungen, Änderungen, Abfragen und Übermittlungen, protokolliert werden. **Die Anforderung „Beschreibung der Anlagen (Hard- und Software bzw. sonstige Infrastruktur)“ ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
Eingehaltene, gemäß Art. 40 DSGVO genehmigte Verhaltensregeln (Art-29-Datenschutzgruppe, WP 248, 21)	Das Instrument der Verhaltensregeln ist für Behörden und öffentliche Stellen nicht anwendbar (Art. 41 Abs. 6 DSGVO bzw. mwN *Schweinoch/Will* in *Ehmann/Selmayr* (Hrsg.), DSGVO[2] Art. 40 Rn. 10). **Die Anforderung „Beschreibung der eingehaltenen, gemäß Art 40 DSGVO genehmigten Verhaltensregeln“ ist aufgrund der angeführten Beschreibung als erfüllbar anzusehen.**
BEWERTUNG der Notwendigkeit und Verhältnismäßigkeit	
Festgelegter, eindeutiger, legitimer Zweck: (Art. 5 Abs. 1 lit. b DSGVO)	Daten im Einrichtungsregister dürfen zu den in Art. 16 SoHO-Verordnung festgelegten Zwecken verarbeitet werden. Diese Zwecke sind von Art. 6 DSGVO bzw. Art. 9 Abs. 2 lit. i DSGVO („öffentliches Interesse im Bereich der öffentlichen Gesundheit“) gedeckt (siehe auch ErwGr. 76 der Verordnung [EU)]2024/1938). Die festgelegten Zwecke (Errichtung und Betrieb eines nationalen Registers der SoHO-Einrichtungen) dienen erheblichen öffentlichen Interessen gemäß Art. 9 Abs. 1 lit. i DSGVO, indem sie dem übergeordneten Ziel der SoHO-Verordnung dienen: der Sicherstellung eines hohen Schutzniveaus für zur Verwendung beim Menschen bestimmte SoHO. Daten im Frequenzregister dürfen zu den in § 56 Abs. 1 und 3 SoHOG sowie Art. 53 Abs. 1 lit. i SoHO-Verordnung definierten Zwecken verarbeitet werden. Mit der Prüfung, ob fachliche Vorgaben der Spendefrequenz im Sinne der Gesundheit lebender SoHO-Spender eingehalten werden, werden Ziele im öffentlichen Interesse im Bereich der öffentlichen Gesundheit (Art. 9 Abs. 2 lit. i DSGVO) verfolgt.

	Die Anforderung „Festgelegter, eindeutiger, legitimer Zweck“ ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.
Rechtmäßigkeit der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 6 DSGVO)	Für beide Register: Die vorgesehenen Datenverarbeitungen sind rechtmäßig, da sie Deckung im SoHOG (insbesondere §§ 55 und 56), der SoHO-Verordnung und der DSGVO finden sowie der Erfüllung der oben dargelegten öffentlichen Interessen dienen. Die Rechtmäßigkeit der Verarbeitung von Daten, die keine Gesundheitsdaten sind, ergibt sich aus Art. 6 Abs. 1 lit. c iVm Abs. 2 und 3 DSGVO („Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt“). **Die Anforderung „Rechtmäßigkeit der Verarbeitung“ ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Angemessenheit und Erheblichkeit der Verarbeitung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO)	Einrichtungsregister: Die Verarbeitung ist angemessen, weil kein gelinderes Mittel zur Erreichung des Zwecks (Überblick über alle tätigen SoHO-Einrichtungen) besteht. Darüber hinaus erfüllt die Datenverarbeitung ein erhebliches öffentliches Interesse im Bereich der öffentlichen Gesundheit. Die Verarbeitung ist auf das erforderliche Maß eingeschränkt. Gemäß Art. 16 Abs. 1 SoHO-Verordnung ist ein Register von SoHO-Einrichtungen im jeweiligen Hoheitsgebiet zu führen, wobei grundsätzlich die SoHO-Plattform der EU zu verwenden ist. Art. 16 Abs. 2 SoHO-Verordnung erlaubt den Mitgliedstaaten aber alternativ, ein eigenes nationales Register einzurichten. Die SoHO-Plattform der EU ist derzeit nur in englischer Sprache verfügbar, weswegen vor dem Hintergrund des Art. 8 B-VG eine nationale Lösung in deutscher Sprache verfassungsrechtlich geboten ist. Die zu verarbeitenden Daten sind für die verfolgten legitimen Zwecke erheblich, da ohne eine entsprechende elektronische Datenverarbeitung die oben dargelegten erheblichen öffentlichen Interessen nicht oder nicht in einem ausreichenden Ausmaß gewährleistet werden können. Frequenzregister: Die Verarbeitung ist angemessen, da ohne nationales Frequenzregister nicht umfassend und einrichtungsübergreifend geprüft werden kann, ob Spendefrequenzen eingehalten werden. Mit dem Frequenzregister werden Daten einzelner SoHO-Einrichtungen miteinander vernetzt, wodurch die Vorgaben zur Spendefrequenz nicht durch Spenden in verschiedenen SoHO-Einrichtungen umgangen werden können. Die verarbeiteten Daten sind auf das erforderliche Ausmaß beschränkt und für die Verfolgung des Zwecks (Gesundheitsschutz der lebenden SoHO-Spender) erheblich. Ohne die entsprechenden Datenverarbeitungen kann der Schutz lebender SoHO-Spender nicht im gleichen Ausmaß gewährleistet werden. Die von Art. 9 Abs. 2 lit. i DSGVO geforderten angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person werden unten unter „Abhilfemaßnahmen“ dargestellt. **Die Anforderung „Angemessenheit und Erheblichkeit der Verarbeitung“ ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Beschränktheit der Verarbeitung auf das notwendige Maß: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. c DSGVO)	Es werden nur jene Daten verarbeitet, die für die Erreichung des Zwecks unbedingt erforderlich sind. Im Einrichtungsregister werden Daten natürlicher Personen nur in ihrer Rolle als verantwortliche Person (Art. 36 der Verordnung [EU] 2024/1938 und § 8 SoHOG) oder als benannte Person (§ 9) verarbeitet.

	Daneben werden Daten von Einrichtungen gemäß § 60 Abs. 5 verarbeitet, wobei hierbei auch Daten natürlicher Personen erfasst werden können (etwa selbständig tätige Ärzte). Im Frequenzregister werden Name und Geburtsdatum der lebenden SoHO-Spender ausschließlich verarbeitet, um das bPK-GH zu generieren. Weitere Datenverarbeitungen erfolgen nur mittels bPK-GH. Ansonsten werden Angaben zu den relevanten erfolgten SoHO-Spenden, zu einer ärztlich begründeten Ausnahme von der Spendefrequenz und zur SoHO-Einrichtung erfasst. Andere Gesundheitsdaten – etwa zu vorliegenden Ausschlussgründen – werden im Frequenzregister nicht verarbeitet. **Die Anforderung „Beschränktheit der Verarbeitung auf das notwendige Maß" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen.**
Speicherbegrenzung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 5 Abs. 1 lit. e DSGVO)	Für das Einrichtungsregister wird keine feste Speicherfrist vorgesehen. Es wird stattdessen eine Löschverpflichtung für den Fall angeordnet, dass die verarbeiteten Daten nicht mehr erforderlich sind. Dies steht im Einklang mit den in EU-Rechtsakten festgelegten Speicherfristen für die Datenverarbeitung zur verantwortlichen Person in der SoHO-Plattform der EU (siehe Anhang II Z 1 der Durchführungsverordnung [EU] 2025/1467). Die personenbezogenen Daten im Frequenzregister sind spätestens nach Ablauf von zehn Jahren ab der letzten Eintragung zu löschen. Durch die explizite Begrenzung auf einen Zeitraum von zehn Jahren wird eine überschießende Aufbewahrung der Daten verhindert. Gleichzeitig sollen SoHO-Spender auch noch längere Zeit nach der zuletzt erfolgten Spende die sie betreffenden Informationen einsehen können. **Die Anforderung „Speicherbegrenzung" ist aufgrund der angeführten Beschreibung als erfüllt anzusehen, weil Maßnahmen zur Begrenzung der Speicherdauer gesetzlich vorgesehen sind.**
Information der betroffenen Personen bei Erhebung: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 13 DSGVO)	Betroffene Personen sind im Einrichtungsregister die verantwortlichen Personen und benannten Personen, die registriert werden. Diese werden im Rahmen der Registrierung der SoHO-Einrichtung über die Datenverarbeitung informiert. Einrichtungen gemäß § 60 Abs. 5 SoHOG haben sich unmittelbar selbst zu registrieren. Betroffene Personen bezüglich des Frequenzregisters sind lebende SoHO-Spender, die Vollblut oder Blutbestandteile spenden. Diese sollen im Rahmen der Spende über die Datenverarbeitungen informiert werden. Datenschutzerklärungen liegen für die Datenverarbeitungen in beiden Registern noch nicht vor. **Die Anforderung „Information der betroffenen Personen bei Erhebung" ist aufgrund der grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.**
Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werden: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 14 DSGVO)	Werden Informationen nicht bei den zuvor genannten Personen selbst erhoben, besteht ein Informationsrecht gemäß Art. 14 DSGVO. Für beide Register ist davon auszugehen, dass die betroffenen Personen von der Datenverarbeitung informiert werden. **Die Anforderung „Information der betroffenen Personen, wenn die Daten nicht bei ihnen erhoben werde" ist aufgrund der**

	grundsätzlichen Machbarkeit einer solchen Information als erfüllbar anzusehen.
Auskunftsrecht der betroffenen Personen: (Art-29-Datenschutzgruppe, WP 248, 21 iVm Art. 15 DSGVO)	Das gemäß Art. 15 DSGVO bestehende Auskunftsrecht wird nicht beschränkt. Betroffenen Personen des Frequenzregisters können die vom für das Gesundheitswesen zuständigen Bundesminister zur Verfügung gestellte Web-Applikation nutzen, um auf die sie betreffenden Daten zuzugreifen. Der Zugriff erfolgt mittels qualifizierter Signatur (ID Austria). **Die Anforderung „Auskunftsrecht der betroffenen Personen" ist aufgrund der Beschreibung und – im Fall des Frequenzregisters – der Zugriffsmöglichkeit mittels Web-Applikation als erfüllt anzusehen.**
Recht auf Datenübertragbarkeit: (Art. 20 DSGVO)	Das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO besteht nicht, da die Datenverarbeitung weder aufgrund einer Einwilligung (Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO) noch aufgrund eines Vertrages (Art. 6 Abs. 1 lit. b DSGVO) erfolgt. **Die Anforderung „Recht auf Datenübertragbarkeit" ist aufgrund der Beschreibung und vor dem Hintergrund der einschlägigen Rechtsgrundlagen als erfüllt anzusehen.**
Auftragsverarbeiter/innen: (Art. 28 DSGVO)	Allfällige Auftragsverarbeitervereinbarungen wären im Einklang mit der DSGVO (insbesondere Art. 28 DSGVO) abzuschließen. **Die Anforderung „Bewertung des Verhältnisses Auftragsverarbeiter/innen" ist aufgrund der grundsätzlichen Umsetzbarkeit als erfüllbar anzusehen.**
Schutzmaßnahmen bei der Übermittlung in Drittländer: (Kapitel V DSGVO)	Eine Übermittlung in Drittländer ist nicht vorgesehen. Es sind daher keine spezifischen Schutzmaßnahmen vorgesehen. **Die Anforderung „Bewertung der Schutzmaßnahmen bei der Übermittlung in Drittländer" ist aufgrund der nicht vorgesehenen Übermittlung in Drittländer als erfüllt anzusehen.**
Vorherige Konsultation: (Art. 36 und ErwGr. 96 DSGVO)	Eine vorherige Konsultation ist nicht erforderlich, da die in Aussicht gestellten Datenverarbeitungen kein hohes Risiko zur Folge haben. **Die Anforderung „Bewertung der vorherigen Konsultation" ist aufgrund der nicht erforderlichen Konsultation als erfüllt anzusehen.**
RISIKEN	
Physische, materielle oder immaterielle Schäden: (ErwGr. 90 iVm 85 DSGVO)	Für das Einrichtungsregister besteht prinzipiell ein Risiko für physische, materielle oder immaterielle Schäden („Data Breach"), dieses ist jedoch als gering einzuschätzen. Die verarbeiteten Daten sind überwiegend organisationsbezogen. Ein Schaden für natürliche Personen durch unbefugte Offenlegung der Kontaktdaten und Daten zur Qualifikation der verantwortlichen Person und benannten Person ist möglich, aber von geringer Schwere. Für das Frequenzregister besteht prinzipiell ebenfalls ein Risiko für physische, materielle oder immaterielle Schäden, dieses ist jedoch ebenfalls als gering einzuschätzen; dies insbesondere, da keine sensiblen Gesundheitsdaten (wie Ausschlussgründe) verarbeitet werden.

	Im Übrigen wird das Risiko durch die angeordneten Datensicherheitsmaßnahmen (siehe Abhilfemaßnahmen) angemessen mitigiert. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten.**
Verlust der Kontrolle über personenbezogene Daten: (ErwGr. 90 iVm 85 DSGVO)	Bei einem Data Breach (siehe den vorherigen Punkt) geraten Daten in unberechtigte Hände. Diese Gefahr wird jedoch durch die angeordneten Datensicherheitsmaßnahmen (siehe Abhilfemaßnahmen) mitigiert. Bei zu weitreichenden Zugriffsrechten könnten missbräuchliche Zugriffe nicht ausgeschlossen werden. Diese Gefahr wird durch ein striktes Zugangskonzept sowie die Protokollierung aller Zugriffe (siehe Abhilfemaßnahmen) im Einklang mit dem Stand der Technik gesenkt. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen ebenfalls als eingeschränkt zu bewerten.**
Diskriminierung: (ErwGr. 90 iVm 85 DSGVO)	Die Gefahr einer Diskriminierung ist für beide Register als gering einzustufen. Insbesondere lassen die im Frequenzregister verarbeiteten Daten keine Rückschlüsse auf das Vorliegen von Ausschlussgründen (wie etwa übertragbaren Krankheiten) zu. Diese Risiken werden durch die jeweiligen Abhilfemaßnahmen (striktes Zugangskonzept) mitigiert. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten**.
Identitätsdiebstahl oder -betrug: (ErwGr. 90 iVm 85 DSGVO)	Theoretisch ist es denkbar, dass sich Unbefugte Zugriff auf die in den Registern vorhandenen Daten verschaffen. Im Einrichtungsregister sind neben Namen und Kontaktdaten auch Daten zur Qualifikation der verantwortlichen und benannten Person vorhanden. Daher ist das Risiko eines Identitätsdiebstahls als mittel einzustufen. Insbesondere für den Bereich des Frequenzregisters würde Zugriff auf einen Datensatz personenbezogener Daten eines großen Personenkreises bestehen. Die vorhandenen Daten könnten missbraucht (z.B. Identitätsdiebstahl), verkauft oder veröffentlicht werden. Da Name und Geburtsdatum der betroffenen Personen nur zur Bildung des bPK-GH verwendet werden dürfen, ist das diesbezügliche Risiko aber als gering einzustufen. Das Risiko lässt sich für beide Register durch die getroffenen Abhilfemaßnahmen gemessen am Stand der Technik angemessen mitigieren. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen ebenfalls als eingeschränkt zu bewerten**.
Finanzielle Verluste: (ErwGr. 90 iVm 85 DSGVO)	Finanzielle Verluste können sich als Folge der oben geschilderten Szenarien zu Erpressungsversuchen und Identitätsdiebstahl ergeben. Dieses Risiko ist aber im Hinblick auf die vergleichsweise geringe Sensibilität der Daten als gering einzustufen und wird ebenfalls durch die stringenten Abwehrmaßnahmen mitigiert. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten.**
Rufschädigung: (ErwGr. 90 iVm 85 DSGVO)	Das entsprechende Risiko ist als gering einzuschätzen. Die Veröffentlichung von Kontaktangaben und Unterlagen zur

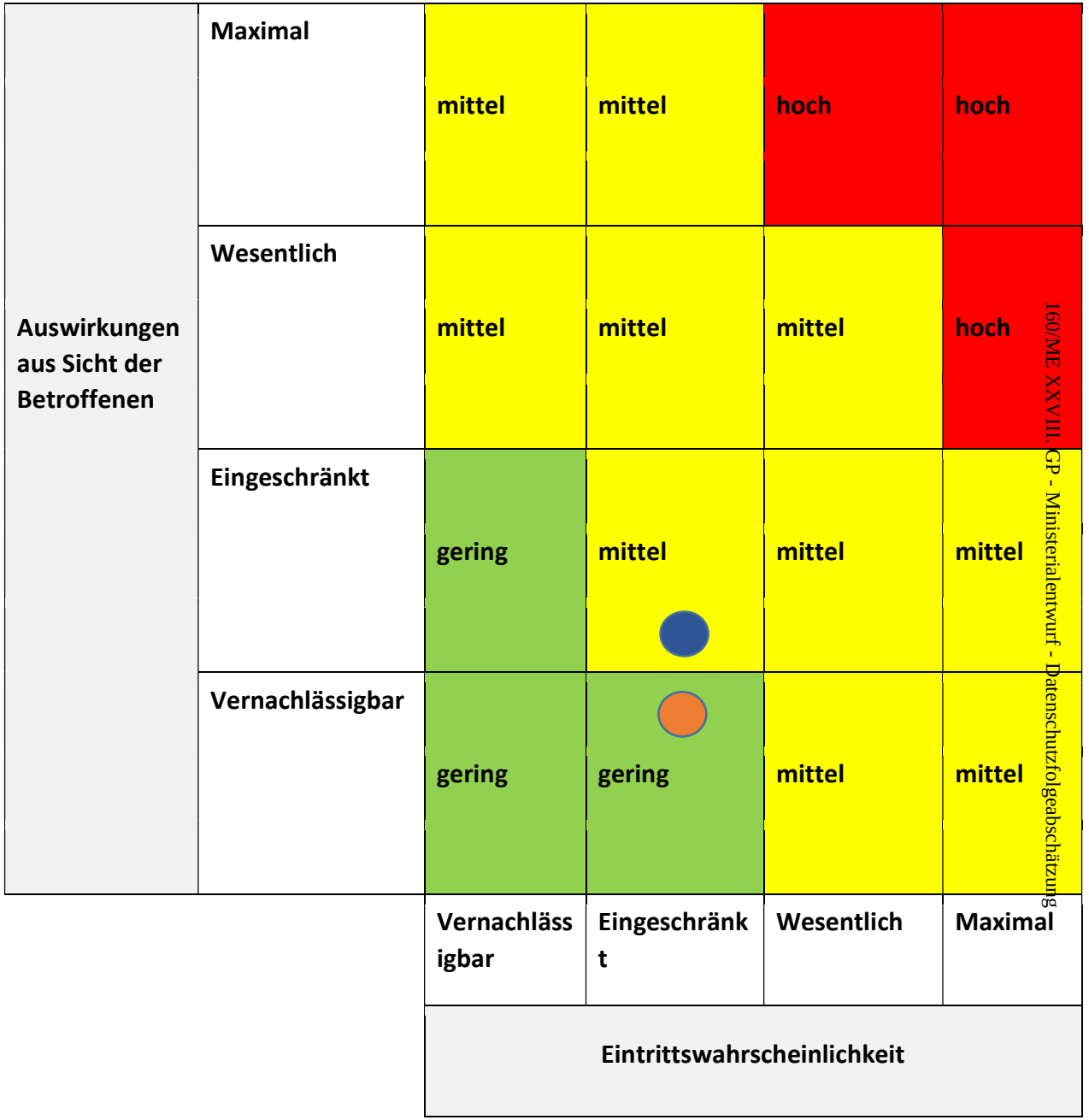
	Qualifizierung ist in aller Regel nicht rufschädigend (Einrichtungsregister). Dies gilt auch für den Umstand, dass man Vollblut bzw. Blutbestandteile spendet (Frequenzregister). Auch dieses Risiko wird im Übrigen durch die getroffenen Abhilfemaßnahmen mitigiert. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten.**
Verlust der Vertraulichkeit bei Berufsgeheimnissen: (ErwGr. 90 iVm 85 DSGVO)	Einrichtungsregister: Es besteht aufgrund der zu verarbeitenden Daten kein bzw. ein vernachlässigbares Risiko. Die an der Untersuchung und Aufklärung von SoHO-Spendern beteiligten Personen unterliegen Berufsgeheimnissen (z.B. § 54 Abs. 1 ÄrzteG) und/oder gesetzlichen Verschwiegenheitsverpflichtungen. Die relevanten Daten werden allerdings nicht im Frequenzregister verarbeitet, so dass auch diesbezüglich kein relevantes Risiko besteht. Im Übrigen lassen sich diese Risiken aufgrund der getroffenen Abhilfemaßnahmen mitigieren. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten.**
Unbefugte Aufhebung der Pseudonymisierung: (ErwGr. 90 iVm 85 DSGVO)	Eine Pseudonymiserung von personenbezogenen Daten findet im Frequenzregister mit Verwendung des bPK-GH statt. Die Aufhebung der Pseudonymisierung mittels bPK-GH durch eine unbefugte Person (intern wie extern) könnte zwar grundsätzlich erfolgen. Für eine derartige Wiederherstellung eines direkten Personenbezugs wäre jedoch umfangreiches Zusatzwissen in der Form von verschiedenen Daten notwendig. Darüber hinaus wäre die Wiederherstellung mit erheblichem Zeitaufwand verbunden. Das Risiko ist daher als äußerst gering einzuschätzen und setzt darüber hinaus strafbares Verhalten voraus. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten.**
Erhebliche wirtschaftliche oder gesellschaftliche Nachteile: (ErwGr. 90 iVm 85 DSGVO)	Erhebliche wirtschaftliche oder gesellschaftliche Nachteile sind unwahrscheinlich, können sich allenfalls aber als Folge der oben unter Punkt „Finanzielle Verluste“ geschilderten Szenarien ergeben. Aufgrund der getroffenen Abhilfemaßnahmen lassen sich diese Risiken mitigieren. **Die Eintrittswahrscheinlichkeit ist als eingeschränkt, die Auswirkungen als vernachlässigbar zu bewerten.**
ABHILFEMASSNAHMEN *Als Maßnahmen, Garantien und Verfahren zur Eindämmung von Risiken werden insbesondere in den ErwGr. 28, 78 und 83 DSGVO genannt:*	
Minimierung der Verarbeitung personenbezogener Daten: (ErwGr. 78 DSGVO)	Frequenzregister: Es werden bereichsspezifische Personenkennzeichen (§ 9 E-GovG) eingesetzt, die nur in Teilbereichen des täglichen Lebens gelten und somit einen wesentlich höheren Schutz, insbesondere gegen erhebliche wirtschaftliche oder gesellschaftliche Nachteile, bieten. Zudem werden im Einrichtungsregister und im Frequenzregister nur die für die Erreichung der Zwecke absolut erforderlichen Daten verarbeitet.

Schnellstmögliche Pseudonymisierung personenbezogener Daten (ErwGr. 28 und 78 DSGVO):	Im Einrichtungsregister ist keine Pseudonymisierung von Daten vorgesehen. Frequenzregister: Der schnellstmöglichen Pseudonymisierung personenbezogener Daten wird durch die Verwendung des bPK-Systems nach den Bestimmungen des E-GovG Rechnung getragen.
Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten (ErwGr. 78 DSGVO)	Für beide Register: Durch die Publikation des SoHOG im Bundesgesetzblatt sowie der parlamentarischen Materialien im Zuge des Gesetzgebungsprozesses können die Hintergründe für die zulässige Verarbeitung personenbezogener Daten von der Öffentlichkeit kostenlos nachvollzogen werden. Darüber hinaus wurde die SoHO-Verordnung im Amtsblatt der EU veröffentlicht, wobei zuvor ein Entwurf (COM [2022] 338 final) veröffentlicht wurde. Zu diesem Entwurf hat der Europäische Datenschutzbeauftragte eine Stellungnahme abgegeben (ABl. C 450 vom 28.11.2022, S 7).
Datensicherheitsmaßnahmen: (ErwGr. 78 und 83 DSGVO)	**Technische Maßnahmen:** • **Secure Coding Standards**: Es ist sicherzustellen, dass bei der Entwicklung von Quellcode für das gegenständliche IT-Verfahren anerkannte Secure Coding Standards nach dem aktuellen Stand der Technik eingehalten werden. Die Entwicklung von Quellcode für das gegenständliche IT-Verfahren erfolgt auf Grundlage von Secure Coding Standards. • **Quellcode-Verwaltung**: Die Verwaltung des entwickelten Quellcodes für das gegenständliche IT-Verfahren erfolgt mittels Quellcodeverwaltungssystem. Durch die Versionierungsfunktion ist sichergestellt, dass jederzeit ein bestimmter Versionsstand rekonstruiert werden kann. Zudem bietet das Werkzeug einen benutzerspezifischen Zugriffsschutz. Der Zugriff auf den Quellcode ist ausschließlich durch berechtigte Softwareentwickler des Projektteams möglich. • **Einschränkung von Drittkomponenten**: Im Falle eines Einsatzes ist sichergestellt, dass für das IT-Verfahren ausschließlich Drittkomponenten, wie z.B. Programm-Bibliotheken, eingesetzt werden, die aus vertrauenswürdigen Quellen bezogen, (mittels Virenscannern) auf Schadsoftware geprüft und entsprechend lizenziert wurden. • **Prüf- und Validierungsverfahren**: Die zu entwickelnde Software unterstützt durch den Einsatz von entsprechenden Vorgehensweisen und Standardmethoden folgende Validierungsverfahren: Plausibilitäts- und Syntaxprüfung von Eingaben und Ausgaben / Formatprüfung von Eingaben / Berechtigungs- und Zugriffskonzept / Prüfsummen und Kontroll-Summen / Steuerung und Kontrolle der Abfolge von Verarbeitungen. • **Rollen- und Rechtekonzept:** Es wird ein Rollen- und Rechtekonzept erstellt, das die vorgesehenen Rollen und Berechtigungsstufen bzw. -ebenen (z.B. Lesen, Schreiben, Ausführen) zwischen Objekten (z.B. Informationen und Daten) und Subjekten (z.B. Personen, Systemen) definiert. • **Authentifizierung und Autorisierung:** Ein geeignetes Authentifizierungs- und Autorisierungsverfahren ist umzusetzen, um ausschließlich autorisierte Zugriffe auf Basis einer eindeutigen Kennung sicherzustellen. Bei der Festlegung der erforderlichen Authentifizierungsmethode und -stärke (Ein-Faktor-Authentifizierung oder Zwei-Faktor-Authentifizierung) sind die geltenden Rechtsvorschriften und E-Government-Konventionen einzuhalten.

	• **Timeout-Funktion**: Es ist eine Timeout-Funktion umzusetzen, die sicherstellt, dass bestehende Sessions nach einem festgelegten Zeitlimit geschlossen und Zugriffe bis zu einer neuerlichen Anmeldung verhindert werden. • **Netzwerksicherheit**: Das gegenständliche IT-Verfahren wird auf Basis der im Rahmen des existierenden ISDS-Prozesses erarbeiteten Schutzbedarfsfeststellung sowie abgeleiteter Risiken und daraus folgenden Risikomanagement- und Sicherheitsmaßnahmen und gemäß den Vorgaben des Netzwerksegmentierungskonzeptes des Rechenzentrums Gesundheit netzwerktechnisch abgesichert entwickelt und betrieben werden. Dabei wird durchgehend auf die Etablierung eines angemessenen, risikoadäquaten Sicherheitsniveaus geachtet. • **Systemtrennung**: Das gegenständliche IT-Verfahren wird über verschiedene Umgebungen verfügen (z.B. Produktiv-, eine Test- und eine Entwicklungsumgebung.) Alle Umgebungen sind logisch voneinander getrennt. Ein Datenaustausch zwischen den Umgebungen ist, mit Ausnahme der fachlichen/technischen Notwendigkeit nicht möglich. • **Systemhärtung:** Es wird eine geeignete Systemhärtung der zum Betrieb des IT-Verfahrens erforderlichen IT-Systeme, einschließlich aller Anwendungen, Betriebssysteme, Datenbanken, Speichersysteme und Netzwerkkomponenten vorgenommen werden. Die Systemhärtung umfasst die Sicherstellung eines möglichst hohen Schutzprofils durch eine entsprechende Konfiguration der Sicherheitsparameter sowie die Entfernung bzw. Deaktivierung von nicht zwingend notwendigen Programmteilen, Funktionen und Diensten, um die potenzielle Angriffsfläche so weit als möglich zu minimieren. • **Schadsoftwareerkennung und -abwehr**: Im gegenständlichen IT-Verfahren werden geeignete Virenschutzverfahren festgelegt und umgesetzt, welche die Erkennung, Entfernung und Verhinderung der Einschleusung von Schadsoftware und von sicherheitsgefährdendem Programmcode sowie eine entsprechende Alarmierung sicherstellen. • **Kryptografie bei der Datenübermittlung:** Geeignete kryptografische Verfahren und Protokolle zur Absicherung der Datenübermittlung werden eingesetzt. Dies gilt insbesondere für die Datenübermittlung über externe bzw. öffentliche Netze und betrifft den Einsatz von Verschlüsselungs-, Signatur- und Hash-Verfahren • **Kryptografie bei der Datenspeicherung:** Geeignete kryptografische Verfahren und Protokolle zur Absicherung der Datenspeicherung werden eingesetzt. • **Datensicherung:** Zur Vermeidung von Datenverlusten werden geeignete Datensicherungs-, Datenauslagerungs- und Wiederherstellungsverfahren umgesetzt. • **Zugriffs-Protokollierung**: Ein Verfahren zur automatisierten Protokollierung und anlassbezogenen Auswertung aller Verarbeitungsvorgänge wird umgesetzt, das sicherstellt, dass die Zulässigkeit der Datenverarbeitung nachvollzogen und überprüft werden kann. Dies gilt insbesondere für die Verarbeitung von personenbezogenen Daten. Die zu protokollierenden Verarbeitungsvorgänge umfassen jedenfalls Erhebungen, Veränderungen, Abfragen, Offenlegungen einschließlich Übermittlungen, Kombinationen sowie Löschungen von Daten. Aus den Protokolldaten müssen zumindest der Zweck, die

	verarbeiteten Daten, das Datum und die Uhrzeit der Verarbeitung hervorgehen. • **Source Code Analysen und Penetrationstests:** Zur Identifizierung von etwaig bestehenden Sicherheitsschwachstellen im Quellcode oder in der Systemkonfiguration des IT-Verfahrens werden Source Code Analysen und Penetrationstests eingeplant und durchgeführt. **<u>Allgemeine Maßnahmen:</u>** • **Geheimhaltung**: Die im Rahmen der Bedienung der Systeme beteiligten Personen unterliegen Verschwiegenheitsverpflichtungen. • **Zulässigkeit der Verarbeitung:** Die Zulässigkeit der Verarbeitung von personenbezogenen Daten wurde im Rahmen des SoHOG bzw. der SoHO-Verordnung gesetzlich vorgezeichnet und festgelegt. • **Dokumentation der Verarbeitungstätigkeiten:** Die Dokumentation der Verarbeitungstätigkeit erfolgt über das Protokollierungssystem, da jede Verarbeitung der im gegenständlichen IT-Verfahren gespeicherten Daten lückenlos protokolliert wird. • **Risikoanalyse**: Eine erste allgemein gehaltene Risikoanalyse zum gegenständlichen IT-Verfahren wurde durchgeführt und entsprechend unter dem Punkt Risiken dokumentiert. • **Vertrag mit Auftragsverarbeiter:** Die Festlegung des Betriebs des gegenständlichen IT-Verfahrens ist zum Zeitpunkt des Aufsetzens dieser Datenschutzfolgeabschätzung noch nicht abschließend geklärt. Nach Festlegung werden der Betrieb des gegenständlichen IT-Verfahrens und insbesondere die Verarbeitung von personenbezogenen Daten in einem Betriebsvertrag schriftlich geregelt. Zusätzlich wird ein Vertrag über die Auftragsverarbeitung abgeschlossen. Sofern das gegenständliche IT-Verfahren nicht nur durch das BMASGPK selbst betrieben wird. • **Maßnahmenumsetzung- und Überwachung:** Die in einem ersten Schritt evaluierten sowie festgelegten Sicherheits- und Datenschutzmaßnahmen sind dokumentiert und werden im Zuge der technischen Umsetzung des gegenständlichen IT-Verfahrens ebenso umgesetzt. Nach erfolgter Umsetzung findet eine entsprechende Überwachung statt.
BERÜCKSICHTIGUNG VON DATENSCHUTZINTERESSEN	
Stellungnahme der/des Datenschutzbeauftragten der erlassenden Stelle: (Art. 35 Abs. 2 DSGVO)	Die Einholung des Rates der Datenschutzbeauftragten (Art. 35 Abs. 2 DSGVO) des BMASGPK zu dieser Datenschutz-Folgenabschätzung erfolgte bei deren Durchführung.
Stellungnahme der Datenschutzbehörde und betroffener Personen: (Art. 36 Abs. 4 DSGVO und Art. 35 Abs. 9 DSGVO)	Die Einholung einer Stellungnahme der Datenschutzbehörde und betroffener Personen erfolgen durch die Publikation des Entwurfes im Rahmen der Begutachtung.

- Physische, materielle und immaterielle Schäden; Verletzung von Berufsgeheimnissen; Diskriminierung; Rufschädigung oder sonstige unbefugte Verarbeitung von personenbezogenen Daten durch Dritte; finanzielle Verluste; unbefugte Aufhebung der Pseudonymisierung (Risiko 1).
- Identitätsdiebstahl; Verlust der Kontrolle über personenbezogene Daten (Risiko 2)



In der Gesamtbetrachtung ergibt sich damit eine

mittlere Einstufung

des Risikos. Damit war die Aufsichtsbehörde nicht vorab zu konsultieren. Die Maßnahmen sind aber laufend zu evaluieren und bei Bekanntwerden von Schwachstellen unverzüglich anzupassen.

www.parlament.gv.at

160/ME XXVIII. GP - Ministerialentwurf - Datenschutzfolgeabschätzung