Checkliste für Datenverarbeitung (DV) inkl. Datenschutzfolgenabschätzung (DSFA)

Die nachfolgende Checkliste kann zur Durchführung und Dokumentation einer Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DSGVO herangezogen werden. Sie dient sowohl der Durchführung der Vorabprüfung, um festzustellen, ob eine DSFA erforderlich ist (sog. Schwellwertanalyse), als auch der Durchführung der DSFA selbst. Die Checkliste ist für jeden neuen Verarbeitungsprozess auszufüllen, auch wenn im Ergebnis keine DSFA erforderlich ist.

Für die Durchführung der Schwellwertanalyse und der DSFA, ist die Organisationseinheit verantwortlich, die über die Zwecke und Mittel der Verarbeitung der betroffenen personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO). Das ist **i.d.R. ein Fachreferat**, das sich hierbei fachlich, datenschutzrechtlich und technisch von anderen Organisationseinheiten beraten lassen kann. Weitergehende Informationen zur DSFA entnehmen Sie bitte dem Merkblatt „DV mit DSFA". Das Merkblatt „DV mit DSFA" ist entsprechend dieser Checkliste aufgebaut und enthält nähere Informationen zu den einzelnen Prüfungspunkten.
Das Merkblatt kann hier abgerufen werden:

01 - R II 4 - Merkblatt DV mit DSFA für Bw -

Hinweis: Die ausgefüllte Checkliste stellt den DSFA-Bericht dar. Ein gesonderter DSFA-Bericht ist i.d.R. nicht erforderlich. Allerdings erfordern komplexere Verarbeitungen ausführlichere Darstellungen und zusätzliche Anlagen (z.B. Datenschutzkonzept mit Regelungen zum Datenschutzmanagement, IT-Sicherheitsdokumentation u.ä.) oder sogar einen umfangreicheren DSFA- Bericht (vgl. Musterbeispiel im Sowohl für die Schwellwertanalyse als auch die Durchführung einer DSFA ist die Zuarbeit durch die Fachseite, die die die Verarbeitung vornimmt, erforderlich. Bei jeder DSFA und bei der Schwellwertanalyse von komplexeren Verarbeitungen ist ein interdisziplinäres Team notwendig, um alle zu betrachtenden Aspekte zu berücksichtigen (vgl. „Merkblatt DV mit DSFA" unter C.1.1).

Vorüberlegung	
Ergebnis: Besteht ein Personenbezug? ☒ **ja** ☐ **nein**	Sollen mit dem geplanten Verfahren **personenbezogene Daten** verarbeitet werden? Nach Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Metadaten in IT-Systemen, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Insofern bestehen sehr viele Möglichkeiten, eine natürliche Person zu identifizieren, so dass ein Personenbezug eher die Regel als die Ausnahme sein wird. ⇨ **Weiteres Vorgehen:** Bitte dokumentieren Sie das Ergebnis der Prüfung auch in der linken Spalte. Bei „nein" ist das Datenschutzrecht nicht einschlägig und nichts zu veranlassen. Bei „ja" ist das Datenschutzrecht anzuwenden und die Prüfung ab A. zu starten.
A. Schwellwertanalyse	

Bei der Schwellwertanalyse handelt es sich um eine Vorabprüfung, um festzustellen, ob die Durchführung einer DSFA überhaupt erforderlich ist. Durch die Schwellwertanalyse wird ermittelt, wie hoch das Risiko für die Rechte und Freiheiten der Personen ist, deren Daten verarbeitet werden.

Sie ist immer dann durchzuführen, wenn

- ein neuer Verarbeitungsvorgang **eingeführt** werden oder ein bereits bestehender Verarbeitungsvorgang **geändert** werden soll **und**
- dabei **personenbezogene Daten** verarbeitet werden.

⇨ **Hinweis:** Die Schwellwertanalyse ist immer nötig, um das Risiko einer geplanten neuen oder veränderten Verarbeitung zu ermitteln. Außer in den gesetzlich (A.5.1) oder von den Aufsichtsbehörden vorgegebenen Fällen (A.5.2 und A.5.3) einer DSFA muss der Verantwortliche durch eine eigene Risikoanalyse das Risiko seiner geplanten Verarbeitung ermitteln. Die Risikoanalyse ist jedoch ein Arbeitsschwerpunkt einer DSFA, der auch bei Verarbeitungsvorgängen mit geringem oder mittleren Risiko, die keine DSFA erfordern anfällt. Zur Arbeitserleichterung können gleichartige Verarbeitungsvorgänge zentral zusammengefasst und bewertet werden (vgl. B.) Bei der Risikoanalyse sind auch die tolerierbaren Restrisiken aus der IT-Sicherheitsdokumentation zu berücksichtigen.

Prüfschritte	Dokumentation
A. 1	**Rechtsgrundlage**
	Welche Rechtsgrundlage liegt der Verarbeitung zu Grunde? *Beschreibung / Nennung der Rechtsgrundlage (n)* Artikel 6 Abs.1 lit.a DSGVO (Einwilligung) i.V.m. Artikel 9 Abs.2 lit.a (Verarbeitung besonderer Kategorien personenbezogener Daten) i.V.m. Artikel 89 DSGVO (Garantien und Ausnahmen in Bezug auf die Verarbeitung (…) zu wissenschaftlichen (…) Forschungszwecken (…)) i.V.m. § 27 BDSG (Datenverarbeitung zu wissenschaftlichen (…) Forschungszwecken (…)) i.V.m. § 11 HmbDSG (Datenverarbeitung zum Zwecke wissenschaftlicher Forschung) **Hinweis:** Die fachlich zuständige Organisationseinheit muss die Rechtsgrundlagen ihres Handelns und deren Grenzen kennen und dem ADSB für die Aufnahme in das Verarbeitungsverzeichnis DATAV mitteilen. Beispiele häufig genutzter oder problematischer Rechtsgrundlagen befinden sich im „Merkblatt DV mit DSFA" unter A.1.
A. 2	**Vorhaben und Zweck der Verarbeitung**
A. 2.1	**Verwendete Systeme** (= Sachverhaltsdarstellung, Beschreibung des Vorhabens)
	Bezeichnung und Beschreibung des verwendeten - automatisierten oder nicht automatisierten - Systems/der verwendeten Systeme: AV unter Nutzung gängiger Bürosoftware und bestimmter IT-gestützten Testverfahren (siehe unter A.2.2) Darzustellen sind daher im Wesentlichen • die zu verarbeitenden personenbezogenen Daten mit allen Datenarten • Datenerhebungen • Datenflüssen • Beschreibung des Verarbeitungszweckes • Erforderlichkeit der Daten für den Verarbeitungszweck • verwendete IT-Systeme • Formate beim Speichern od. Transferieren (Kommunikationsprotokolle)

	• Schnittstellen der verwendeten IT-Systeme • Prozesse und Funktionsrollen • Maßgebliche Rechtsgrundlagen • Mögliche künftige Zweckänderungen
A. 2.2	**Zweck und Inhalt der Verarbeitung**
	Beschreibender Text zum Zweck und Inhalt der Verarbeitung: Die EHA-Studie wird im Rahmen eines Promotionsvorhabens durchgeführt. Der Beginn der Studie ist derzeit (aufgrund der Corona-Situation) nicht zu konkretisieren. Es wird von einem Erhebungszeitraum von einem halben Jahr ausgegangen. Der konkrete Zweck wird beschrieben in der Studieninformation und in der Einwilligung selbst. In der EHA-Studie sollen mit Hilfe eines quasi-experimentellen Ansatzes und mittels eines Fragebogens Erkenntnisse zum Zusammenhang von Aufmerksamkeit und Hochsensibilität gewonnen werden. Es ist ein Stichprobenumfang von 200 bis 300 Studienteilnehmern geplant. Es werden standardisierte und validierte Fragebogen digitalisiert (am PC) dargeboten und bearbeitet. Zudem werden klassische (Stroop, CPT) und neuere Aufmerksamkeitsaufgaben (CMT) bearbeitet. Teilweise sind diese im Wiener Testsystem integriert. Teilweise sind sie auf einer eigenen Softwaregrundlage (Testsystem) programmiert worden. Erhobene Daten im Rahmen der Einwilligung (getrennte Speicherung von den Untersuchungsdaten): ○ Name, Vorname ○ E-Mail-Anschrift Erhobene soziodemographische Daten: ○ Geschlecht (m,w,d) ○ Geburtsjahr ○ Schulbildung ○ Berufsbildung Erhobene andere Merkmale: ○ Händigkeit ○ Fehlsichtigkeit und entsprechende Korrektur Durchzuführende Testverfahren: ○ SAM (self-assessment manikin) – subjektive Befindlichkeitseinschätzung ○ ACE-D (adverse childhood experiences) ○ HSPS-G (Grad der Hochsensibilität) ○ SOC-13 (Grad des Kohärenzsinns) ○ *B5PO (Big Five Plus One – Erfassung von Persönlichkeitsmerkmalen) ○ *INSBAT (3 Subtests: Kurzzeitgedächtnis, Langzeitgedächtnis und figural-induktives Denken) ○ Stroop Word-Color Test (SWCT) ○ Continous performance task (CPT) ○ Continuous matching task (CMT) ○ TLX (NASA task load index) ○ CAARS (Connors adult ADHS scale) Die Aufzeichnung der Herzfrequenz erfolgt über ein Messsystem der Fa. POLAR (V800).

	Die Tests werden in einem speziell dafür konfigurierten IT-System mit bis zu 5 Test-Plätzen durchgeführt. Dieses System ist nicht mit anderen IT-Umgebungen oder IT-Netzen verbunden und es ist keine Verbindung zum Internet herstellbar. Dieses Test-IT-System im Labor wird durch einen der beiden Studienleiter administriert. In diesem Testsystem findet die Aufzeichnung der Testdaten statt. Die Testdaten werden täglich auf einer externen Festplatte gesichert. Die externe Festplatte wird in einem verschlossenen Raum in einem verschlossen Schrank aufbewahrt. Zu diesem Schrank haben nur die Studienleiter Zugang und geben diese Festplatte täglich (an Untersuchungstagen) zum Zwecke der Datensicherung an die Versuchsleiterinnen und -leiter heraus. An der Studie sind zwei Studienleiter (die Doktoranden) und 5 Versuchsleiter (maximale Anzahl der Testplätze) beteiligt. Versuchsleiter leiten die Probanden während des Tests an und begleiten diese durch die Tests. Die Versuchsleiter starten, überwachen und schließen die Testsysteme. Die Datenaufzeichnung erfolgt im Hintergrund. Am Ende eines "Untersuchungstags" transferieren die Studienleiter die erhobenen Daten auf eine externe Festplatte zum Zwecke der Sicherung. Zugriff auf die Inhalte der Testdateien ist den Versuchsleitern nicht möglich. Der Umgang mit den konkreten Daten beschränkt sich ausschließlich auf die beiden Studienleiter. Die Testdaten werden pseudonymisiert verarbeitet. Es ist vorgesehen, die Daten so früh wie möglich zu anonymisieren. Anonymisiert werden die Daten der Probanden, die sich nicht für eine Folgeuntersuchung eignen. Dazu müssen Sensitivitätsanalysen mit dem deutschsprachigen Instrument zur Feststellung der Merkmalsausprägung von Hochsensibilität durchgeführt werden. Der Zeitbedarf hierfür ist derzeit nicht genau bestimmbar. Die Daten der Probanden, die sich für eine Folgeuntersuchung eignen (und ihre Einwilligung hierzu erteilt haben) werden personenbezogen in die Folgeuntersuchung übernommen. Insbesondere die in den Tests CAARS, HSPS, ACE und SOC13 gewonnenen Daten werden der Intimsphäre von Personen, dem Bereich der inneren Gedanken- und Gefühlswelt sowie des Sexualbereichs, somit dem Schutzbereich 3 zugeordnet. Mit den möglichen Angaben zu sexuellem Missbrauch in der Kindheit und Jugend wird potentiell eine besondere Kategorie personenbezogener Daten verarbeitet.
A. 3	**Beteiligte Organisationeinheiten und Referate**
	Fachseitig beteiligte Organisationeinheiten *(vollständige Auflistung)*: Fakultät für Geistes- und Sozialwissenschaften Psychologische Diagnostik und Persönlichkeitspsychologie Helmut-Schmidt-Universität – Universität der Bw Hamburg IT-Seitig beteiligte Organisationseinheiten *(vollständige Auflistung)*: Rechenzentrum der HSU / UniBw H Beteiligte Referate *(vollständige Auflistung)*: --
A. 4	**Betroffene Personen**

	Auflistung aller Personengruppen, deren Daten durch den Verarbeitungsvorgang betroffen sind: Teilnehmerinnen und Teilnehmer an der Studie
A. 5	**Risikoanalyse**
A. 5.1	**Gesetzliche Muss-Liste** (sog. Positivliste)
Ergebnis: Ist aufgrund der Prüfung der gesetzlichen Muss-Liste eine DSFA erforderlich? ☒ **ja** ☐ **nein**	Bitte kreuzen Sie die zutreffenden Aussagen an. Sofern Sie mindestens **eines** der folgenden Merkmale mit „ja" beantworten können, ist die Durchführung einer DSFA erforderlich (Weitere Einzelheiten zur gesetzlichen Muss-Liste entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter 5.1 sowie Art. 35 Abs. 3 DSGVO): ☒ Datenverarbeitung zum Zwecke des **Profilings oder in Scoringverfahren**. ☒ Verarbeitung besonders schützenswerter personenbezogenen Daten i.S.d. **Art. 9 Abs. 1 DSGVO** oder **Art. 10 DSGVO in besonders großem Umfang**. ☐ Systematische umfangreiche **Überwachung im öffentlichen Raum**. ⇨ **Weiteres Vorgehen:** Bitte dokumentieren Sie das Ergebnis der Prüfung auch in der linken Spalte. Bei „nein" ist die Prüfung unter A.5.2 fortzusetzen und eine Prüfung anhand der BfDI-Liste durchzuführen. Bei „ja" ist eine DSFA grundsätzlich erforderlich und Sie können die Prüfung unter B. fortsetzen.
A. 5.2	**BfDI-Muss-Liste** (sog. Blacklist)
Ergebnis: Ist aufgrund der Prüfung der BfDI-Liste eine DSFA erforderlich? ☒ **ja** ☐ **nein**	Bitte kreuzen Sie die zutreffenden Aussagen an. Sofern Sie mindestens **zwei** der folgenden Merkmale mit „ja" beantworten können, ist die Durchführung einer DSFA erforderlich (Weitere Einzelheiten zur BfDI-Muss-Liste entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter 5.2): ☒ **1.** Die Verarbeitung umfasst eine **Bewertung oder Einstufung** der Betroffenen, darunter das Erstellen von Profilen und Prognosen. ☐ **2.** Die Verarbeitung umfasst eine **automatisierte Entscheidungsfindung** mit Rechtswirkung oder ähnlich bedeutsamer Wirkung. ☐ **3.** Die Verarbeitung hat die **Beobachtung**, Überwachung oder Kontrolle von Betroffenen zum Ziel *(Maßnahmen der Dienst- und Fachaufsicht sowie der IT-Sicherheit zum Zugangs- und Zugriffsschutz gehören nicht hierzu.)*. ☒ **4.** Bei der Verarbeitung werden vertrauliche oder höchst persönliche Informationen nach **Art. 9 Abs. 1** oder **Art 10 DSGVO**, Gesundheitsdaten, Sozialdaten oder Finanzdaten verarbeitet. ☐ **5.** Es handelt sich um eine **Datenverarbeitung in großem Umfang**, d.h. Daten von über 5.000.000 Betroffenen oder mindestens 40% der betroffenen Personengruppe werden verarbeitet *(Bezugsgröße sind insbesondere sämtliche Beschäftigten des Geschäftsbereiches des BMVg, derzeit ca. 270.000)*. ☐ **6.** Im Rahmen der Verarbeitung werden Datensätze aus zwei oder **mehreren Verarbeitungen zusammengeführt** und/**oder abgeglichen**, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden *(vgl. „Merkblatt DV mit DSFA" unter C.5.3)*. ☐ **7.** Bei der Verarbeitung werden Daten von **schutzbedürftigen Betroffenen** verarbeitet (Kinder, **Arbeitnehmer / Beamte / Soldaten im Falle einer Verarbeitung durch den Arbeitgeber / Dienstherrn**, Personen mit besonders hohem Schutzbedarf, Betroffene die in einem besonderen Ober-

	Unter-Ordnungsverhältnis zum für die Verarbeitung Verantwortlichen stehen). ☐ **8.** Bei der Verarbeitung **werden neue Technologien oder organisatorische Lösungen** in einer Art und Weise eingesetzt, die dem gegenwärtigen Stand der Technik voraus ist *(z.B. bei Einführung einer neuen Software, die bisher nicht mögliche technische Verarbeitungen ermöglicht)*. ☐ **9.** Die Verarbeitung an sich **hindert die Betroffenen** an der Ausübung eines Rechts, der Nutzung einer Dienstleistung oder der Durchführung eines Vertrags *(z. B. durch Verarbeitung entsteht ein SCHUFA-Eintrag, der den Abschluss eines Handy-Vertrags verhindert)*. ⇨ **Weiteres Vorgehen:** Bitte dokumentieren Sie das Ergebnis der Prüfung auch in der linken Spalte. Bei „nein" ist die Prüfung unter A.5.6 fortzusetzen und eine eigene Risikoabschätzung durchzuführen. Treffen zwei der Merkmale zu, ist eine DSFA grundsätzlich erforderlich und Sie können die Prüfung unter B. fortsetzen.
A. 5.3	**DSK-Muss-Liste** (ist auch eine sog. Blacklist)
Ergebnis: Ist aufgrund der Prüfung der DSK-Muss-Liste eine DSFA erforderlich? ☐ **ja** ☒ **nein**	**Hinweis:** Die Datenschutzkonferenz (DSK) der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes (BfDI) und der Länder (alle 16 LfDI) hat die folgende Muss-Liste mit **Schwerpunkt für den nicht öffentlichen Bereich** herausgegeben. Da einige der dort aufgeführten Verarbeitungen auch in der Bundeswehr vorkommen können, wird hier die DSK-Muss-Liste ebenfalls aufgenommen. Bitte kreuzen Sie die zutreffenden Aussagen an. Sofern Sie mindestens **eines** der folgenden Merkmale mit „ja" beantworten können, ist die Durchführung einer DSFA erforderlich (Weitere Einzelheiten und Beispiele zur DSK-Muss-Liste entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter 5.3): ☐ **1.** Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und 10 DSGVO handelt. ☐ **2.** Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen. ☐ **3.** Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und • der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können. ☐ **4.** Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus ein oder mehreren Erfassungssystemen in großem Umfang zentral zusammengeführt werden. ☐ **5.** Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen.

	(Jeder, der nicht Partei des betreffenden Rechtsverhältnisses – das kann eine gesetzliche Vorschrift oder ein Vertrag sein – ist, ist ein sog. Dritter.) ☐ **6.** Verarbeitung von umfangreichen personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden. ☐ **7.** Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der Betroffenen. ☐ **8.** Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind, und • der Entdeckung vorher unbekannter Zusammenhänge zwischen den Daten für nicht im Vorhinein bestimmte Zwecke dienen. ☐ **9.** Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person. ☐ **10.** Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der betroffenen Personen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum. ☐ **11.** Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit der Betroffenen. ☐ **12.** Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind, das die Betroffenen nicht erkennen können. ☐ **13.** Erstellung umfassender Profile über die Bewegung und das Kaufverhalten von Betroffenen. ☐ **14.** Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DSGVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte *(Jeder, der nicht Partei des betreffenden Rechtsverhältnisses – das kann eine gesetzliche Vorschrift oder ein Vertrag sein – ist, ist ein sog. Dritter.)*. ☐ **15.** Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DSGVO - auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b DSGVO anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden. ☐ **16.** Verarbeitung von Daten gemäß Art. 9 Abs. 1 DSGVO und Art. 10 DSGVO – auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b DSGVO anzusehen ist – sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Personen zu bestimmen. ⇨ **Weiteres Vorgehen:** Bitte dokumentieren Sie das Ergebnis der Prüfung auch in der linken Spalte. Bei „nein" ist die Prüfung unter A.5.6 fortzusetzen und eine eigene

Risikoabschätzung durchzuführen. Trifft mindestens eines der Merkmale zu, ist eine DSFA grundsätzlich erforderlich und Sie können die Prüfung unter B. fortsetzen.

Nach der EU-Methode zur Ermittlung des Schwellwertes für eine DSFA (2 aus 10) liegt ebenfalls die Notwendigkeit der Durchführung einer DSFA vor.

Punkte aus "Zehnerregel"	Vorhanden
(1) Scoring	x
(2) Automatisierte Einzelentscheidung (mit Rechtswirkung)	
(3) Systematisches Beobachten	
(4) Sensitive Daten	x
(5) Umfangreiche Datenverarbeitung	
(6) Verkettung von Daten	
(7) Besonders schutzwürdige Betroffene	
(8) Neue Technologien/Verarbeitungen	
(9) Verarbeitung außerhalb EU	
(10) Hürde für den Betroffenen, ein Recht auszuüben/ Dienst zu nutzen	

A. 5.4 Ausschluss einer DSFA durch BfDI (sog. Negativliste)

Ergebnis: Ist eine DSFA durch BfDI ausgeschlossen?

☐ **ja**

☒ **nein**

Der BfDI hat nach Art. 35 Abs. 5 DSGVO die Möglichkeit, eine Liste von Verarbeitungstätigkeiten herauszugeben, für die keine DSFA erforderlich ist. Hiervon hat der BfDI bisher **keinen** Gebrauch gemacht.

A. 5.5 Ausschluss einer DSFA durch Gesetzgebungsverfahren

Ergebnis: Ist eine DSFA durch BfDI ausgeschlossen?

☐ **ja**

☒ **nein**

Nach Art. 35 Abs. 10 DSGVO ist eine DSFA entbehrlich, wenn die Auswirkungen auf den Datenschutz bereits im Gesetzgebungsverfahren überprüft wurden. Dies trifft bisher auf **kein** bestehendes Gesetz zu. Es dürfte auch in Zukunft eher eine theoretische Möglichkeit bleiben, da die Sachverhalte, die ein Gesetz regelt sehr vielfältig und unterschiedlich sind.

A. 5.6 Eigene Risikoabschätzung

Ergebnis: Ist aufgrund der eigenen Risikoabschätzung eine DSFA erforderlich?

☐ **ja**

☐ **nein**

Hat der Verarbeitungsvorgang auf Grundlage einer eigenen Risikoabschätzung voraussichtlich ein „hohes" Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, ist die Durchführung einer DSFA erforderlich. Die Einzelheiten zur Durchführung der Risikoabschätzung entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter 5.6".

Beschreibung des Risikos

(Bitte beschreiben Sie die folgenden Kategorien.)

1. Mögliche Schäden

Prüfung auf mögliche Schäden gem. Erwägungsgrund 75 DSGVO . (siehe auch: www.govdata.de/dl-de/by-2-0). Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kurzpapier Nr.18: Risiko für die Rechte und Freiheiten natürlicher Personen, 7. Mai 2018)

Mögliche Schäden	
Diskriminierung: Diskriminierung ist die ungleiche, benachteiligende und ausgrenzende Behandlung von Gruppen und	Die Angaben, wegen derer ein gesetzliches Diskriminierungsverbot besteht, werden in dieser Verarbeitung nicht er-

	Individuen ohne sachlich gerechtfertigten Grund. In Deutschland regelt Artikel 3 des Grundgesetzes das Diskriminierungsverbot: „Niemand darf wegen seines Geschlechts, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen benachteiligt oder bevorzugt werden. Niemand darf wegen seiner Behinderung benachteiligt werden.“	hoben. Diskriminierung als möglicher Schaden kann aus diesen Gründen nicht eintreten. **Diskriminierung aus Bösartigkeit**, z.B. wegen irgendwelcher unangenehmen Erlebnisse in der Kindheit oder Jugend oder z.B. wegen irgendwelcher ADHS-Symptome, **ist möglich.** Der wahrscheinlichste Schaden ist die **Kompromittierung (peinliche Beschämung)** gegenüber anderen Personen, wenn Daten unbefugt bekannt gemacht werden.
	Identitätsdiebstahl oder –betrug: Als Identitätsdiebstahl wird die missbräuchliche Nutzung von persönlichen Daten durch Dritte bezeichnet. Dabei wird neben dem Namen eine Reihe persönlicher Daten wie z.B. Geburtsdatum, Anschrift, Führerschein- oder Sozialversicherungsnummer, Bankkonto oder Kreditkartennummer genutzt, um die Feststellung der tatsächlichen Identität des Schädigers zu umgehen oder zu verfälschen. Die (vorteilziehende) missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte (den Schädiger) kann einen betrügerischen Vermögensvorteil zum Ziel haben oder es wird versucht, den rechtmäßigen Inhaber der Identität in Misskredit zu bringen. Identitätsdiebstahl oder –betrug selbst ist kein möglicher Schaden im engen Sinne, denn erst eine missbräuchliche Nutzung führt zu Schäden, z.B. Rufschädigung oder Vermögensschaden.	Entscheidend ist das Motiv zum Identitätsdiebstahl. In dieser Verarbeitung werden keine Daten verarbeitet, die Zugang zu materiellen Ressourcen verschaffen oder z.B. Bestellungen unter falschem Namen ermöglichen könnten oder die Zugang zu Unterlagen schafft, in denen fiktive (schlechte) Prüfungsleistungen (zur Diskreditierung) der betroffenen Person eingeschmuggelt werden könnten. Es kann kein „sinnvoller“ Nutzen für einen Schädiger konstruiert werden, der aus einem Identitätsdiebstahl oder –betrug im Rahmen dieser Studie resultieren könnte. Der mögliche Schaden „Diskriminierung aus Bösartigkeit“ ist bereits oben festgestellt.
	Finanzieller Verlust	Dieser Schaden kann nicht entstehen, da keine Daten verarbeitet werden, die kriminellen Zugang zu Finanzquellen der betroffenen Personen ermöglichen.
	Rufschädigung: Bei der Rufschädigung handelt es sich um eine ehrenrührige und unwahre Tatsachenbehauptung. Der Tatbestand der Rufschädigung wird dadurch verwirklicht, dass man, obwohl man es besser weiß, eine Behauptung über einen anderen Menschen verbreitet, um so dessen Ansehen in der Öffentlichkeit zu beschädigen. Eine üble Nachrede begeht, wer eine Tatsache behaup-	Wenn wahre Angaben aus den verarbeiteten Daten unbefugt verbreitet werden, kann daraus keine Rufschädigung resultieren, da es sich nicht um ehrenrührige oder unwahre Angaben handeln kann. Die unwahre Tatsachenbehauptung ist möglich, stellt aber immer einen unbefugten Umgang mit personenbezogenen Daten dar.

tet oder verbreitet, die zur Herabwürdigung geeignet ist und die erweislich nicht wahr ist.	
Verlust der Vertraulichkeit bei Berufsgeheimnis	Es werden keine Angaben verarbeitet, die dem Berufsgeheimnis unterliegen. Verlust der Vertraulichkeit bei Berufsgeheimnis ist daher kein möglicher Schaden dieser Verarbeitung.
wirtschaftliche oder gesellschaftliche Nachteile: Gesellschaft bezeichnet in der Soziologie allgemein eine durch unterschiedliche Merkmale zusammengefasste und abgegrenzte Anzahl von Personen, die als sozial Handelnde miteinander verknüpft leben und direkt oder indirekt sozial inter-agieren. Soziale Interaktion ist das wechselseitig aufeinander bezogene Handeln von Akteuren, also das Geschehen zwischen Personen, die aufeinander reagieren, miteinander umgehen, einander beeinflussen und steuern. Gesellschaftliche Nachteile können also nur dort entstehen, wo das vorhandene Geschehen zwischen Personen durch das Ereignis verschlechtert wird.	Wirtschaftliche Nachteile im Zusammenhang mit den bei dieser Studie verarbeiteten Daten sind nicht zu erwarten. Gesellschaftliche Nachteile sind im Rahmen der Teilnahme an dieser Studie lediglich als Folge von Diskriminierung oder Rufschädigung denkbar und möglich.
Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen	Die Verarbeitung personenbezogener Daten im Rahmen der EHA-Studie erfolgt mit informierter Einwilligung der Testpersonen. Diese sind über ihr Recht, die Einwilligung zurückzunehmen nachweislich informiert. Dieser mögliche Schaden ist nicht gegeben.
Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten: Es wird davon ausgegangen, dass nicht eine umfängliche Prüfung bezüglich aller Rechte und Freiheiten (z.B. gem. der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten oder die Grundrechte gem. Grundgesetz oder der grundrechtsgleichen Rechte) vorgenommen werden muss, sondern diese Prüfung sich auf die Rechte bezüglich Datenschutz bezieht.	Es ist grundsätzlich allen betroffenen Personen möglich, Rechte gem. DSGVO geltend zu machen. Der Ausschluss oder die Einschränkung der Ausübung von Rechten und Freiheiten ist kein möglicher Schaden.
Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte (z.B. Vorlieben, Interessen, Aufenthaltsort, Ortswechsel, usw.)	„Profiling“ meint jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Bewertet werden z.B.

	ADHS-Symptome, Hochsensibilität, die Senso-Motorik. Diese Profilerstellung ist für jede einzelne Testperson erforderlich, um im Rahmen der späteren Auswertung aggregierte allgemein gültige Aussagen treffen zu können. Die Erhebung der o.g. Profile ist Mittel zum Zweck der wissenschaftlichen Forschung. Sie ist allerdings nicht zu einer Nutzung bezogen auf die Probanden vorgesehen. Aber: die Profilerstellung ist Ziel der Testung, die Profilnutzung ein möglicher Schaden.
körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten: Hier ist das Recht auf körperliche Unversehrtheit angesprochen. Körperliche Schäden entstehen durch physische Gewalteinwirkung oder im Falle von auch psychischen Erkrankungen durch nicht-physische Einwirkung (z.B. Mobbing, üble Nachrede etc.).	Es sind keine physischen Handlungen denkbar, die auch bei offengelegten Daten aus der EHA-Studie zu körperlichen Schäden führen könnten. Dies ist kein möglicher Schaden. Die möglichen Handlungen Diskriminierung aus Bösartigkeit und Rufschädigung, hier besonders im Sinne von Kompromittierung der betroffenen Person können geeignet sein, körperliche Schäden auf der Grundlage psychischer Gewalteinwirkung hervorzurufen.

Das Recht auf informationelle Selbstbestimmung ist grundsätzlich nicht ausgeschlossen oder eingeschränkt, es ist in seiner Garantie prinzipiell durch unbefugten Umgang mit personenbezogenen Daten gefährdet.

Die Rechte der betroffenen Person gem. DSGVO sind durch diese Verarbeitung nicht ausgeschlossen oder eingeschränkt.

Mögliche Schäden sind:

- Diskriminierung aus Bösartigkeit, Kompromittierung (peinliche Beschämung)
- Rufschädigung aus unwahren Tatsachenbehauptungen
- Profilnutzung (Profile, die während der Tests ermittelt werden)
- Körperliche Schäden aufgrund psychischer Gewalteinwirkung.

Ein immer möglicher Schaden ist unbefugte Kenntnis / unbefugter Umgang mit personenbezogenen Daten durch Unbefugte, dem durch technische und organisatorische Maßnahmen begegnet wird. Hierzu siehe Datenschutzkonzept und IT-Sicherheitskonzept der HSU/UniBw H.

2. Mögliche Schadensereignisse

Mögliche Schadensereignisse	
Unbefugte oder unrechtmäßige Verar-	Dies ist immer eine latente Gefahr, da

	beitung	Daten versehentlich Unbefugten zur Kenntnis gelangen können (z.B. durch Unterlassen des Abschließens des Büros beim Verlassen, versehentliche falsche Adressierung einer Nachricht, nicht sichere Speicherung u.ä.). Dies führt immer zur Einschränkung des Rechts auf informationelle Selbstbestimmung.
	Verarbeitung wider Treu und Glauben: Treu und Glauben ist ein in der Rechtsprechung und Lehre beherrschender Grundsatz, der nach seinem Wortlaut in § 242 BGB nur die Art und Weise einer geschuldeten Leistung erfasst. Entgegen den meisten anderen zivilrechtlichen Vorschriften enthält § 242 BGB einen „offenen" Tatbestand. Das bedeutet, dass er in den einzelnen Situationen wertend konkretisiert werden muss und die Verkehrssitte berücksichtigt werden muss. Das Merkmal Treue bedeutet innerhalb der Generalklausel nach seinem Wortsinn eine auf Zuverlässigkeit, Aufrichtigkeit und Rücksichtnahme beruhende äußere und innere Haltung gegenüber einer anderen Person. Glauben meint das Vertrauen auf eine solche Haltung. Sofern der Grundsatz Treu und Glauben Anwendung finden soll, erfordert es eine umfassende Interessenabwägung aller in Betracht kommenden Interessen, um ein gerechtes Ergebnis zu erzielen.	Unbefugte oder unrechtmäßige Verarbeitung - wie jeder Verstoß gegen Datenschutz-Grundsätze - verstößt gegen eine auf Zuverlässigkeit, Aufrichtigkeit und Rücksichtnahme beruhende äußere und innere Haltung gegenüber einer anderen Person und verletzt das Vertrauen auf eine solche Haltung. Sobald also irgendein Verstoß vorliegt, liegt auch ein Verstoß gegen eine Verarbeitung nach Treu und Glauben vor. **Dieser Verstoß braucht nicht separat betrachtet zu werden.**
	Für den Betroffenen intransparente Verarbeitung	Die Transparenz von Verarbeitungstätigkeiten als Voraussetzung dafür, dass die rechtlich festgelegten Anforderungen an eine Verarbeitung sowohl für die Organisation selber, als auch zumindest in einer allgemeinverständlichen Form für den Betroffenen sowie für die Aufsichtsbehörden überprüfbar sind, ist gegeben. Die Betroffenen sind aufgeklärt über die Studie, nehmen selbst daran aufgrund einer informierten Einwilligung teil, können uneingeschränkt ihre Datenschutz-Rechte wahrnehmen.
	Unbefugte Offenlegung von und Zugang zu Daten	Dies kann nur unter Verstoß gegen die vorgesehenen TOM passieren, die im IT-Sicherheitskonzept der HSU / UniBw H, dem Datenschutzkonzept der HSU / UniBw H, projekt-/verfahrensbezogenen Datenschutzkonzepten und den DATAV-Anmeldungen beschrieben sind.

	Dies ist ein mögliches Schadensereignis.
Unbefugte Aufhebung einer Pseudonymisierung	Die Daten werden gem. Aussage in den Studieninformationen pseudonymisiert verarbeitet. Dies ist hier ein mögliches Schadensereignis.
Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten	Dies ist eine immer latent vorhandene Gefahr. Über Brandschutzmaßnahmen (gem. Brandschutzkonzept) und IT-Sicherheitsmaßnahmen (gem. IT-Sicherheitskonzept) wird dieser Gefahr entgegengewirkt. Für das Testsystem wird Brandschutz über die tägliche Trennung der IT vom Stromnetz des Labors erreicht.
Verweigerung der Betroffenenrechte	Dies ist kein mögliches Schadensereignis. Alle Teilnehmer an der Studie werden über ihre Rechte in der Einverständniserklärung aufgeklärt. Im Datenschutzkonzept der HSU / UniBw H wir ebenso auf die Rechte der betroffenen Personen hingewiesen. Die ADSB der HSU / UniBw H ist gem. Datenschutzkonzept der HSU / UniBw H generell an Auskunftserteilungen und Bearbeitung von Widerspruchserklärungen beteiligt.
Verwendung der Daten durch den Verantwortlichen zu inkompatiblen Zwecken	Dies ist kein mögliches Schadensereignis. Die Ergebnisse und Daten dieser Studie werden als wissenschaftliche Publikationen in anonymisierter Form veröffentlicht. Die vollständig anonymisierten Daten dieser Studie werden nach Abschluss der Studie als offene Daten im Internet in einem Datenarchiv zugänglich gemacht. Der Verantwortliche hat keine konkrete Kenntnis der personenbezogenen Rohdaten. Gem. Artikel 5 Abs.1 lit.b DSGVO gilt eine Weiterverarbeitung für wissenschaftliche Forschungszwecke nicht als unvereinbar mit den ursprünglichen Zwecken. Im Auftrag des Verantwortlichen führt die ADSB Kontrollen bezüglich der Einhaltung von Datenschutz-Vorschriften durch.
Verarbeitung nicht vorhergesehener Daten	Dies ist nur bei unzulässiger und/oder nicht autorisierter Datenerhebung möglich. Hier ist die Verarbeitung nicht vorhergesehener Daten kein mögliches Schadensereignis, da nur die im Rahmen der zur Anwendung kommenden standardisierten Testverfahren und des Fragebogens erhobenen Daten zur Verarbei-

	tung kommen.
Verarbeitung nicht richtiger Daten	Dies ist hier kein mögliches Schadensereignis, da alle Daten von den betroffenen Personen selbst kommen bzw. die Daten von den betroffenen Personen selbst in den Testverfahren generiert werden.
Verarbeitung über die Speicherfrist hinaus	Dies ist ein mögliches Schadensereignis, wenn die Anonymisierung zum frühest möglichen Zeitpunkt gem. § 11 Abs.2 HmbDSG nicht durchgeführt wird.

3. Risikoquellen

Risikoquellen	
Interne menschliche Quellen - Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler	Dies ist ein **geringes Risiko**, da wissenschaftlich gebildetes und ausgebildetes Personal eingesetzt ist und lange bewährte Verfahren angewendet werden.
Interne menschliche Quellen - Vorsätzliches Handeln: Schaden für den Betroffenen wird entweder billigend in Kauf genommen oder wird vom Verursacher beabsichtigt und stellt Ziel der Handlung dar	Dieses Risiko ist immer vorhanden (die meisten Täter sind Innentäter). Von der Tat wird aber durch die Androhung dienstrechtlicher und zivilrechtlicher Maßnahmen abgeschreckt. **Geringes Risiko.**
Externe menschliche Quellen - Unbeabsichtigtes Handeln: individuelle oder strukturelle Fehler	Dies kann kaum geschehen. Unbefugter Umgang kann nur geschehen, wenn eine Person unbefugt zugängliche Daten dann auch wissentlich verwendet. Dann liegt vorsätzliches Handeln vor. **Geringes Risiko.**
Externe menschliche Quellen - Vorsätzliches Handeln: Angreifer oder Verursacher außerhalb der verantwortlichen Stelle mit dem Ziel der Schädigung des Unternehmens oder der Betroffenen	Dieses Risiko entsteht - durch Hacker (s.u.) oder - Spionage. Für beides besteht ein **geringes Risiko**.
Nichtmenschliche Quellen – intern / extern: Systemfehler (Software/Hardware) führen zu Verlust, Veränderung oder missbräuchlicher Verwendung personenbezogener Daten	Das Testsystem ist sehr speziell angelegt, wird durch die Studienleitung selbst administriert und hat keine Schnittstellen zu anderen IT-Systemen oder Netzen. Dieses Risiko ist eher **sehr gering**.
Hauptangreifer VwSt (Risikogeber): Die VwSt erzeugt die Grundrechtsbeeinträchtigung, bricht die informationelle Selbstbestimmung, erzeugt durch Verarbeitung die Risiken bzgl. Informationssicherheit	Die Verarbeitung der Daten ist rechtmäßig. Ein Nutzen zu niederen Beweggründen (finanzielles Interesse, Rufschädigung, Diskriminierung, Kompromittierung o.ä.) kann nicht konstruiert werden. Es wird mit der EHA-Studie eine der Kernkompetenzen einer Universität berührt. Ein Angriff auf die Rechte und Freiheiten der Probanden würde den Ruf der Uni-

	versität gefährden, ist daher unwahrscheinlich. **Geringes Risiko**.
Staatliche Stellen: Unbefugter Zugriff / Motiv?	Dt. staatliche Stellen sind in ihrer Arbeit an Recht und Gesetz gebunden. Keine dt. staatliche Stelle darf sich unbefugten Zugriff auf personenbezogene Daten verschaffen. Ein Interesse anderer staatlicher Stellen erscheint wenig plausibel, da keine wertvollen Informationen aus den Rohdaten der Probanden gezogen werden können. Die interessanten Ergebnisse sind erst nach der Auswertung – dann anonymisiert – verfügbar. **Geringes Risiko**.
Unternehmen: Wirtschafts- / Forschungsspionage aus finanziellen oder Wettbewerbsgründen	Unternehmen können h.E. keine direkten finanziellen oder Wettbewerbsvorteile aus der Kenntnis von EHA-Studien-Rohdaten ziehen. Es sind keine Umsatzsteigerungen, Vorteile bei der Gewinnung von Personal oder technologische Wettbewerbsvorsprünge aus diesen Daten herzuleiten. **Geringes Risiko**.
Gesundheitswesen: (Motiv oder Aktion)	Als Angreifer nicht plausibel konstruierbar, da es zwar um z.B. ADHS-Symptome im CAARS-Test geht, aber keinerlei therapeutische Aspekte oder Lösungen behandelt werden. Im Gesundheitswesen kann kein direkter Vorteil aus der unbefugten Kenntnis der verarbeiteten Daten hergeleitet werden. **Geringes Risiko.**
Forschung	Theoretisch könnte durch Ausspionieren eine parallele Forschung zum von der EHA-Studie behandelten Thema profitieren. Da keinerlei direkte hohe finanzielle Vorteile in Aussicht stehen, besteht hier ein **geringes Risiko**.
Hacking: Datenvandalismus aus Spaß an der Freude	„Professionelle“ Gründe für Hacking können nicht plausibel konstruiert werden. Hacking als Datenvandalismus ist zwar nicht auszuschließen, aber die Qualität der IT-Organisation an der HSU / UniBw H lässt die Bewertung **geringes Risiko** zu.
einzelne Personen: „Gelegenheitsfund“ aus Neugier oder aus Zufall	Angriffe aus niederen Motiven sind nie auszuschließen, aber wenig wahrscheinlich. Aufgrund der arbeitsrechtlich zu erwartenden Nachteile bei Verstoß gegen Datenschutzbestimmungen besteht hier ein **geringes Risiko**.
Plausible Angriffsmotive auf die in der EHA-Studie verarbeiteten Daten lassen sich h.E.	

nicht konstruieren.

Es können keine harten Vorteile (finanzieller Gewinn, personelle oder technologische Vorteile) mit den unbefugt gewonnenen Daten erzielt werden.

Der h.E. schlimmste Schaden bei unbefugter Nutzung der Daten besteht in der Kompromittierung von Probanden.

Das irrationale Angriffsmotiv Hacking mit dem Ziel Datenvandalismus, dem aber über technische und organisatorische Schutzmaßnahmen begegnet werden kann, ist nicht kalkulierbar, aber aufgrund der Absicherungsmaßnahmen eher unwahrscheinlich.

Organisatorische Schwachstellen sind nicht erkennbar. Schutzmaßnahmen sind im Datenschutzkonzept der HSU / UniBw H geregelt. Ein beanstandungsfreier Umgang mit den Daten im Rahmen der EHA-Studie liegt im Interesse derjenigen, die die Studie durchführen, um einerseits keine Angriffe auf das Promotionsvorhaben zuzulassen und um die eigene und Reputation der HSU / UniBw H nicht zu gefährden.

Eintrittswahrscheinlichkeit der möglichen Schäden

Sowohl für die Differenzierung der Eintrittswahrscheinlichkeit als auch für mögliche Schäden könnten jeweils folgende Abstufungen verwendet werden:

	Eintrittswahrscheinlichkeit
Vernachlässigbar	Fast unmöglich / nicht vorstellbar
Begrenzt	Mit gewissem Aufwand machbar (schwierig)
Wesentlich	Mit geringem Aufwand machbar
Maximal	Einfach

Mögliche Schadensereignisse		
		Wahrscheinlichkeit
x	Unbefugte oder unrechtmäßige Verarbeitung	vernachlässigbar
	Verarbeitung wider Treu und Glauben	nb
	Für den Betroffenen intransparente Verarbeitung	nb
x	Unbefugte Offenlegung von und Zugang zu Daten	vernachlässigbar
x	Unbefugte Aufhebung einer Pseudonymisierung	vernachlässigbar
x	Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten	vernachlässigbar
	Verweigerung der Betroffenenrechte	nb
	Verwendung der Daten durch den Verantwortlichen zu inkompatiblen Zwecken	nb
	Verarbeitung nicht vorhergesehener Daten	nb
	Verarbeitung nicht richtiger Daten	nb
x	Verarbeitung über die Speicherfrist hinaus	vernachlässigbar

Das Risiko des Eintritts der o.g. möglichen Schadensereignisse ist insgesamt vernachlässigbar, da es an der HSU / UniBw H eine etablierte Datenschutzorganisation gibt und das Personal für Datenschutzbelange sensibilisiert ist. Die Vorkehrungen des Verantwortlichen zur Sorge für die Einhaltung der Datenschutzbestimmun-

gen werden für wirkungsvoll gehalten. Einem sorglosen Umgang der handelnden Personen mit personenbezogenen Daten wird durch die Kontrollinstanz ADSB entgegen gewirkt, die eine wirkungsvolle Datenschutzorganisation etabliert hat. Technische Fehlfunktionen in der IT-Organisation bleiben nicht unentdeckt, es sind wirksame technische Maßnahmen zum Schutz personenbezogener Daten etabliert. Ausspähung durch Dritte ist über die technischen und organisatorischen Maßnahmen gem. Datenschutzkonzept und IT-Sicherheitskonzept der HSU / UniBw H.

Die zuständigen Bearbeiter und Bearbeiterinnen in der EHA-Studie unterliegen der Treuepflicht und für eine beabsichtigte Verletzung von Datenschutzregelungen sind keine plausiblen Motive denkbar. Eine grundlose menschliche Niedertracht als Motivation für eine bewusste Verletzung von Datenschutzregeln ist nicht einschätzbar.

Eintrittswahrscheinlichkeit der möglichen Schäden		
	Mögl. Schaden	**Wahrscheinlichkeit**
x	Diskriminierung, Kompromittierung	begrenzt
	Identitätsdiebstahl oder -betrug	nb
	finanzieller Verlust	nb
x	Rufschädigung	vernachlässigbar
	Verlust der Vertraulichkeit bei Berufsgeheimnis	nb
	wirtschaftliche oder gesellschaftliche Nachteile	nb
	Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen	nb
	Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten	nb
x	Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte	vernachlässigbar
x	körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten (aufgrund psychischer Gewalteinwirkung)	begrenzt

Die Eintrittswahrscheinlichkeit der möglichen Schäden wird insgesamt als begrenzt eingestuft. In der Studie ist eine Profilerstellung der Probanden hinsichtlich Aufmerksamkeit und Hochsensibilität beabsichtigt, wobei die gewonnenen Profile nach der Auswertung anonymisiert werden. Die Gefahr besteht also lediglich in der Nutzung der gewonnenen Profile durch Unbefugte. Die Wahrscheinlichkeit, dass Ereignisse eintreten, die die sensiblen Daten personenbezogen Unbefugten zur Kenntnis gelangen lassen können, wurde oben als vernachlässigbar eingestuft.

Die h.E. schlimmste Folge dieser möglichen Schadensereignisse kann die Kompromittierung (peinliche Beschämung) der betroffenen Probanden sein, sofern diese insbesondere sehr intime Erlebnisse in ihrer Kindheit oder Jugend angegeben haben. Sind diese Personen insgesamt verletzlich oder nicht gefestigt in ihrer Persönlichkeit, könnten daraus psychische Probleme erwachsen.

Aber alleine die Tatsache, dass alle Probanden freiwillig an der Studie teilnehmen, spricht dafür, dass diese Personen sich der Situation gewachsen fühlen.

Abschließend wird die **Eintrittswahrscheinlichkeit der möglichen Schäden** als **begrenzt** bewertet, weil die kritischen möglichen Schäden Kompromittierung

(peinliche Beschämung) und daraus potentiell resultierende psychische Schädigungen vorliegen könnten.

4. Schwere der möglichen Schäden

Wesentliche Faktoren zur Bewertung der Schwere der möglichen Schadens sind:

Wesentliche Faktoren zur Bewertung der Schwere möglicher Schäden	
Faktor	**Bewertung**
Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DSG-VO, bei denen die DSGVO ausdrücklich eine gesteigerte Schutzbedürftigkeit vorsieht	Es werden Daten des Schutzbereichs 3 verarbeitet. Es werden Gesundheitsdaten (z.B. Erfassung von ADHS-Symptomen) und Angaben zu sexuellen Erlebnissen in Kindheit und Jugend erfasst, die gem. DSGVO ausdrücklich besonders zu schützen sind.
Verarbeitung von Daten schützenswerter Personengruppen (z. B. Kinder (gem. Erwägungsgrund 38 zur DSGVO), Beschäftigte (insbesondere bei Verarbeitung von Daten im Beschäftigungskontext auf der Grundlage der Einwilligung))	Die Probanden sind erwachsen und gehören im Zusammenhang mit der EHA-Studie keiner der genannten schützenswerten Personengruppen an.
Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten wie z. B. eindeutige Personenkennzahlen, Sozialversicherungsnummer, Ausweis-Nr., Passwörter der Betroffenen u.ä.)	Solche Daten werden nicht verarbeitet.
Automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z. B. Profiling) beinhalten und auf deren Grundlage dann **Entscheidungen mit erheblichen Rechtswirkungen** für betroffene Personen getroffen werden (vgl. Art. 35 Abs. 3 lit. a DSGVO)	Aufgrund der verarbeiteten Daten werden keine Entscheidungen mit Rechtswirkung getroffen. Die erhobenen Daten werden ausgewertet und zu prinzipiellen Aussagen verarbeitet.
Wenn der **Schaden nicht oder kaum reversibel ist** oder die betroffene Person nur wenige oder beschränkte Möglichkeiten hat, die Verarbeitung selbst zu prüfen oder gerichtlich prüfen zu lassen oder sich dieser Verarbeitung zu entziehen, etwa, weil sie von der Verarbeitung gar keine Kenntnis hat	Dieser Faktor trifft im Rahmen der EHA-Studie nicht zu. Mögliche Schäden sind seelische Schäden, im Wesentlichen durch Kompromittierung. Aber jeder Proband nimmt freiwillig an der Studie teil und kann jederzeit die Teilnahme abbrechen und – bis zur Anonymisierung der erhobenen Daten – die Löschung der Daten verlangen.
Wenn die Verarbeitung eine **systematische Überwachung** ermöglicht	Dies ist nicht gegeben.
Die **Anzahl** der betroffenen Personen, die Anzahl der Datensätze und die Anzahl der Merkmale in einem Datensatz sowie die geographische Abdeckung	Dies ist hier kein Kriterium. Die Studie wird 200 bis 300 Studienteilnehmer haben.

Die Schwere der möglichen Schäden ist ausschließlich am Faktor „Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DSG-VO, bei denen die DSG-

VO ausdrücklich eine gesteigerte Schutzbedürftigkeit vorsieht“ zu messen. Alle anderen Faktoren treffen auf die Verarbeitung personenbezogener Daten in der EHA-Studie nicht zu.
Die Risiken für die Rechte und Freiheiten natürlicher Personen — mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere — können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte.
Die Schwere des möglichen Schadens wird in folgenden Kategorien eingeschätzt:

Schwere des Risikos	
Vernachlässigbar	Kleine Unannehmlichkeiten
Begrenzt	Größere Unannehmlichkeiten
Wesentlich	Wesentliche Folgen
Maximal	Wesentliche und/oder irreversible Folgen

Bewertung der Schwere der möglichen Schäden		
	Mögl. Schaden	**Schwere des mögl. Schadens**
x	Diskriminierung, Kompromittierung	begrenzt; die Probanden nehmen freiwillig an der Studie teil. Wer Kompromittierung befürchtet, wird eher nicht an dieser Studie teilnehmen oder die Teilnahme abbrechen.
	Identitätsdiebstahl oder -betrug	nb
	finanzieller Verlust	nb
x	Rufschädigung	vernachlässigbar; die Probanden geben im Wesentlichen Selbsteinschätzungen über ihre eigenen Wesenszüge und/oder Verhaltensweisen ab, die für Personen, mit denen die Probanden täglichen Umgang haben, wahrnehmbar sind. Hiervon ausgenommen sind die Angaben zu unangenehmen Erlebnissen in Kindheit und Jugend. Hier wird das Risiko aber eher in der Kompromittierung gesehen.
	Verlust der Vertraulichkeit bei Berufsgeheimnis	nb
	wirtschaftliche oder gesellschaftliche Nachteile	nb
	Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen	nb
	Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten	nb
x	Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte	vernachlässigbar; die Probanden wissen, dass ihr Profil hinsichtlich Aufmerksamkeit und Hochsensibilität erstellt und nach Auswertung anonymisiert wird. Eine Benutzung dieses Profils durch Unbefugte

		kann weder zu physischem, noch zu materiellem Schaden führen. Der größte mögliche immaterielle Schaden wird h.E. durch Kompromittierung erreicht. Dies ist oben diskutiert.
x	körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten (aufgrund psychischer Gewalteinwirkung)	vernachlässigbar; physische Schäden könnten aus der Kompromittierung als Folge von psychischer Erkrankung resultieren. Diese Art Schaden ist unwahrscheinlich und behebbar.

Insgesamt wird die **Schwere der möglichen Schäden** als **begrenzt** eingestuft.

Die Festlegung des Risikowertes mit
Schwere des möglichen Schadens **begrenzt** und
Eintrittswahrscheinlichkeit des möglichen Schadens **begrenzt**
ergibt sich in Anlehnung an das Kurzpapier Nr.18 (Risiko für die Rechte und Freiheiten natürlicher Personen) des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein vom 07. Mai 2018 wie folgt:
(leichtes) **Risiko**

Schutzbedarf
Aus der Standard-Datenschutzverordnung: „Jede Verarbeitung personenbezogener Daten durch eine Organisation stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.“ Das Recht auf informationelle Selbstbestimmung ist im Grundgesetz nicht explizit geregelt. Das Bundesverfassungsgericht hat es in seinem Volkszählungs-Urteil aus dem allgemeinen Persönlichkeitsrecht (Art.2 Abs. 1 GG i.V.m. Art.1 Abs.1 GG) entwickelt und versteht es als eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts. Die Intim- und Privatsphäre (besonders geschützter und geschützter innerer Lebensbereich) genießen starken Schutz, während die Sozial- und Öffentlichkeitssphäre eher schwach geschützt sind.

	Bedeutung
Intimsphäre	… ist der Kernbereich privater Lebensgestaltung, der Bereich der inneren Gedanken- und Gefühlswelt sowie des Sexualbereichs, der dem hoheitlichen Zugriff entzogen ist.
Privatsphäre	… wird einerseits räumlich (Leben im häuslichen Bereich, im Familienkreis, Privatleben), andererseits aber auch gegenständlich (Sachverhalte, die typischerweise privat bleiben) definiert. Eingriffe in diese Sphäre sind in der Regel unzulässig, wenn nicht ausnahmsweise Umstände hinzutreten, die die gegenläufigen Interessen überwiegen lassen (z.B. bei Presseveröffentlichungen aus dem Privatleben von Politikern, wenn ein überwiegendes öffentliches Informationsinteresse besteht).
Sozialsphäre	… ist der Bereich, in dem sich der Mensch als „soziales Wesen“ im Austausch mit anderen Menschen befindet. Hierzu zählt insbesondere die berufliche, politische oder ehrenamtliche Tätigkeit. Diese Sphäre ist – z.B. gegen Veröffentlichungen – relativ schwach geschützt, sodass Eingriffe in aller Regel zulässig sind, wenn nicht ausnahmsweise Umstände hinzutreten, die den Persönlichkeitsschutz überwiegen lassen.
Öffentlichkeits-	… ist der Bereich, in dem der Einzelne sich der Öffentlichkeit

sphäre	bewusst zuwendet, etwa wenn er bewusst an die Öffentlichkeit tritt und sich öffentlich äußert. Diese Sphäre genießt den schwächsten Schutz.

Die im Rahmen der EHA-Studie verarbeiteten Daten werden der Intimsphäre zugeordnet.

Zunächst wird geprüft, ob Verarbeitungsszenarien vorliegen, die die Schutzbedarfskategorie „hoch" rechtfertigen.

Schutzbedarfskategorie „hoch" gem. Standard-Datenschutzmodell	
Beispielhafte Verarbeitungsszenarien	**Bewertung für diese AV**
Verarbeitung nicht veränderbarer Personen-Daten, die ein Leben lang als Anker für Profilbildungen dienen können bzw. zuordenbar sind (z.B. biometrische Daten, Gen-Daten)	nein
Verbreitung eindeutig identifizierter, hoch verknüpfbarer Daten (z.B. lebenslang gültige Krankenversicherungsnummer, Steuer-ID)	nein
Gesetzlich begründete oder anderweitig zu erklärende Intransparenz der Verfahrensweisen für Betroffene (z.B. Verfassungsschutz, Schätzwert im Scoring)	Nicht zutreffend
Verarbeitung von Daten in einem Verfahren mit **möglichen Auswirkungen auf das Ansehen / die Reputation** des Betroffenen	Der mögliche Schaden Kompromittierung (peinliche Beschämung) tendiert in diese Richtung.
Verarbeitung von Daten in einem Verfahren mit möglichen gravierenden finanziellen Auswirkungen für Betroffene	nein
Verarbeitung von Daten in einem **Verfahren mit möglichen Auswirkungen auf die körperliche Unversehrtheit** des Betroffenen	Dies kann mittelbar der Fall sein.
Verarbeitung von Daten, die realistischer Weise zu erwartende Auswirkungen auf die Grundrechtsausübung einer Vielzahl Betroffener haben können (z.B. bei zunehmend flächendeckender, öffentlicher Videoüberwachung)	nein
Gefahr von **Diskriminierung, Stigmatisierung** (z.B. durch Algorithmen, intransparentes Zustandekommen von Entscheidungen eines Betroffenen)	Diskriminierung in Form der Kompromittierung besteht als Gefahr, allerdings nicht wegen der links genannten Gründe. Die Stigmatisierung / Brandmarkung durch Dritte aufgrund unbefugt bekannt gewordener Rohdaten (z.B. über unangenehme Erlebnisse in Kindheit und Jugend) besteht ebenfalls als Gefahr. Die Gefahr einer willkürlichen Benachteiligung oder Benachteiligung aus Gründen der Rasse, der ethischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, der sexuellen Identität oder des Alters nach § 1 AGG durch den Verantwortlichen besteht nicht.
Eingriffe in besonders geschützten inneren Lebensbereich eines Betroffenen	Sie in einigen Tests erhobenen Daten sind eindeutig dem geschützten inneren Lebensbereich zuzuordnen.
Betroffene sind von den Entscheidungen bzw. Leistungen einer Organisation abhängig (etwa in der Leistungsverwaltung oder im medizinischen Bereich) und	nein. Die Erhebung der Daten ist in keiner Weise mit der Lebensführung oder dem Berufsleben der betroffe-

die Organisation verarbeitet Daten mit einer weitreichenden Eingriffsintensität, was zu erheblichen Konsequenzen für den Betroffenen führen kann	nen Personen verknüpft.
Betroffene sind von den Entscheidungen bzw. Leistungen einer Organisation abhängig (etwa in der Leistungsverwaltung oder im medizinischen Bereich) und die Organisation verarbeitet Daten, welche gesetzlich als besonders schutzwürdig ausgewiesen sind	nein. Die Erhebung der Daten ist in keiner Weise mit der Lebensführung oder dem Berufsleben der betroffenen Personen verknüpft.

Vier Szenarien, für die die Schutzbedarfskategorie „hoch“ gilt, treffen für die EHA-Studie zu.

Prüfung, ob Kriterien zur Einstufung in die Schutzbedarfskategorie „sehr hoch“ gegeben sind:
Die Einstufung in die Schutzbedarfskategorie „sehr hoch“ ist geboten, wenn ein Betroffener von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existentiell abhängig ist und zusätzliche Risiken für den Betroffenen nicht bemerkbar sind.

Eine unmittelbare existentielle Abhängigkeit im Sinne der Sicherung des Lebensunterhalts kann in der Teilnahme an der EHA-Studie nicht angenommen werden. Zusätzliche Risiken für die informationelle Selbstbestimmung, Rechte und Freiheiten für den Betroffenen sind nicht erkennbar.

Die Daten, die im Rahmen der EHA-Studie verarbeitet werden, sind nicht einem Szenarium zuzuordnen, dass die Schutzbedarfskategorie „sehr hoch“ rechtfertigt.

Ergebnis: Die Verarbeitung der in der EHA-Studie erhobenen Daten wird der Schutzbedarfskategorie „hoch“ zugeordnet.

Festlegung eines Risikowertes

(Bitte wählen Sie den ermittelten Risikowert aus.)

☐ Geringes Risiko

☒ Risiko

☐ **Hohes Risiko**

Eine Datenschutz-Folgenabschätzung ist nicht erforderlich.

⇨ **Weiteres Vorgehen:** Bitte dokumentieren Sie das Ergebnis der Prüfung auch in der linken Spalte. Ergibt die Risikoabschätzung, dass lediglich ein „geringes Risiko“ oder ein „Risiko“ besteht, ist keine DSFA erforderlich. Die Prüfung ist dann beendet. Ergibt die Risikoabschätzung, dass ein „hohes“ Risiko besteht, ist eine DSFA grundsätzlich erforderlich und die Prüfung unter B. fortzusetzen.

B. Ähnlicher Verarbeitungsvorgang	**(führt zur Sammelerfassung in DATAV)**
Prüfschritte	**Dokumentation**
Ergebnis: Ist eine DSFA auch nach diesem Prüfungsschritt erforderlich? ☐ **ja** ☒ **nein**	Können Sie die folgende Frage mit „Ja" beantworten, ist die Durchführung einer DSFA **nicht erforderlich**: ☐ Es liegt bereits eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken vor (Art. 35 Abs. 1 Satz 2 DSGVO). Bitte beschreiben Sie den ähnlichen Verarbeitungsvorgang, sofern ein solcher vorliegt: ⇨ **Weiteres Vorgehen:** Wurde bereits eine DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken durchgeführt, ist die Durchführung einer weiteren DSFA nicht erforderlich. Die DSFA und die darin getroffenen Erkenntnisse können dann für den neuen Verarbeitungsvorgang herangezogen werden. Sie können unmittelbar zu Prüfungsschritt D. übergehen. Dies gilt auch dann, wenn die Prüfung unter A.5. ergeben hat, dass eine DSFA aufgrund der gesetzlichen Liste, der BfDI-Muss-Liste, der DSK-Muss-Liste oder einer eigenen Risikoabschätzung durchzuführen ist. Liegt allerdings keine DSFA für einen ähnlichen Verarbeitungsvorgang vor, ist die DSFA unter C. und D. durchzuführen und zu dokumentieren.

C. Durchführung einer DSFA

Sofern die Schwellwertanalyse ergeben hat, dass die Durchführung einer DSFA erforderlich ist, ist der nachfolgende Prozess zu beachten. Über die Prüfschritte in der linken Spalte können Sie dokumentieren, wie weit die Bearbeitung fortgeschritten ist. Weitergehende Informationen zu der Durchführung der einzelnen Prüfschritte entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter C.

C. 1	**DSFA-Team**
☐ **offen** ☐ **in Bearbeitung** ☒ **abgeschlossen**	Die Durchführung einer DSFA obliegt gem. Art. 35 Abs. 1 DSGVO und Art. 4 Nr. 7 DSGVO dem Verantwortlichen (i.d.R. der Dienststellenleiter). Bei der Umsetzung datenschutzrechtlicher Vorgaben wird der Verantwortliche vom ADSB seiner Dienststelle unterstützt. Daher wirkt der / die zuständige **ADSB der verantwortlichen Dienststelle** bei der Durchführung der Organisation des Prozesses der DSFA in jedem DSFA-Team seiner Dienststelle mit und kann bei Bedarf auf die Expertise des Fachstranges Administrativer Datenschutz zurückgreifen. **Hauptverantwortlicher** für die Durchführung der DSFA ist die für die jeweilige DSFA **fachlich zuständige Organisationseinheit**, die über die Zwecke und Mittel der Verarbeitung der betroffenen personenbezogenen Daten entscheidet. Die **weiteren Beteiligten** sind abhängig vom konkreten Verarbeitungsvorgang. Falls es zur Feststellung und Durchführung der technischen Maßnahmen erforderlich ist, sollte je nach geplantem Vorhaben ggf. auch der IT-Sicherheitsbeauftragte einbezogen werden. An der Durchführung der DSFA beteiligte Organisationseinheiten (Name und Organisationsbezeichnung): Johann-Christoph Münscher, Mag. rer. nat. und Marcus Bürger, M.Sc. (Wissenschaftliche Mitarbeiter) als Studienleiter Fakultät für Geistes- und Sozialwissenschaften Psychologische Diagnostik und Persönlichkeitspsychologie

	Helmut-Schmidt-Universität Hamburg UniBw/HH ADSB HSU / UniBw H IT-SiBe HSU / UniBw H Nach Art. 35 Abs. 2 DSGVO und § 7 Nr. 3 BDSG ist das DSFA-Team verpflichtet, den Rat der Beauftragten für den Datenschutz in der Bundeswehr (**BfDBw**) einzuholen *(Siehe C. 7)*. Diese gibt ihren Rat und ihre Einschätzung zu den geplanten Verarbeitungsvorgängen ab. Zeitpunkt und Form der Einbindung der BfDBw ist gesetzlich nicht vorgeschrieben.
C. 2	**Beschreibung der Verarbeitungsvorgänge**
☐ **offen** ☐ **in Bearbeitung** ☒ **abgeschlossen**	Bitte nehmen Sie eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und des Zwecks der Verarbeitung vor, einschließlich der verfolgten berechtigten Interessen: **Siehe A.2.** **Hinweis:** Bei der Bearbeitung kann auf A.2 verwiesen werden.
C. 3	**Notwendigkeits- und Verhältnismäßigkeitsprüfung**
☐ **offen** ☐ **in Bearbeitung** ☒ **abgeschlossen**	Bitte bewerten Sie die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge. Berücksichtigen Sie dabei insbesondere die Frage, ob es eine sinnvolle alternative Vorgehensweise gibt, die weniger stark in die Rechte und Freiheiten der Personen, deren Daten verarbeitet werden, eingreifen würde. Eine Notwendigkeits- und Verhältnismäßigkeitsprüfung im Zusammenhang mit Forschung kann nicht im Voraus objektiv durchgeführt werden, da es um Erkenntnisgewinn über eher un- oder wenig(er) erforschte Gebiete geht. Es kann nur darum gehen, eklatante Missverhältnisse zwischen erhobenen Daten und Forschungszweck bezüglich der Notwendigkeit und Verhältnismäßigkeit der erhobenen Daten zu ermitteln. Gem. Merkblatt der BfDBw ist insbesondere zu prüfen, ob der Zweck der Datenverarbeitung nicht durch eine Anonymisierung oder zumindest eine Pseudonymisierung der personenbezogenen Daten erreicht werden kann. Nach der Erhebung der Daten im Rahmen der EHA-Studie werden die gewonnenen Daten pseudonymisiert verarbeitet und zum frühest möglichen Zeitpunkt anonymisiert. Gem. Merkblatt der BfDBw ist auch zu prüfen, ob die Datenverarbeitung überhaupt zur Erreichung des angestrebten Zwecks geeignet ist oder ob hierfür andere Maßnahmen ergriffen werden müssen. Die Auswahl der Kontaktdaten (Name, Vorname, E-Mail-Adresse) und der Daten zur Bildung von Forschungskategorien (Geschlecht (m,w,d), Geburtsjahr, Schulbildung, Berufsbildung, Händigkeit, Fehlsichtigkeit und entsprechende Korrektur). In der EHA-Studie soll der Zusammenhang von Aufmerksamkeit und Hochsensibilität untersucht werden. Dass hier Untersuchungsgruppen nach Geschlecht, Alter und Bildungsstand gebildet werden, erscheint plausibel. Es ist m.E. hinreichend plausibel, dass auch die Hochsensibilität in Abhängigkeit von Händigkeit untersucht wird da von der Händigkeit auch die Nutzung von Hirnarealen abhängt. Ebenso plausibel erscheint die Untersuchung der Hochsensibilität in Abhängigkeit von der Sehfähigkeit, da Aufmerksamkeit auch durch die visuellen Fähigkeiten bestimmt ist. Gem. Merkblatt der BfDBw muss ebenso die Rechtmäßigkeit des angestrebten Zwecks

	dahingehend geprüft werden, ob der vorgesehene Verarbeitungszweck von der Rechtsgrundlage überhaupt erfasst wird. Dies ist eindeutig zu bejahen, denn jeder Studienteilnehmer willigt in die Teilnahme an der Studie ein und hat sogar im Lauf der Studie jederzeit das Recht, die Teilnahme abzubrechen und die Einwilligung zurückzunehmen. Gem. Merkblatt der BfDBw sind bei dieser Notwendigkeits- und Verhältnismäßigkeitsprüfung insbesondere Schutzziele zu berücksichtigen. Unter C.5. sind Abhilfemaßnahmen aufgelistet, um die Schutzziele zu erreichen. Dies Maßnahmen werden getroffen. Insgesamt werden diese Maßnahmen als hinreichend bewertet, um die Grundprinzipien zur Absicherung des Rechts auf informationelle Selbstbestimmung (Zweck der Schutzziele gem. Standard-Datenschutzmodell) zu gewährleisten. **Insgesamt werden die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge im Rahmen der EHA-Studie als gegeben bewertet, um Erkenntnisse zum Zusammenhang von Aufmerksamkeit und Hochsensibilität zu gewinnen. Eine sinnvolle alternative Vorgehensweise, die weniger stark in die Rechte und Freiheiten der Personen, deren Daten verarbeitet werden, eingreifen würde, wird nicht gesehen.**
C. 4	**Risikobewertung**
☐ **offen** ☐ **in Bearbeitung** ☒ **abgeschlossen**	Bitte nehmen Sie eine Identifizierung und Bewertung der möglichen Risiken des Verarbeitungsvorganges für die Rechte und Freiheiten der Personen, deren Daten verarbeitet werden, vor. Die Einzelheiten der Risikobewertung entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter A.5.6. **Hinweis:** Sofern Sie im Rahmen von A.5.6 bereits eine eigene Risikoabschätzung vorgenommen haben, können Sie hierauf zurückgreifen. **Beschreibung des Risikos** *(Bitte beschreiben Sie die folgenden Kategorien.)* **1. Mögliche Schäden** Siehe A.5.6. **2. Mögliche Schadensereignisse** Siehe A.5.6. **3. Risikoquellen** Siehe A.5.6. **4. Eintrittswahrscheinlichkeit der möglichen Schäden** Siehe A.5.6. **5. Schwere der möglichen Schäden** Siehe A.5.6. **Festlegung eines Risikowertes** *(Bitte wählen Sie den ermittelten Risikowert aus.)*

	☐ Geringes Risiko ☒ Risiko ☐ **Hohes Risiko**
C. 5	**Abhilfemaßnahmen**
☐ **offen** ☐ **in Bearbeitung** ☒ **abgeschlossen**	Bitte stellen Sie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen dar, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird. Die Einzelheiten zu den Abhilfemaßnahmen entnehmen Sie bitte dem „Merkblatt DV mit DSFA" unter C.5. **Technische Maßnahmen** *(Beispiele nach ISO-Standard 29151:2016)* ☒ Pseudonymisierung ☒ Need-to-know Prinzip ☒ Minimierung der Verkettbarkeit ☒ Zugriffsbeschränkung bei Weitergabe ☐ Sperrung von Daten ☐ Löschung von Daten ☐ Monitoring des Zugriffs ☒ Verschlüsselung ☐ Löschen von temp-Daten ☐ Penetrationstest ☐ Löschen ☐ Implementierung eines IT-Sicherheitsmanagements nach ISO27001 ☐ Schutz vor Straftaten ☐ sonstige technische Maßnahmen: **Organisatorische Maßnahmen** • Anonymisierung der Daten von Probanden, die nicht für eine Folgestudie zur Verfügung stehen. • Speicherung der personenbezogenen Rohdatensätze verschlüsselt oder passwortgeschützt auf einem externen Speicher • Die gewonnenen Daten werden vertraulich behandelt, pseudonymisiert verarbeitet und erst später (s.u.) in anonymisierter Form an Dritte weitergegeben. • Es erfolgt eine Trennung von Studiendaten (Quasi-Experiment und Fragebogen) und personenbezogenen Daten (Name, Vorname, E-Mail-Adresse). • Name, Vorname und E-Mail-Anschrift werden gesondert und kodiert gespeichert und sind nur den beiden Studienleitern zugänglich. • Die Testdatensätze werden unter Pseudonym erhoben und gespeichert. • die Auswertung erfolgt pseudonymisiert und später anonymisiert • der Klarname ist nur für den Widerruf/Löschungswunsches des Teilnehmers und eine mögliche Folgeuntersuchung (gemäß Ausprägung der Hochsensibilität) nach separater Einverständniserklärung erforderlich

- im Fall der Eignung des Studienteilnehmers (nach Auswertung festgestellt) erfolgt der Einbezug der personenbezogenen Daten erst im Nachhinein zum Zwecke der Kontaktaufnahme.

Abhilfemaßnahmen		
Schutzziel	**Komponente**	**Maßnahme**
Verfügbarkeit	Daten	Gem. IT-Notfallvorsorgekonzept und IT-Notfallhandbuch; Gem. Teilkonzept Storage und Backup. Sicherungskopien der erhobenen Daten; Sicherung des Metadatenverzeichnisses zur Wiederherstellung nach Verlust; Von den Bereichen des Storage-Area-Network (SAN), auf denen die Daten aller virtualisierten Server, sowie die Datenbanken liegen, werden mehrmals täglich „Crash-Consistent-Snapshots“ angefertigt und einmal täglich VMSnapshots erstellt. Zur Absicherung der Standortbedrohung dient ein Spiegelsystem im Gebäude H2, in welches sämtliche Daten repliziert werden. Somit sind die Daten sämtlicher Systeme redundant ausgelegt; Virenscan
	Systeme	Um einem Systemausfall vorzubeugen sind Kernkomponenten des Datennetzes, Anbindungen an das Internet, Serverstrukturen sowie Netzteile an Servern und Kernkomponenten redundant ausgelegt. Die Stromversorgung ist redundant und unterbrechungsfrei eingerichtet. Die Internetzuleitung erfolgt redundant über verschiedene Trassen. Für den Fall eines Krisenszenarios wurde ein Notfall-Rechenzentrum in den Räumen des Rechenzentrums der Bundeswehruniversität München eingerichtet; Firewall; Bauliche Brandschutzmaßnahmen, Organisatorisches Brandschutzkonzept der HSU/ UniBwH
	Prozesse	Durch EHA-Studieninformation für alle teilnehmenden Personen. Diese Studie folgt den Empfehlungen der Deutschen Forschungsgesellschaft (DFG) und der Deutschen Gesellschaft für Psychologie (DGPs) zur Qualitätssicherung in der Forschung.
Integrität	Daten	Zugangskontrolle durch Passwortschutz; Schutz vor unbefugtem Zugriff wird durch Fragmentierung der gespeicherten Inhalte

			vorgenommen.
		Systeme	Nur die beiden Studienleiter haben Zugriff auf die Daten der Studienteilnehmer.
		Prozesse	Diese Studie folgt den Empfehlungen der Deutschen Forschungsgesellschaft (DFG) und der Deutschen Gesellschaft für Psychologie (DGPs) zur Qualitätssicherung in der Forschung.
	Vertraulichkeit	Daten	Codierung der Studienteilnehmerdaten (Name, Vorname, E-Mail-Anschrift) bei Speicherung, die getrennt, von den Testdaten erfolgt.
		Systeme	Passwort-geregelter Zugang zu PC / Laptop; Durch die Integration der genutzten IT in die DMZ des Rz der HSU / UniBw H sind die Anwendungen im Rahmen der EHA-Studie gem. Stand der Technik im Bereich Virenerkennung und –beseitigung, Intrusion Detection und Intrusion Prevention gesichert. Zusätzlich • Protokollierung • Firewall
		Prozesse	Zutrittskontrolle zu den Studienräumen; Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO) Jährliche Belehrung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)
	Nichtverkettbarkeit durch Zweckbestimmung	Daten	Pseudonymisierung / Anonymisierung
		Systeme	Von anderen Daten / Studien getrennte Aufbewahrung der Daten der EHA-Studie
		Prozesse	zentrale (Be-)Nutzerverwaltung (Identitätsmanagement), die Authentifizierung und Autorisierung von Benutzern an Rechnerplattformen und Diensten, sowie die Bereit- und zur Verfügungstellung darauf aufbauender Anwendungen.
	Transparenz durch Prüffähigkeit	Daten	Aufnahme ins Verzeichnis der Verarbeitungstätigkeiten
		Systeme	Protokollierung in den zentral bereitgestellten Systemen / Servern
		Prozesse	Einwilligungen werden dokumentiert; Betroffene können uneingeschränkt ihre Rechte wahrnehmen
	Intervenierbarkeit durch Ankerpunkte	Daten	Geregelte Anonymisierung
		Prozesse	Probanden werden die gesamte Zeit der Untersuchung von einem Versuchsleiter begleitet und angeleitet. Sie können Ihn jederzeit ansprechen und Fragen klären.

C. 6	**Restrisiko nach Abhilfemaßnahmen**
☐ **offen** ☐ **in Bearbeitung** ☒ **abgeschlossen**	Bitte stellen Sie das Restrisiko für die Rechte und Freiheiten der Personen, deren Daten verarbeitet werden, nach Berücksichtigung der Abhilfemaßnahmen für die Verarbeitungsvorgänge dar. Ein Beispiel finden Sie im „Merkblatt DV mit DSFA" unter C.6. **Beschreibung des Risikos** *(Bitte beschreiben Sie die folgenden Kategorien.)* **1. Mögliche Schäden** Es bleiben grundsätzlich die möglichen Schäden bestehen. **2. Mögliche Schadensereignisse** Es bleiben grundsätzlich die möglichen Schadensereignisse bestehen. **3. Risikoquellen** Als Risikoquelle bleiben mögliche Innentäter, alle anderen Quellen sind sehr wahrscheinlich ausgeschlossen. **4. Eintrittswahrscheinlichkeit der möglichen Schäden** Die Eintrittswahrscheinlichkeit möglicher Schadensereignisse bleibt **vernachlässigbar**. Die Eintrittswahrscheinlichkeit möglicher Schäden wird nunmehr als **vernachlässigbar** eingestuft. **5. Schwere der möglichen Schäden** Der Eintritt von Schadensereignissen und Schäden ist nunmehr als fast unmöglich oder schwer vorstellbar bewertet. Sollte – so unwahrscheinlich dies auch ist - dennoch ein Schadensereignis mit entsprechendem Schaden eintreten, wird sich die Schwere der möglichen Schäden im Eintretensfall nicht mindern. Das verbleibende Restrisiko (des Eintretens von Schadensfällen und Schäden) ist aber gemindert. **Festlegung eines Risikowertes** *(Bitte wählen Sie den ermittelten Risikowert aus.)* ☒ Geringes Risiko ☐ Risiko ☐ **Hohes Risiko**
C. 7	**Rat der BfDBw**
☐ **offen**	Nach Art. 35 Abs. 2 DSGVO und § 7 Nr. 3 BDSG ist das DSFA-Team des Verantwortlichen verpflichtet, den Rat der **BfDBw** einzuholen. Zeitpunkt und Form der Einbindung

☐ **in Bearbeitung** ☐ **abgeschlossen**	der BfDBw ist gesetzlich nicht vorgeschrieben. Aber **spätestens an dieser Stelle** muss die Beratung der BfDBw erfolgen. **Erster sinnvoller Zeitpunkt** für die Einbindung der BfDBw ist **nach** Abschluss von **C.2**. **Stellungnahme der BfDBw**
C. 8	**Standpunkt der betroffenen Personen**
Ergebnis: Stellungnahme der Betroffenen eingeholt? ☐ **ja** ☒ **nein**	Nach Art. 35 Abs. 9 DSGVO ist gegebenenfalls der Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge einzuholen. Form und Zeitpunkt sind gesetzlich nicht vorgeschrieben, so dass entweder einzelne betroffene Personen od. ihre Personalvertretung ohne Formvorgaben beteiligt werden können. **Stellungnahme der Betroffenen** --- oder/und **Begründung** **Nichtbeteiligung der Betroffenen od. Nichtberücksichtigung ihrer Stellungnahme** Zum jetzigen Zeitpunkt sind noch keine betroffenen Personen bekannt. Da die Teilnahme an der EHA-Studie nur mit informierter Einwilligung geschieht und auch während der Studie der Ausstieg und die Löschung der erhobenen Daten jederzeit möglich ist, wird auf eine Einholung des Standpunkts der betroffenen Personen verzichtet. **Hinweis:** Die Beteiligung der betroffenen Personen oder ihrer Vertreter ist zwar nicht zwingend gesetzlich vorgeschrieben, es ist jedoch empfehlenswert bei z.B. bei der Festlegung der Verarbeitung von Beschäftigtendaten die Personalvertretung in eine DSFA einzubinden. Ähnliches gilt für die Verarbeitung von medizinischen Daten von Beschäftigten.
C. 9	**Ergebnis der DSFA**
☐ **offen** ☒ **in Bearbeitung** ☐ **abgeschlossen**	Bitte bestimmen Sie einen neuen Risikowert unter Berücksichtigung der geplanten Abhilfemaßnahmen. Hierbei können Sie auf das Verfahren nach A.5.6 dieser Checkliste bzw. des „Merkblatts DV mit DSFA" zurückgreifen. **Verbleibender Risikowertes** *(Bitte wählen Sie den verbleibenden Risikowert aus.)* ☒ Geringes Risiko ☐ Risiko ☐ **Hohes Risiko** ⇨ **Weiteres Vorgehen:** Ergibt der verbleibende Risikowert ein „geringes" oder „normales" Risiko, kann der Verarbeitungsvorgang durchgeführt werden. Bitte beachten Sie, dass dann auch ein Nachweis zur Umsetzung der Abhilfemaßnahmen und zur Freigabe des Verarbeitungsvorganges erforderlich und unter D. zu dokumentieren ist. Ergibt der verbleibende Risikowert ein „hohes" Risiko, kann der Verarbeitungsvorgang nicht angewendet werden. In diesem Fall ist das weitere Vorgehen im DSFA-Team zu erörtern.

C. 10	Konsultation des BfDI bei hohem Restrisiko
☐ offen ☐ in Bearbeitung ☐ abgeschlossen	Soll der Verarbeitungsvorgang trotz eines verbleibenden Risikowertes „hohes" Risiko angewendet werden, ist nach Art. 36 DSGVO der BfDI vor Beginn der Verarbeitung zu konsultieren. **Stellungnahme der BfDI** ☐ Verarbeitung zulässig, da Restrisiko minimierbar ☐ Verarbeitung unzulässig, da Restrisiko nicht minimierbar **Hinweis:** Kommt ein DSFA-Team zu dem Ergebnis, dass der BfDI zu beteiligen ist, hat es zunächst BfDBw über diese Entscheidung zu informieren. Erst wenn in Zusammenarbeit mit BfDBw keine Risikominimierung möglich ist, informiert das DSFA-Team den BfDI.

D. Folgemaßnahmen

Nachdem die DSFA durchgeführt wurde, ist ein Nachweis darüber zu erbringen, dass die ermittelten Abhilfemaßnahmen durchgeführt und die Verarbeitungsvorgänge freigegeben wurden (Art. 35 Abs. 7 lit. d DSGVO). Bitte beachten Sie, dass dieser Prüfungsschritt auch dann durchzuführen ist, wenn nach B. keine neue DSFA durchgeführt werden muss.

Prüfschritte	Dokumentation
D. 1	**Umsetzung und Test der Abhilfemaßnahmen**
☐ offen ☐ in Bearbeitung ☐ abgeschlossen	Bitte dokumentieren Sie die Umsetzung der unter C.5. und ggf. C.8 ermittelten Abhilfemaßnahmen und deren Wirksamkeit:
D. 2	**Dokumentation**
☐ offen ☐ in Bearbeitung ☐ abgeschlossen	Bei den meisten Verarbeitungen genügt diese Checkliste als Dokumentation. Sollte die Verarbeitungsvorgänge komplexer sein, sind entweder ergänzende Dokumente in die Checkliste einzufügen oder es ist ein gesonderter DSFA-Bericht zu erstellen.
D. 3	**Freigabe der Verarbeitungsvorgänge**
☐ offen ☐ in Bearbeitung ☐ abgeschlossen	Die Verarbeitungsvorgänge wurden freigegeben durch: ***Name/n des/der Verantwortlichen*** Die Verarbeitungsvorgänge wurden freigegeben am:
D. 4	**Aufnahme in Verarbeitungsverzeichnis DATAV**
☐ offen ☐ in Bearbeitung ☐ abgeschlossen	Der Verantwortliche ist gem. Art. 30 DSGVO verpflichtet, seine Verarbeitungsvorgänge in einem Verarbeitungsverzeichnis einzutragen. Für die gesamte Bundeswehr besteht ein gemeinsames Verarbeitungsverzeichnis namens DATAV, in das die zulässigen Verarbeitungsvorgänge einzutragen sind. Hierbei sollte diese Checkliste eingefügt werden, sobald Anhänge in DATAV technisch möglich sind.

E. Veränderungen	
Ergebnis: Ist eine Überprüfung der DSFA erfolgt? ☐ **ja, am** ☐ **nein**	Die DSFA ist gem. Art. 35 Abs. 11 DSGVO erneut zu prüfen, wenn ☐ sich das Risiko der Verarbeitungsvorgänge geändert hat ☐ der Verarbeitungsvorgang bearbeitet werden soll ☐ das der Verarbeitung zugrundeliegende System bearbeitet werden soll **Hinweis:** Es empfiehlt sich daher, regelmäßige Überprüfungen vorzusehen (z.B. alle 1 oder 2 Jahre), ob sich die o.g. Kriterien der DSFA verändert haben. Liegen Änderungen vor, muss die DSFA erneut durchgeführt werden.