Oktober 2023

National Academics Panel Study (Nacaps)

Datenschutz- und Sicherheitskonzept

für die Deutsche Zentrum für Hochschul- und Wissenschaftsforschung GmbH (DZHW) im Rahmen der Promoviertenbefragung von Nacaps

DZHW
Deutsches Zentrum für
Hochschul- und Wissenschaftsforschung

Projektleitung
Dr. Kolja Briedis
Telefon +49 (0)511 45 06 70-132 | Fax +49 (0)511 45 06 70-960
E-Mail: briedis@dzhw.eu

Dr. Sarah Widany
Telefon +49 (0)30 20 64 177-10 | Fax +49 (0)30 20 64 177-99
E-Mail: widany@dzhw.eu

Erstellt unter Mitwirkung des betrieblichen Datenschutzbeauftragten:
Martin Fuchs
Betrieblicher Datenschutzbeauftragter
Telefon +49 (0)511 45 06 70-491 | Fax +49 (0)511 45 06 70-960
E-Mail: datenschutz@dzhw.eu

Impressum

Herausgegeben von
Deutsches Zentrum für Hochschul- und
Wissenschaftsforschung GmbH (DZHW)
Lange Laube 12 | 30159 Hannover | www.dzhw.eu
Postfach 2920 | 30029 Hannover
Tel.: +49 511 450670-0 | Fax: +49 511 450670-960

Geschäftsführung
Prof. Dr. Monika Jungbauer-Gans
Axel Tscherniak

Vorsitzender des Aufsichtsrats
Ministerialdirigent Peter Greisler

Registergericht
Amtsgericht Hannover | B 210251
Umsatzsteuer-Identifikationsnummer:
DE291239300

Oktober 2023

Inhaltsverzeichnis

1 Einleitung

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die entsprechenden Verantwortlichkeiten des DZHW im Rahmen der Befragungen der National Academics Panel Study (Nacaps) der Abteilung 1 – Bildungsverläufe und Beschäftigung. Alle Mitarbeiter*innen des Projekts sind zur Einhaltung dieser Richtlinie verpflichtet.

Die Nacaps Academics Panel Study (Nacaps) ist eine Multikohorten-Längsschnittstudie. Nacaps umfasst sowohl die Promotionsphase als auch die Phase des Übergangs nach der Promotion sowie den weiteren beruflichen Verlauf innerhalb und außerhalb des Wissenschaftssystems als auch alternativen Tätigkeiten (z. B. Familienarbeit) bis ca. zehn Jahre nach der Promotion. Damit stellt Nacaps eine wichtige Ergänzung zur amtlichen Statistik dar und geht zugleich weit über deren Analysemöglichkeiten hinaus. Mit Nacaps können bspw. Determinanten des erfolgreichen und/oder zügigen Abschlusses der Promotion sowie Faktoren für den Verbleib bzw. das Verlassen der Wissenschaft und Werdegänge Promovierender und Promovierter in den Blick genommen werden. Ein Ziel des Projektes ist es, kausalanalytische Fragen beantworten zu können, deren Bearbeitung mit dem bisher für Deutschland verfügbaren Datenmaterial nicht oder nur bedingt möglich ist. Zudem sollen auch Daten für das Bildungsmonitoring an die Bildungspolitik, die Öffentlichkeit und die Wissenschaft geliefert werden. Aktuell geschieht dies u. a. in der Bereitstellung von zentralen Befunden für den „Bundesbericht Wissenschaftlicher Nachwuchs“ (BuWiN) und über das Nacaps-Datenportal (www.nacaps-datenportal.de).

In der ersten Runde von Nacaps wurden Promovierende an über 50 promotionsberechtigten Hochschulen in Deutschland befragt, die zum Stichtag 01.12.2018 an den jeweiligen Hochschulen als Promovierende registriert wurden. Seitdem wurden in zwei weiteren Runden mit jeweils mehr als 60 Hochschulen die jeweils neu registrierten Promovierenden zu den Stichtagen 01.12.2020 und 01.12.2022 befragt. Zudem soll eine Untersuchung mit den Promovierten des Prüfungsjahrgangs 2023 im Frühjahr 2024 starten.

In jeder Runde werden alle promotionsberechtigten Hochschulen in Deutschland zur Kooperation eingeladen. Die Befragungen finden ausschließlich als Online-Erhebungen statt. Jede Kohorte wird nach der Initialerhebung, die zu Beginn eines Jahres stattfindet, im jährlichen Turnus weiterbefragt. Alle zwei Jahre sollen neue Promovierendenkohorten und alle vier Jahre sollen neue Promoviertenkohorten aufgenommen werden.

Die erste Kontaktierung der Promovierenden findet innerhalb der ersten zwei Jahre nach Promotionsbeginn statt. Diese Erstbefragung startet im Februar (zuletzt im Februar 2023). Die Promovierten werden ca. ein Jahr nach Abschluss der Promotion befragt (im ersten Quartal des Folgejahres des Prüfungsjahrs – für das Prüfungsjahr 2023 ist eine Befragung also im 1. Quartal 2024 vorgesehen). Dazu werden die Befragten über einen Link zu der jeweiligen Initialbefragung eingeladen. Dieser Link wird von den Ansprechpersonen an den teilnehmenden Hochschulen verteilt. Sofern die Befragten auch an den Folgebefragungen teilnehmen möchten, geben sie am Ende der Befragung eine Mailadresse an, über die sie weiterhin kontaktiert werden möchten. Diese Adressanagaben werden auf einem anderen Server gespeichert als die Befragungsdaten. Erst durch die freiwillige Angabe der Mailadresse erhält das DZHW Kenntnis von den Adressen, da die Einladung (bzw. die Erinnerungen) zuvor durch die kooperierenden Hochschulen versendet wurde.

Technische und organisatorische Maßnahmen, die durch die Gesellschaft für wissenschaftliche Datenverarbeitung mbg Göttingen (GWDG), den zentralen IT-Dienstleister des DZHW am Standort Hannover, in deren Verantwortungsbereich ergriffen werden, sind im Dokument „Technisch-organisatorische Maßnahmen“ der GWDG, dessen aktuelle Fassung vom 11.01.2023 als Anlage Teil des vorliegenden Datenschutz- und Sicherheitskonzepts ist.

2 Begriffsdefinitionen

- **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 Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
- **Besondere Kategorien personenbezogener Daten (vormals besondere personenbezogene Daten):** Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
- **Personenbeziehbare Daten: Alle** Informationen, die erst durch Verknüpfung mit weiteren Informationen und/oder Datenquellen auf eine identifizierte oder identifizierbare natürliche Person beziehen. Beispiele: Studienfach, Abschluss, Fachsemesterzahl, Amts-/ Dienstbezeichnung, Besoldungs-/Entgeltgruppe, Arbeitszeitanteil.
- **Verantwortlicher (vormals verantwortliche Stelle):** Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.
- **Befragungsdaten:** Angaben der Befragten, die von diesen im Rahmen der Befragung gemacht wurden (z. B. durch die Beantwortung einer Frage).
- **Paradaten:** Paradaten sind technische Informationen, die bei der Benutzung des Onlinefragebogens ohne Mitwirkung der Befragungsteilnehmer*innen automatisch erhoben werden (wie z. B. verwendete Geräte und Betriebssysteme, Zeitpunkt des Webseitenaufrufs, die Verweildauer auf den einzelnen Fragebogenseiten, eventuelle Unterbrechungen in der Befragungsteilnahme und weitere ähnliche Informationen), die Auskunft über die Art und Weise der Beantwortung des Fragebogens geben können.
- **Adressdaten:** Kontaktdaten der Befragten bezüglich deren Anschrift oder Emailadresse sowie Informationen zum Umgang mit diesen im Zuge der Durchführung von Befragungen und der Verarbeitung der Kontaktdaten wie das Datum der Übermittlung der Kontaktdaten durch die Befragten, ob an diese Adressen Befragungsunterlagen versandt wurden oder ob eine Teilnahme erfolgt ist.

3 Beschreibung der Verarbeitung personenbezogener Daten

3.1 Die Probandengruppen (Promovierte)

- Promovierte, die im Prüfungsjahr 2023 eine Promotion erfolgreich abgeschlossen haben. Mit erfolgreichem Abschluss ist das erfolgreiche Bestehen der letzten Prüfung (i. d. R. die Disputation) gemeint.

3.2 Ablauf der Erhebung

- Es werden alle promotionsberechtigen Hochschulen in Deutschland kontaktiert.
- Die Hochschule/Hochschulleitung entscheidet über die (Nicht)Teilnahme. Die Teilnahme der Hochschulen ist freiwillig.
- Bei positiver Rückmeldung teilt die Hochschule die Zahl der voraussichtlichen Absolvent*innen sowie die Kontaktperson/Ansprechperson an der Hochschule mit, die unsere Befragung vor Ort koordiniert.
- Die Hochschulen erhalten vor Beginn der Feldphase ausführliche Informationen zur Durchführung des Versands und Vorlagen für Anschreiben an die Proband*innengruppe sowie eine Excel-Tabelle, mit deren Hilfe die Befragungseinladung durchgeführt werden kann. Zusätzlich erhalten die Ansprechpersonen/Einrichtungen zufällig generierte Zugangsschlüssel („Token“) für die Befragung, die in die Excel-Liste eingetragen werden. Seitens der Hochschulen wird diese Tabelle mit den E-Mail-Adressen der Proband*innengruppe befüllt. Die Token müssen den zu kontaktierenden Promovierten von den Hochschulen eindeutig zugeordnet werden und dienen dem individuellen Aufruf der Befragung durch die Proband*innengruppe. Die Zugangsschlüssel ermöglichen zudem eine optionale Begrenzung von Erinnerungsschreiben zur Teilnahme auf Personen, die noch nicht (abschließend) an der Erhebung teilgenommen haben.
- Die Kontaktierung der Promovierten erfolgt in der Feldphase aus datenschutzrechtlichen Gründen ausschließlich durch die Ansprechpersonen/Einrichtungen der Hochschulen, nicht durch das DZHW. Kontaktdaten der Promovierten werden von den Hochschulen nicht mit dem DZHW geteilt. Ebenso wird dem DZHW nicht mitgeteilt, welchen Promovierten an der jeweiligen Hochschule ein spezifischer Token zugeordnet wurde.
- Zum geplanten Feldstart (1. Quartal 2024) versendet die Hochschule zunächst eine Ankündigung der Befragung an die Promovierten des Prüfungsjahres. Ca. eine Woche später folgt die Einladungsmail, in der ein Link zur Befragung enthalten ist. Die Links sind personalisiert und enthalten individuelle Token. Nach Ablauf einer Frist übermittelt das DZHW die Token, bei denen die Befragung noch nicht abgeschlossen wurde, an die Hochschule. Dadurch kann die Hochschule gezielt die Personen an die Befragung erinnern, die noch nicht teilgenommen/abgeschlossen haben ohne, dass das DZHW Kontaktdaten von der Hochschule übermittelt bekommt. Insgesamt sind drei Erinnerungen vorgesehen.
- Die Fragebögen werden von den Befragten ausgefüllt, dabei ist die Teilnahme an der Befragung freiwillig. Die Befragten werden darauf hingewiesen, dass bei Fragen mit Freitextfeldern aus Datenschutzgründen keine Angaben gemacht werden dürfen, die Aussagen über erkennbare Personen treffen, da dies zur Unverwertbarkeit ihrer Angaben führt.
- Die befragungsbereiten Promovierten können mittels eines Zugangslinks, der in den Anschreiben durch die Ansprechpersonen/Einrichtungen an den Hochschulen eingebettet wurde, über einen Webbrowser eine internetbasierte Online-Befragung beantworten. Die Teilnahme ist

ausschließlich innerhalb des Zeitraums der Feldphase möglich. Mittels ihrer Zugangsschlüssel können die Befragten die Beantwortung unterbrechen und erneut aufnehmen.

- Nach Abschluss der Befragung können die Befragten über einen Link zu einer separaten Datenerfassung gelangen und dort zum einen ihre Kontaktinformationen eintragen und zum anderen erklären, ob diese für die Teilnahme an der Verlosung, die Einladung zu Folgebefragungen (Panelbereitschaft) oder beides genutzt werden dürfen.
- Unter den Teilnehmenden, die der Verlosung zugestimmt haben, werden nach Ende der Feldphase Preise (Incentives) verlost.
- Die Erhebung der Befragungsdaten und der Adressdaten erfolgt getrennt über das DZHW-Onlinebefragungssystem ZOFAR.
- Die Angaben der Befragten gehen auf den Servern des DZHW ein. Nach Abschluss der Befragung wird die Befragung vom Server genommen und die Daten werden dort gelöscht.
- Nach Abschluss der Feldphase erfolgen ein Transfer der erfassten Befragungsdaten durch eine*n benannte*n IT-Mitarbeiter*in in den extra geschützten Bereich (Level 1) und ein separater Transfer der erfassten Adressdaten durch eine*n benannte*n IT-Mitarbeiter*in in einen separaten, gesondert geschützten Bereich (Level 2; siehe hierzu „Zugangskontrolle“).
- Die Adressdaten von Befragten, die ausschließlich der Teilnahme an der Verlosung zugestimmt haben, werden nach Abschluss der Verlosung umgehend gelöscht.
- Die Befragungsdaten werden für die spätere Auswertung und Veröffentlichung als Scientific-Use-File aufbereitet (v. a. Codierung offener Angaben und Anonymisierung).
- Die Befragungsdaten werden mithilfe gängiger statistischer Auswertungsverfahren (u. a. Deskription, multivariate Analysen wie Regression, Ereignisdatenanalyse) ausgewertet und die Ergebnisse in den Publikationsformaten des DZHW, in Vorträgen, Zeitschriftenartikeln oder Monographien wiedergegeben. Ausgewählte Ergebnisse werden über das Nacaps-Datenportal (www.nacaps-datenportal.de) veröffentlicht. Außerdem erhalten die Hochschulen Zugang zu einem passwortgeschützten Partnerbereich, in dem hochschulspezifische Ergebnisse bereitgestellt werden und auf Wunsch einen Mikrodatensatz mit den Angaben aller Befragten. In diesem Mikrodatensatz sind die Angaben von Befragten aus anderen Hochschulen in zahlreichen Merkmalen aggregiert (die Fächer werden z. B. auf einer hohen Aggregatebene ausgewiesen und Herkunftsländer werden nach Weltregionen zusammengefasst) bzw. werden komplett gelöscht (wie die Angabe zur Hochschule; im Datensatz ist dann nur die Unterscheidung zwischen einer befragten Person aus der eigenen und allen anderen Hochschulen möglich.
- Die Adressdaten werden separat der Projektassistenz von Nacaps übergeben. Die Projektassistenz hat keinen Zugriff auf die Befragungsdaten. Umgekehrt haben Teammitglieder, die Zugriff auf die Befragungsdaten haben, keinen Zugriff auf die Adressdaten. Die Adressdaten sind auf einem weiteren gesonderten Bereich des geschützten Bereichs gespeichert.

3.3 Die Datenflüsse

- Die Promovierten füllen die Online-Befragung mithilfe eines internetfähigen Endgeräts (bspw. Laptop, Tablet, Smartphone) aus. Die eingetragenen Angaben werden im DZHW-Befragungssytem ZOFAR zusammen mit dem Zugangsschlüssel/Token abgelegt.
- Befragte, die zur Teilnahme an Folgebefragungen im Rahmen des Panels bereit sind oder an der Verlosung teilnehmen möchten, geben ihre Adressdaten sowie den Zweck der Adressangabe über eine separate Online-Befragung an. Diese Angaben werden im DZHW-Befragungssystem ZOFAR separat abgelegt. Für die Zuordnung von Adressdaten zu Befragungsdaten erzeugt das System zufällige temporäre IDs. Diese IDs werden benötigt, um Zuordnungen gewährleisten zu können.
- Die Befragungsdaten werden von einer*m benannten IT-Mitarbeiter*in im geschützten Bereich (Level 1) gespeichert.
- Die erfassten Adressdaten werden von den Befragungsdaten getrennt durch eine*n benannte*n IT-Mitarbeiter*in in einem separaten, gesondert geschützten Bereich (Level 2) gespeichert (siehe Kapitel 7).

- Für die Integration der Befragungsdaten in das Datenportal wird ein Datensatz erstellt, der ausschließlich Daten zu den im Portal vorhanden Indikatoren und Filterfunktionen enthält. Dieser konsolidierte Datensatz wird in fragmentierten und passwortgeschützten Dateien aus dem geschützten Bereich (Level 1) exportiert und auf einen eigens für das Datenportal eingerichteten und von der HIS-IT administrierten Server importiert. Auf diesem Server erfolgt die Integration der Dateien für die Visualisierung im Datenportal. Der Zugang auf diesen speziell für diesen Zweck eingerichteten Server ist auf die Mitarbeiter*innen des Nacaps-Datenportal am Standort Berlin sowie eine benannte Person der HIS-IT beschränkt. Durch ein Nutzer*innenmanagement haben außerdem die Partnerhochschulen mit einem Vertrag für das Datenportal einen passwortgesteuerten Zugang zu ihren hochschulspezifischen Ergebnissen (siehe 3.5).
- Bei der Aufbereitung für die hochschulspezifischen Mikrodatensätze erfolgt die Aufbereitung und Anonymisierung der Fälle aus anderen Hochschulen im geschützten Bereich (Level 1). Die Datensätze werden dann mit Passwort verschlüsselt. Die Datensätze werden über Academic Cloud mit einer Zeitschaltung von 24 Stunden zum Download zur Verfügung gestellt. Jede Hochschule erhält einen eigenen Link, über den nur der eigene Datensatz verfügbar ist. Das Passwort zum Öffnen der Datei wird auf einem anderen Weg (z. B. per Telefon oder SMS, aber nicht per Mail oder Internet) zur Verfügung gestellt.

3.4 Die konkret eingesetzten Verfahren und Methoden

- internetbasierte Online-Befragung der Promovierten über das DZHW-eigene Befragungssystem ZOFAR
- gängige statistische Auswertungsverfahren (u. a. Deskription, multivariate Analysen wie Regression, Ereignisdatenanalyse)
- Anonymisierung und Pseudonymisierung

3.5 Weitere Verarbeitung und beabsichtigte Verwendung der Daten

- Die Befragungsdaten werden für wissenschaftliche Publikationen und zur Erstellung von Indikatoren zum Bildungsbereich auf Grundlage eines pseudonymisierten Befragungsdatensatzes ausgewertet.
- Auf Grundlage eines pseudonymisierten Befragungsdatensatzes können Analysen zur Verbesserung der Qualität der Erhebungen und die Ausfallgewichtung für Folgewellen durchgeführt werden. Einzelne Befragungsdaten können zeitlich begrenzt als Preloads für Onlinebefragungen in Folgewellen herangezogen werden. (Preloads sind Befragungsdaten aus vorherigen Befragungen, die zur Anzeige oder Steuerung der Befragung genutzt werden – z. B. zur Abfrage, ob eine zuletzt angegebene Beschäftigung noch fortbesteht.)
- Die Forschungsergebnisse werden in einer Form veröffentlicht, die keine Rückschlüsse auf einzelne Befragungsteilnehmer*innen erlaubt.
- Hochschulspezifische Auswertungen sind über das Nacaps-Datenportal und den dort aufbereiteten konsolidierten Datensatz möglich: Im Partnerbereich des Datenportals (www.nacaps-datenportal.de) erhalten die Partnerhochschulen von Nacaps einen passwortgeschützten Zugang, mit dem sie für ausgewählte Variablen die Ergebnisse der Promovierenden ihrer Hochschule einsehen und mit den durchschnittlichen Ergebnissen der anderen Partnerhochschulen (Insgesamt-Werte) vergleichen können. Diese Randauszählungen können mittels Filteroptionen (bspw. Geschlecht oder Kohorte) differenziert werden. In Absprache mit dem Datenschutz wird sichergestellt, dass die Anzahl der Befragten bzw. das Aggregationsniveau der Angaben ausreichend hoch genug für die entsprechenden Auswertungen ist. Für besondere Kategorien personenbezogener Daten werden zusätzliche Maßnahmen getroffen (bspw. Einschränkung der Filteroptionen). Rückschlüsse auf Einzelpersonen dürfen nicht möglich sein. Die Einhaltung des Datenschutzes ist in den Verträgen zur Nutzung des Nacaps-Datenportals festgehalten.

- Hochschulspezifische Auswertungen sind über die hochschulspezifischen Mikrodatensätze möglich: Die Partnerhochschulen erhalten zum Zweck der Forschung und Evaluation einen passwortgeschützten Datensatz mit den Angaben der Befragten der Hochschule. Ausgenommen sind Angaben über Dritte, mit denen eine Deanonymisierung dieser dritten Personen möglich ist (wie z. B. Angaben zum Geschlecht des/der Betreuer/in). Ebenso werden Angaben zum gesundheitlichen Zustand nicht mit übermittelt. Darüber hinaus enthält der Mikrodatensatz ebenfalls die Angaben aller weiteren Befragten. Diese sind jedoch so aggregiert, dass Einzelpersonen – insbesondere mit der Möglichkeit zur Erkennung der Zugehörigkeit zu einer Hochschule – nicht identifiziert werden können. Die Einhaltung des Datenschutzes ist in den Verträgen zur Weitergabe der Mikrodatensätze festgehalten.
- Es werden keine Informationen an die Hochschule weitergegeben, welche Promovierten an der Befragung final teilgenommen haben. Hochschulspezifische Auswertungen werden nur für die jeweilige Hochschule erstellt. Angaben zu einzelnen Hochschulen werden nicht über das FDZ der wissenschaftlichen Öffentlichkeit verfügbar gemacht (siehe „Löschung und Anonymisierung“).
- Die nicht-anonymisierten Befragungsdaten werden gemäß den Richtlinien der DFG für gute wissenschaftliche Praxis zehn Jahre aufbewahrt und anschließend gelöscht.
- Die Adressdaten werden nicht an Dritte weitergegeben und nur zur Kontaktaufnahme für Folgebefragungen sowie zum Versand von Ergebnissen verwendet.
- Die Adressdaten mit ausschließlicher Einwilligung zur Teilnahme an der Verlosung werden nur für die damit verbundenen Schritte (Auslosung, Kontaktaufnahme, Versand) verwendet und unmittelbar nach Ende der Verlosung bzw. nach dem eventuellen vorherigen Widerruf der Einwilligung gelöscht.
- Die Adressdaten mit Einwilligung zur Kontaktaufnahme für Folgebefragungen werden nach der letzten Befragung bzw. nach dem eventuellen vorherigen Widerruf der Einwilligung gelöscht.

3.6 Bereitstellung als Scientific Use File für externe Wissenschaftler*innen

- Die Befragungsdaten werden in anonymisierter Form durch das Forschungsdatenzentrum des DZHW (FDZ-DZHW) ausschließlich für wissenschaftliche Forschungsfragen externen Wissenschaftler*innen (nicht am DZHW beschäftigt) zur Verfügung gestellt.
- Bei anonymisierten Daten in Form von Scientific Use Files für wissenschaftliche Zwecke müssen die potentiellen Datennutzer*innen zunächst einen Datennutzungsantrag stellen. Nur sofern ein wissenschaftlicher Nutzungszweck mit dem Ziel von Erkenntnisgewinn vorliegt, wird ein Datennutzungsvertrag abgeschlossen. Die Kommunikation im Rahmen der Antragsprüfung, des Vertragsabschlusses und der Datenbereitstellung dient zusätzlich der Sensibilisierung der Datennutzer*innen für den Datenschutz.
- Die statistisch anonymisierten Daten werden dann über verschiedene technische Zugangswege bereitgestellt (Download Zugang, Remote-Desktop und On-Site bzw. Gastwissenschaftler*innenaufenthalt im DZHW an einem gesicherten Rechner des DZHW). Diese Zugangswege bieten dem FDZ-DZHW während der Nutzung unterschiedliche Kontrollmöglichkeiten der Datennutzer*innen. Ein Zugriff für externe Personen auf nichtanonymisierte Daten ist nur unter sehr strengen Auflagen möglich (Arbeit mit den Daten vor Ort am DZHW, intensive Kontrolle der Auswertungen durch das DZHW).
- Die unterschiedlichen Zugangswege ermöglichen die Bereitstellung der Befragungsdaten in unterschiedlichen Graden der Aggregation. Das DZHW folgt hier dem vom Bundesbeauftragten für die Informationsfreiheit und den Datenschutz geprüften Konzept des Nationalen Bildungspanels (NEPS) in Bamberg.

4 Verpflichtung zur Vertraulichkeit

- Alle Mitarbeiter*innen des Nacaps-Projektes sind bei Aufnahme ihrer Tätigkeit beim DZHW schriftlich auf Vertraulichkeit (Wahrung des Datengeheimnisses) verpflichtet worden.

5 Der betriebliche Datenschutzbeauftragte

- Das DZHW hat nach Maßgabe von Art. 37 Abs. 1 lit. b) DSGVO einen betrieblichen Datenschutzbeauftragten (bDSB) bestellt. Dieser nimmt die ihm kraft Gesetzes und in dieser Richtlinie genannten Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr. Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden ist allein der bDSB zuständig. Die Fachabteilungen stellen die hierfür erforderlichen Informationen, Unterlagen etc. zur Verfügung. Gleiches gilt für Anfragen, Beschwerden oder Auskunftsersuchen. Jede*r Mitarbeiter*in des DZHW kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den bDSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.
- Die Aufgabe des bDSB wird im DZHW von Herrn Martin Fuchs (datenschutz@dzhw.eu) wahrgenommen.

6 IT-Dienstleistende

- Die zentralen IT-Dienstleistenden des DZHW sind an den Standorten Hannover und Leipzig die Gesellschaft für wissenschaftliche Datenverarbeitung mbg Göttingen, Burckhardtweg 4, 37077 Göttingen, sowie am Standort Berlin die Sal.A iT-Services GmbH, Albertstr. 12, 10827 Berlin.
- Die IT-Dienstleistenden erbringen das gesamte Portfolio der IT-Dienstleistungen: Arbeitsplatz-Services (IT-Arbeitsplatz, E-Mail, Endpoint Security, Druckdienste), Basis-Applikations-Services (LDAP/Active Directory), Informations-Services (Fileserver), System-Services (Managed Server Hosting inkl. geschütztem Bereich, Server Housing), Netzwerk-Services (LAN, WLAN, VPN), übergreifende Services (Backup/Restore, Monitoring), IT-Security-Services (Sicherer Internetzugang und Content Security, Zertifikate).
- Die Verarbeitung personenbezogener Daten im Rahmen von Nacaps erfolgt ausschließlich an den DZHW-Standorten Hannover und Berlin, die für diesen Bereich relevanten Systeme werden ausnahmslos von der GWDG und Sal.A IT betreut.

7 Technische und organisatorische Maßnahmen im Rahmen der Verarbeitung der von den Vertragspartner*innen übermittelten Daten

- Technische und organisatorische Maßnahmen, die durch die GWDG, die zentrale IT-Dienstleistende des DZHW am Standort Hannover, in deren Verantwortungsbereich ergriffen werden, sind im Dokument „Technisch-organisatorische Maßnahmen“ der GWDG aufgeführt, dessen aktuelle Fassung vom 11.01.2023 als Anlage Teil des vorliegenden Datenschutz- und Sicherheitskonzept ist.
- In den folgenden Kapiteln werden nur diejenigen Maßnahmen aufgeführt, welche darüber hinaus im Rahmen des Projektes National Academics Panel Study (Nacaps) durch das DZHW ergriffen werden.

7.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

7.1.1 Zutrittskontrolle

Ziel:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.

Maßnahmen des DZHW:

- Der selbstständige Zutritt zu den Räumen des DZHW ist nur mit personalisierten Transpondern, elektronischen Schlüsseln oder Sicherheitsschlüsseln möglich, welche nur für berechtigte Mitarbeiter*innen freigeschaltet bzw. ausgegeben werden.
- Die Mitarbeiter*innen des DZHW sind angewiesen, bei Abwesenheit ihre Büroräume abzuschließen (Standort Hannover) bzw. ihren Computer zu sperren (Standort Berlin).

7.1.2 Zugangskontrolle

Ziel:

- Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahmen des DZHW:

- Die Zugangskontrolle erfolgt durch persönliche, passwortgesicherte Anmeldung am Netzwerk des DZHW. Das Passwort muss den Anforderungen der Passwort-Richtlinie des DZHW entsprechen und regelmäßig geändert werden.
- Die Mitarbeiter*innen des DZHW sind angewiesen, bei Abwesenheit ihre Rechner zu sperren.
- Die Verarbeitung speziell der personenbezogenen Daten erfolgt in einem geschützten Bereich (Level 1). Der geschützte Bereich ist ein besonders abgeschotteter Netzwerkbereich, der durch Netzwerkkonfigurationen und den Einsatz von Firewalls von anderen Netzwerksegmenten getrennt ist. Der geschützte Bereich besitzt eine eigene Windows Domäne. Der geschützte Bereich

verfügt über keine direkte Verbindung ins Internet, ein Fernzugriff auf den geschützten Bereich (z. B. aus dem Homeoffice) ist nur indirekt über den Umweg einer verschlüsselten Verbindung (VPN) ins allgemeine Firmennetz möglich.

- Die Verarbeitung der Adressangaben erfolgt in einem gesondert geschützten Bereich Level 2) auf einem netzwerkseitig nochmals abgeschotteten Server, der speziell zu diesem Zweck eingerichtet wurde. Der Zugriff erfolgt über eine virtuelle Remote-Desktop-Verbindung und ist nicht parallel zum Zugriff auf die Befragungsdaten möglich. Auch hier gilt: Es handelt sich um einen abgeschotteten Netzwerkbereich, der durch Netzwerkkonfigurationen und den Einsatz von Firewalls von anderen Netzwerksegmenten getrennt ist. Der gesondert geschützte Bereich besitzt eine eigene Windows Domäne. Der gesondert geschützte Bereich verfügt über keine direkte Verbindung ins Internet, ein Fernzugriff auf den gesondert geschützten Bereich (z. B. aus dem Homeoffice) ist nur indirekt über den Umweg einer verschlüsselten Verbindung (VPN) ins allgemeine Firmennetz möglich.

7.1.3 Zugriffskontrolle

Ziel:

- Es ist zu gewährleisten, dass Benutzer*innen nur entsprechend ihrer Berechtigung auf Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahmen des DZHW:

- Der geschützte Bereich besitzt ein eigenes, vom übrigen Netzwerk getrenntes Usermanagement (Active Directory). Die Vergabe und der Entzug von Rechten zur Nutzung des geschützten Bereichs sowie zum Zugriff auf spezifische projektbezogene Dateiordner innerhalb des geschützten Bereichs erfolgt durch ausgewählte Administrator*innen des DZHW im Auftrag der jeweiligen Projektleitung.
- Die Verarbeitung der Daten im geschützten Bereich erfolgt durch Nutzung einer virtuellen Desktop-Infrastruktur (VDI) ausschließlich im Remote-Desktop-Betrieb. Dabei verbleiben die Daten jederzeit auf den abgeschotteten Servern des geschützten Bereichs. Ein Kopieren der Daten an einen anderen Ort, beispielsweise auf die Arbeitsplatzrechner der Bearbeiter*innen, wird durch technische Maßnahmen unterbunden. Ein Zugriff im Remote-Desktop-Betrieb aus dem Homeoffice wird nur von Dienstrechnern aus und über besonders verschlüsselte Verbindungen (VPN) ermöglicht.
- Datenaustausch in und aus dem geschützten Bereich ist (mit Ausnahme für benannte Administrator*innen des DZHW) nur über eine besonders gesicherte Transferroutine möglich. Dabei werden alle Transfers protokolliert. Aus dem gesondert geschützten Bereich dürfen Adressdaten nur für die Erstellung von Einladungsschreiben transferiert werden.

7.1.4 Trennbarkeit

Ziel:

- Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Maßnahmen des DZHW:

- Innerhalb des geschützten Bereichs bestehen spezifische projektbezogene Dateiordner, auf die nur die an den jeweiligen Projekten beteiligten Mitarbeiter*innen Zugriff erhalten.
- Die differenzierte Rechtevergabe dient der Einhaltung des Trennungsgebots.
- Zugriff auf die Adressdaten haben nur ausgewählte Mitarbeiter*innen, die nicht mit der Auswertung der Befragungsdaten betraut sind. Diese Mitarbeiter*innen erhalten keinen Zugriff auf die Befragungsdaten.

7.1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Ziel:

- Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

Maßnahmen innerhalb von Nacaps:

- Die Datensätze enthalten eine Identnummer (im Befragungsdatensatz).
- Die Identnummer führt an den ersten beiden Stellen die Kohorte auf, der die Befragten angehören (z. B. 23 für die Promoviertenkohorte des Prüfungsjahre 2023).
- Alle weiteren Ziffern der Identnummer werden in Abhängigkeit von der Reihenfolge im Primärdatensatz (i.d.R. nach dem Eingangsdatum auf dem Befragungsserver) vergeben. Dadurch wird sichergestellt, dass die Identnummern, die später im Kontaktdatensatz verwendet werden, keinerlei Informationen über die Hochschule der Befragungsteilnehmer*innen enthalten.
- Während einer Befragung wird für den technischen Ablauf für jeden Fall ein Token (i. e. ein zufälliger eineindeutiger Code aus Buchstaben und Zahlen) vergeben. Am Ende der Befragung können die Befragten freiwillig ihre Adressdaten für Folgebefragungen hinterlassen. Diese werden in einer separaten Befragung (Add-On) gespeichert, die sich mit der Einwilligung zur Weitergabe der Adressdaten öffnet. Dort wird ein zusätzlicher Token erstellt (Add-On-Token) und dem Token aus der Hauptbefragung zugeordnet. Diese Zuordnungsliste wird nur im geschützten Bereich (Level 1) aufbewahrt und dient dazu, Personen, die an der Erstbefragung teilgenommen haben, an Folgewellen erneut einladen zu können. Der Zugriff auf die Zuordnungsfunktion ist nur für Projektmitarbeiter*innen möglich, die keinen Zugriff auf die Befragungsdaten haben.
- Außerdem wird eine zweite Zuordnungsliste erstellt, in der die Identnummer aus dem Befragungsdatensatz mit dem Token verknüpft wird. Auch diese Liste wird im geschützten Bereich (Level 1) aufbewahrt. Diese Liste dient dazu, Angaben von Personen, die an mehreren Befragungswellen teilgenommen haben, personengenau miteinander verknüpfen zu können. Der Zugriff auf die Zuordnungsfunktion ist nur für Projektmitarbeiter*innen möglich, die keinen Zugriff auf die Befragungsdaten haben.
- Die Mikrodatensätze, die an die beteiligten Hochschulen herausgegeben werden, enthalten ausschließlich die Identnummer.
- Der konsolidierter Datensatz für das Datenportal, der lediglich in fragmentierten und passwortgeschützten Dateien zerlegt auf dem Server des Datenportals verwendet wird, enthält keine Identnummern.

7.2 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

7.2.1 Übertragungskontrolle

Ziel:

- Bei der Übertragung oder während ihres Transports dürfen personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Maßnahmen des DZHW:

- Gemäß dienstlicher Anweisung sind personenbezogene Daten auf mobilen Datenträgern (z. B. Laptop, USB-Stick) für den Transport, z. B. von und zu Auftragsverarbeitern, zu verschlüsseln. Das jeweilige Passwort ist auf einem getrennten Informationsweg zu übermitteln.

7.2.2 Eingabekontrolle

Ziel:

- Es muss nachträglich festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt wurden.

Maßnahmen innerhalb von Nacaps:

- Die Verarbeitung von Adressdaten erfolgt durch eine*n benannte*n Projektmitarbeiter*in, der*die keinen Zugriff auf die Befragungsdaten hat. Jede Änderung der Adressdaten wird durch die*den Projektmitarbeiter*in dokumentiert.
- Die Befragungsdaten werden in ihrem ursprünglichen Zustand belassen und lediglich per Skripten (Stata-Do-Files) mit eindeutiger Autor*innenschaft aufbereitet. Soweit im Rahmen der Plausibilisierung (Überprüfung des Datensatzes auf Widerspruchsfreiheit) Veränderungen am Datensatz erforderlich werden, so werden neben dem unveränderten Ursprungsdatensatz regelmäßig Bearbeitungszwischenstände gespeichert. So sind alle Bearbeitungsschritte nachvollziehbar, reproduzierbar und reversibel. Die Projektmitarbeiter*innen, die mit diesen Arbeiten betraut sind, haben keinen Zugang zu Adressdaten.
- Die Projektmitarbeiter*innen sind angewiesen, keine händischen Bearbeitungen an personenbezogenen Daten vorzunehmen; es sei denn, dass dies für einen fehlerfreien Import dieser Daten in das relationale Datenbankmodell erforderlich ist. Dies ist zu dokumentieren.

7.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Ziele:

- Personenbezogene Daten sollen gegen zufällige Zerstörung oder Verlust geschützt sein.
- Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Maßnahmen des DZHW:

- Die GWDG sichert im Auftrag des DZHW einmal täglich alle Daten des geschützten Bereichs bzw. des gesonderten Bereichs. Die täglichen Sicherungen werden für einen Zeitraum von 30 Tagen aufbewahrt, bevor sie automatisiert wieder gelöscht werden.

Maßnahmen innerhalb von Nacaps:

- Sowohl die Befragungsdaten als auch die Adressdaten werden im geschützten (Level 1) bzw. gesondert geschützten Bereich (Level 2) gespeichert und somit täglich gesichert.
- Die pseudonymisierten Befragungsdaten werden in einer Datei mit Schreibschutz gespeichert.

7.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

7.4.1 Leitlinien, Richtlinien, Arbeitsanweisungen und Sicherheitskonzepte

Maßnahmen innerhalb von Nacaps:

- Spezielle schriftliche Verfahrensbeschreibungen gibt es für die Aufbereitung (wie die Codierung und Plausibilisierung) der Befragungsdaten. Darüber hinaus erhalten die Projektmitarbeiter*innen von der Projektleitung jeweils arbeitsschrittbezogene schriftliche und mündliche Arbeitsanweisungen bezüglich der Verarbeitung personenbezogener Daten.

7.4.2 Regelmäßige Kontrollen, Dokumentation und ggf. Optimierungen

Maßnahmen innerhalb von Nacaps:

- Die Projektleitung und die Projektassistenz kontrollieren die Einhaltung der Arbeitsanweisungen zum Umgang mit personenbezogenen Daten und dokumentieren ggf. Anpassungen.
- Die Projektleitung stellt die fristgerechte Löschung personenbezogener Daten sicher.

7.4.3 Auftragskontrolle

Ziel:

- Bei der Verarbeitung personenbezogener Daten im Auftrag darf nur entsprechend den Weisungen des/der Auftraggeber*in gehandelt werden.

Maßnahmen innerhalb von Nacaps:

- Es werden keine Aufträge an Auftragsverarbeiter*innen vergeben. Sämtliche Datenverarbeitung erfolgt innerhalb des Projektes.

8 Löschung und Anonymisierung

- Die personenbezogenen Daten werden entsprechend der vorherigen Beschreibung der Verarbeitung (siehe 7.) gelöscht bzw. anonymisiert.
- Die Anonymität der Befragten wird durch eine Kombination von statistischen, technischen und vertraglichen Maßnahmen gesichert (sogenannter Portfolio Ansatz; wird u.a. auch vom FDZ der National Educational Panel Study – NEPS – genutzt).
- Die Daten werden dann durch statistische Maßnahmen anonymisiert. Verwendet werden insbesondere Löschungen und Aggregationen von Informationen (Variablen). Sofern notwendig, werden darüber hinaus Substichprobenziehungen vorgenommen.
- Die Anonymisierung der Daten erfolgt in Abstimmung mit dem Datenschutzbeauftragten. Dabei werden die Angaben betrachtet, für die eine Wahrscheinlichkeit besteht, dass andere Datenquellen übereinstimmende Informationen über die Befragten enthalten, so dass eine Deanonymisierung durch eine Kombination der Angaben oder durch Heranspielen externer Informationen - wenn auch mit großem Aufwand - möglich wäre. Um eine eindeutige Zuordnung der Daten zu unterbinden, werden diese Schlüsselmerkmale – je nach Datenprodukt bzw. Zugangsweg – aggregiert oder gelöscht. Beispielsweise werden die Angaben zur Hochschule, zum Zeitpunkt des Promotionsabschlusses sowie zur Art des Promotionsprogramms gelöscht. Die offenen Angaben zum Promotionsfach werden zunächst vercodet und dann unterschiedlich stark aggregiert. Im On-Site- und Remote-Desktop-SUF werden Angaben zum Promotionsfach aggregiert zu DZHW-Fächergruppen freigegeben. Im Download-SUF und im Download-CUF erfolgt eine noch etwas stärkere Aggregation zu Destatis-Fächergruppen.
- Da sich nicht alle Hochschulen an der Befragung beteiligen und die Teilnahme der Befragten zudem freiwillig ist, kann bei eventuell auftretenden Übereinstimmungen im Datensatz mit identifizierbaren Personen kein Nachweis geführt werden, dass dieser Einzelfall sich dieser konkreten Person zuordnen lässt, da auf Grund der Ausfälle auf Hochschul- und Individualebene nicht festgestellt werden kann, dass diese Person an der Befragung teilgenommen hat und somit die Daten auf eine andere Person zutreffen.
- Da bei Fragen mit offener Antwortmöglichkeit die Gefahr besteht, dass Befragte bei eigentlich unbedenklichen Fragen kritische Informationen preisgegeben haben, die zu einer Identifikation führen könnten, werden offene Angaben entweder vercodet und (teilweise aggregiert) zur Verfügung gestellt, oder gelöscht.
- Eine Anonymisierung nach reinen Zahlengrößen erfolgt nicht, vielmehr wird die Wahrscheinlichkeit eingeschätzt, dass Angaben zur Deanonymisierung geeignet sind. Weltsprachen wie Englisch, Französisch oder Spanisch sind als Angaben zur Muttersprache z. B. nicht geeignet, Hinweise auf ein konkretes Herkunftsland zu geben. Daher kann hier auch mit kleineren Fallzahlen gearbeitet werden.
- Angaben, die auf subjektiven Wertungen und Einschätzungen der Befragten beruhen, werden nicht anonymisiert, da eine Wahrscheinlichkeit des Bestehens von anderen Datenquellen mit übereinstimmenden Informationen nicht besteht.
- Gesundheitsinformationen, für die eine zusätzliche Einverständniserklärung eingeholt wurde, dürfen im On-Site- und Remote-Desktop-SUF herausgegeben werden. Weitere Einzelinformationen zur Gesundheit, für die nicht explizit eine Einwilligung eingeholt wurde, sowie ggf. gemachte sensible Angaben z. B. zur sexuellen Orientierung oder politischen Einstellung, werden gelöscht.
- Im CUF werden zum einen im Vergleich zu den SUF-Varianten teils restriktivere statistische Anonymisierungsmaßnahmen auf Variablenebene vorgenommen, zum anderen wird eine per Zufallsauswahl gewonnene Substichprobe der Daten (25 % der Befragten) gezogen.