Deutsches Zentrum
DLR für Luft- und Raumfahrt

Forschungsprojekt „DLR Moving Lab – Projekt „Freemove“

Datenschutzkonzept

Das vorliegende Datenschutzkonzept beschreibt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen des DLR MovingLab.

Es beantwortet die sich daraus ergebenden Fragen zum Datenschutz und definiert technische und organisatorische Schutzmaßnahmen. Zentrale Punkte des Datenschutzkonzeptes sind die transparente Information sowie die Einverständniserklärung zur Erhebung und Verarbeitung personenbezogener Daten, die sich an die Teilnehmenden der Studie richtet. Die erhobenen Daten werden vom DLR entsprechend den Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Bundesdatenschutzgesetzes in seiner aktuellen Fassung (BDSG) nur für wissenschaftliche Zwecke erhoben und verarbeitet, wenn und soweit die Teilnehmenden der Studie hiermit ihr Einverständnis erklären.

Das vorliegende Datenschutzkonzept beschreibt die stattfindende Datenverarbeitung im Rahmen des Projektes „Freemove“.

Weitere Informationen, insbesondere zu den gesetzlichen Rechten der Teilnehmenden sowie Kontaktmöglichkeiten bei allen Fragen zum Datenschutz finden sich in den Datenschutzhinweisen, die den Teilnehmenden im Zusammenhang mit der Einverständniserklärung zur Kenntnis gegeben werden.

1. Projektbeschreibung und Forschungszweck der Datenerhebung

a. Kurzbeschreibung des Projektes „Freemove“

Ziel des Projektes „Freemove“ ist es, ein wissenschaftlich fundiertes Framework zu entwickeln, welches die Anforderungen an eine faire, nützliche, sichere und verständliche Bereitstellung von Bewegungsdaten für öffentliche und private Anwender:innen konkretisiert. Das Potential der Analyse von Bewegungsdaten ist enorm für die Bewältigung kritischer Probleme wie beispielsweise Epidemien und Katastrophen, aber auch für eine nachhaltige, menschzentrierte und umweltbewusste Stadt- und Verkehrsentwicklung. Dem stehen Herausforderungen, die mit der Verfügbarmachung solcher Bewegungsdaten verbunden sind, gegenüber: Der rechtlich wie ethisch erforderliche hohe Schutz der Privatsphäre von Personen verlangt anspruchsvolle mathematische und technische Anonymisierungsverfahren.

Mit dem DLR MovingLab werden Bewegungs- und Befragungsdaten zur Mobilität von Studierenden erhoben, mithilfe derer die im Projekt „Freemove“ entwickelten Verfahren der Anonymisierung und Synthetisierung erprobt und kalibriert werden können.

b. Kurzbeschreibung des Projektverantwortlichen

Das Forschungsprojekt wird in Verantwortung des **Deutschen Zentrum für Luft- und Raumfahrt e.V. (DLR), Institut für Verkehrsforschung, Rutherfordstraße 2, 12489 Berlin** (nachfolgend: „**DLR**“) durchgeführt.

2. Typisierung der Daten

Im Rahmen der Hauptphase werden verschiedene Datenkategorien erhoben und verarbeitet:

Datentyp	Kurzbeschreibung
Datentyp I	**Probandeninformationen (Teilnehmendendaten und Methodeninformationen)** Es handelt sich um persönliche Basisdaten der Probandinnen und Probanden (Alter, Kontaktdaten, demographische Daten, freiwillige Angaben), Angaben zu den Umständen der Probandenansprache (Zeitpunkt, Ort, Erfassungsmethode) sowie Zuordnungsdaten, anhand derer eine Probanden-ID einer bestimmten Probandin oder Proband zugeordnet werden kann.
Datentyp II	**Interviewdaten** Es handelt sich um Angaben der Probandinnen und Probanden aus individuellen Befragungen (telefonisch, persönlich oder elektronisch) und ggf. Gruppendiskussionen, die im Rahmen der Mobilitätsanalyse erfolgen.
Datentyp III	**Wegedaten** Es handelt sich um Daten über die im Wegetagebuch automatisch und manuell erfassten Wege einschließlich deren jeweiligen Start- und Zielpunkte, Routen, Etappen und ggf. POI; jeweils mit Start- und Zielzeitpunkten und Angaben zu den genutzten Verkehrsmitteln. Auch manuell von der Probandin oder dem Probanden per App oder Website oder von einer datenverarbeitenden Stelle vorgenommene manuelle Ergänzungen oder Korrekturen der bereits erfassten Wege sind Wegedaten.
Datentyp IV	**Validierungsdaten** Es handelt sich um Wegedaten, die von der Probandin oder dem Probanden im Rahmen einer Validierung der erfassten Wegedaten mitgeteilt werden (telefonisch, persönlich oder elektronisch).
Datentyp V	**Zugangsdaten** Es handelt sich um Daten, die aus technischen Gründen benötigt werden, damit die Probandin oder der Proband auf sein persönliches Teilnehmerkonto zugreifen kann bzw. mit denen er sich auf der Website oder in der App anmelden kann, z. B. E-Mail-Adressen, Codes, Benutzernamen, Passwörter, Tokens.
Datentyp VI	**Servicedaten** Es handelt sich um Angaben, die im Zusammenhang mit Supportanfragen der Probandinnen und Probanden, z. B. wegen Fehlfunktionen der App, anfallen.

3. Beteiligte natürliche und juristische Personen

Betroffene und Datengeber (einschließlich Datentypen)		
Probanden Hauptphase	PP	Probandinnen und Probanden, die im Rahmen der Hauptphase an der Mobilitätsanalyse teilnehmen und deren Wegedaten erfasst werden. • Probandeninformationen • Interviewdaten • Wegedaten • Validierungsdaten • Zugangsdaten • Nutzungsdaten
Datenverarbeitende Stellen		
Deutsches Zentrum für Luft- und Raumfahrt e. V., Institut für Verkehrsforschung, Rutherfordstr. 2, 12489 Berlin	DLR	Projektleitung und verantwortlich für die wissenschaftliche Begleitung, Teil der Forschungsgemeinschaft
Kooperationspartner	PT	- Hochschule für Technik und Wirtschaft Berlin (HTW) - Universität der Künste Berlin (UdK) - Freie Universität Berlin - Technische Universität Berlin
Dienstleister Computacenter AG & Co. oHG, LimeSurvey GmbH	DL	Support und Wartung von Servern des DLR mit temporärem Zugriff auf die Forschungsdaten

4. Welche Beteiligten haben mit welchen Daten in welcher Art zu tun?

Datentyp	PP	DLR	PT	DL
I	1	1,2,3,4,5	3,4,5	3
II	1	2,3,5	3,4,5	3
III	1	2,3,4,5	3,4,5	3
IV	1	2,3,5		3
V	1	2,3,4		3
VI	1	2,3,5		3

1: Preisgabe/Erzeugung von Daten (Datengeber)
2: Speicherung der Daten
3: Verarbeitung der Daten
4: Weitergabe der Daten
5: Veröffentlichung der Daten in aggregierter Form, z. B. im Rahmen des Schlussberichts

5. Erläuterung der Verarbeitungsschritte und Risikobewertung

Im Folgenden werden die Verarbeitungsschritte, die Zwecke und die getroffenen technischen und organisatorischen Maßnahmen für die einzelnen Datentypen beschrieben.

a. Datentyp I: Probandeninformationen

Im Rahmen der Mobilitätsanalyse spielen die Probandeninformationen für die wissenschaftliche Forschung eine wichtige Rolle. Die demographischen Angaben werden in Verbindung mit der Nutzung der App (Datentyp VI) und den Interviewdaten (Datentyp II) und dem DLR im Rahmen der Forschungsgemeinschaft wissenschaftlich ausgewertet.

Erhebung während der Rekrutierung

Im Rahmen der Rekrutierung werden die Probandinnen und Probanden über den Zweck und das Ziel des Forschungsvorhabens, die beteiligten Akteure, die Funktionsweise und Bedienung des jeweiligen Endgerätes zur Erhebung der Wegedaten informiert und es wird ggfs. die App initialisiert und installiert.

Anhand der Kurzinformation und der ausführlichen Datenschutzhinweise werden die Probandinnen und Probanden über die datenschutzrechtlichen Aspekte des Forschungsvorhabens umfassend informiert. Damit ist sichergestellt, dass die Probandinnen und Probanden vor Beginn der Datenverarbeitung transparent informiert sind und die Einwilligung in Kenntnis der maßgeblichen Aspekte der Datenverarbeitung abgeben.

Die die Erhebung und anschließende Verarbeitung zu wissenschaftlichen Zwecken rechtfertigende Einwilligung wird online erteilt. Auf die Erforderlichkeit der Abgabe einer datenschutzrechtlichen Einwilligung in die Datenverarbeitung zu Forschungszwecken wird hingewiesen. Diese Einwilligung ist erforderlich, da die App von den Probandinnen und Probanden genutzt werden, um detaillierte Standortdaten (Wegedaten) zu erheben, die die Qualität von Bewegungsprofilen erreichen werden. Die Formulierung der Einwilligung kann im Rahmen der Datenschutzhinweise vom Probanden jederzeit eingesehen werden. Die vollständige Information der Probandinnen und Probanden wird durch die Datenschutzerklärung der App und der Projektwebseite flankiert, in der auch die ausführlichen Datenschutzhinweise für die Studienteilnehmenden sowie die Einwilligung abgerufen werden können.

Im Rahmen der Datenschutzhinweise wird zudem das Pseudonymisierungskonzept erläutert, das der Ausgestaltung der Datenverarbeitung im Forschungsprojekt zugrunde liegt.

Die folgende Tabelle gibt einen detaillierten Überblick über die Daten, die in der Hauptphase erhoben werden.

Datenkategorien Probandeninformationen	Erläuterungen und Zwecke
Kontaktdaten	E-Mail-Adresse der Probandin oder des Probanden. Es handelt sich um die Kontaktdaten einer natürlichen Person. Die Kontaktdaten dienen der Kontaktaufnahme im Rahmen der Rekrutierung und ggf. der anschließenden Projektdurchführung und Einladung zu Gruppendiskussionen.
Sozio-demographische Merkmale	Alter, Geschlecht, Bildungsabschluss, Tätigkeit, Einkommen, Haushaltsgröße, Haushaltszusammensetzung. Es handelt sich hierbei um die Angaben der Probandin oder des Probanden, die Angaben sind personenbezogen. Die sozio-demographischen Merkmale werden im Rahmen der Auswertung des Tests und anschließend im Zusammenhang mit anderen Datenkategorien zu wissenschaftlichen Zwecken genutzt.

Speicherung der Probandeninformationen

Die Speicherung der Probandeninformationen der Probandinnen und Probanden erfolgt im DLR. Die Zweckbindung und die anschließende Löschung der projektbezogenen Probandendaten werden durch dieses Datenschutzkonzept und die Rechte- und Rollenkonzepte im DLR festgelegt.

Das DLR nutzt zur Speicherung von jeglichen Daten der Probandinnen und Probanden ausschließlich eigene Rechenzentren. Ein unbefugter Zugang durch Dritte zu dem System ist nicht möglich.

Die Daten werden im DLR auf IT-Systemen abgelegt, die von der Computacenter AG & Co. oHG betreut werden. Zwischen diesem Dienstleister und dem DLR bestehen aktuelle Auftragsverarbeitungsvereinbarungen gem. Art. 28 Abs. 3 DSGVO, die Zugriffe im Fall von Wartungsarbeiten sachgerecht regeln.

Bei Bedarf kann für diese Systeme eine Spezifikation der eingerichteten Schutzmaßnahmen geliefert werden.

Des Weiteren wird auch das datenschutzrechtliche Trennungsgebot umfassend beachtet: Die unmittelbar identifizierenden Angaben und insbesondere die Kontaktdaten der Probandinnen und Probanden werden getrennt von den sonstigen Probandeninformationen und sonstigen Datenkategorien gespeichert. Es bestehen lediglich interne IDs als Zuordnungsfunktion, so dass die weitere Speicherung der Wegedaten anhand dieses Pseudonyms erfolgen kann. Eine Speicherung von Probandeninformationen durch das im Auftrag des DLR tätigen IT-Support-Unternehmens ist, abgesehen von im Einzelfall erforderlichen, kurzfristigen Speicherungen im Rahmen von Wartungstätigkeiten, vertraglich ausgeschlossen.

Verarbeitung der Probandeninformationen

Die demographischen Angaben werden in Verbindung mit den Wegedaten und den Interviewdaten wissenschaftlich ausgewertet, um den Forschungszweck zu erreichen.

Vor Beginn der wissenschaftlichen Auswertung der Probandeninformationen durch die Kooperationspartner im Projekt Freemove werden die personenbezogenen Angaben von den erhobenen Wegedaten getrennt, indem eine zufällig vergebene individuelle Kennnummer, die jeder Probandin oder Proband fest zugewiesen wird (Probanden-ID) entfernt wird. Bei der Verwendung des für die wissenschaftliche Auswertung relevanten Teils der Probandeninformationen ist somit kein Rückschluss auf einzelne Personen möglich.

Die so anonymisierten Angaben werden zur weiteren Verarbeitung auf passwortgeschützten Speichersystemen im DLR abgelegt. Ein unbefugter Zugang durch Dritte zu dem System ist nicht möglich.

Alle Personen, die mit Probandeninformationen im Rahmen ihrer Tätigkeit in Berührung kommen, sind im Hinblick auf die datenschutzrechtlichen Sorgfaltspflichten geschult und schriftlich auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtet. Die Systeme und Prozesse im DLR unterliegen einem durchgängigen Prüfungskonzept des verantwortlichen Datenschutzbeauftragten des DLR.

Weitergabe der Probandeninformationen

Die Probandeninformationen können zum Zweck der Validierung und Reproduzierung von Forschungsergebnissen an andere, nicht im Vorhinein bekannte Wissenschaftlerinnen und Wissenschaftler weitergegeben werden. Der Zeitpunkt und der Umfang der Offenlegung der Daten ist durch die Anforderungen der Leitlinien guter wissenschaftlicher Praxis der Deutschen Forschungsgemeinschaft in der jeweils aktuellen Fassung zur Dokumentation von den für das Zustandekommen eines Forschungsergebnisses relevanten Informationen begrenzt. Die Daten werden dementsprechend nur dann und nur insoweit offengelegt, wie dies zur Validierung und Reproduzierung der Forschungsergebnisse erforderlich ist.

Dauer der Speicherung, Anonymisierung und Veröffentlichung der Probandeninformationen

Die Probandeninformationen werden bis zum Ende der Projektlaufzeit gespeichert. Während der Projektlaufzeit werden die Probandeninformationen unter Verwendung der Probanden-ID personenbezogen gespeichert, um die Validierung zu ermöglichen und die Ansprache einzelner Probandinnen oder Probanden zu ermöglichen, sofern dies aus Sicht des DLR zu Erreichung des wissenschaftlichen Zwecks erforderlich ist.

Bei Abschluss des Projektes liegen alle Probandeninformationen so anonymisiert vor, dass eine direkte und indirekte Zuordnung zu den personenbezogenen Daten unmöglich ist. Die Zuordnungstabellen, in denen persönliche Informationen der Probandinnen und Probanden und die Probanden-ID gespeichert sind, werden jeweils irreversibel gelöscht.

Die anonymisierten Daten werden entsprechend den Regeln des DLR zur Sicherung guter wissenschaftlicher Praxis auf Grundlage der „Vorschläge zur Sicherung guter wissenschaftlicher Praxis“ der DFG von 1998 i. d. F. von 2019 zehn Jahre lang nach Ende des Projektes, also bis zum 31.12.2033 auf einem Server des DLR gespeichert.

Abschließende Risikoeinschätzung zur Verarbeitung der Probandeninformationen

Das Verarbeitungskonzept bezüglich der Probandeninformationen berücksichtigt, dass aus Gründen des Studiendesigns eine Ansprache der Probandinnen und Probanden erforderlich werden kann, um bspw. Wege durch die Probandin oder den Probanden validieren zu lassen, Fragen zur Teilnahme am Projekt zu klären oder die Probandinnen und Probanden zu einer Gruppendiskussion oder sonstigen Befragung einzuladen. Aus diesem Grund werden die Probandeninformationen unter Einhaltung sachgerechter technischer und organisatorischer Maßnahmen durch das DLR gespeichert. Die

Verarbeitung erfolgt unter Beachtung des Trennungsgebotes und strikter Einhaltung der Zweckbindung. Für alle einzelnen Datenkategorien der Probandeninformationen wurden die Erforderlichkeit für die Verwirklichung des spezifischen Verarbeitungszwecks berücksichtigt. Die Methodeninformationen werden nur anhand der Probanden-ID beim DLR gespeichert, um den im Rahmen der Datenverarbeitung zu wissenschaftlichen Zwecken erforderlichen Vorrang der pseudonymisierten Verarbeitung zu gewährleisten. Dieses Pseudonymisierungskonzept stellt sicher, dass nach Abschluss der Erhebung eine sichere Anonymisierung der Probandeninformationen möglich ist.

Der Grundsatz der Datensparsamkeit wird beachtet. Es werden jeweils lediglich die Daten verarbeitet, die zur Erfüllung der jeweiligen Zwecke und insbesondere im Hinblick auf die wissenschaftliche Forschung erforderlich sind. Die vertraglichen Vereinbarungen stellen die Einhaltung der datenschutzrechtlichen Grundsätze sicher. Die Transparenz der Erhebung und Verarbeitung der Umfragedaten der Probandinnen und Probanden ist durch die Informationstexte auf der Website und in der App sichergestellt. Die Betroffenen können ihre datenschutzrechtlichen Rechte gegenüber dem DLR geltend machen und eine entsprechende Umsetzung der Rechte bei Eingang einer Anfrage ist operativ sichergestellt (insbesondere Auskunft anhand Probanden-ID). Ein im Einzelfall zu Wartungszwecken erforderlicher Zugriff durch den IT-Support-Dienstleister des DLR ist datenschutzkonform ausgestaltet. Wartungszugriffe auf personenbezogene Daten erfolgen ausschließlich im Rahmen einer Auftragsverarbeitung gem. Art. 28 Abs. 3 DSGVO.

Die Einwilligungserklärung der Probandinnen und Probanden entspricht den Vorgaben gem. Art. 7 DSGVO.

b. Datentyp II: Interviewdaten

Es sind mit den Probandinnen und Probanden Befragungen und ggf. Gruppendiskussionen geplant. Einladungen werden durch das DLR anhand der dort vorhandenen Kontaktdaten durchgeführt. Die Interviewdaten werden anhand der Probanden-ID zu den vorhandenen Datensätzen gespeichert. Eine vollständige Anonymisierung ist erst nach Abschluss der Erhebungsphase möglich, da die Angaben zu Zwecken der Auswertung zu den sonstigen Datensätzen gespeichert werden müssen, um den Forschungszweck zu realisieren. Bei der Einladung zu den Befragungen und Gruppendiskussionen werden die Probandinnen und Probanden über die genauen Abläufe und auch die datenschutzrechtlichen Vorkehrungen gesondert informiert. Die Befragungen und Gruppendiskussionen werden möglichst unter Verzicht auf vollständige Namen und sonstige unmittelbare identifizierende Angaben durchgeführt, um das vorhandene Pseudonymisierungskonzept nicht zu gefährden. Die Befragungen und Gruppendiskussionen werden ausschließlich durch auf die Vertraulichkeit im Umgang mit personenbezogenen Daten verpflichtete Mitarbeiter des DLR und der Kooperationspartner durchgeführt.

Datenkategorien „Interviewdaten“	**Erläuterungen und Zwecke**
Angaben zu Fragestellungen aus dem inhaltlichen Kontext des Projektes Freemove	Verständlichkeit der Datenschutzdokumentationen und Auswirkungen dieser auf die Teilnahme am Tracking Es handelt sich hierbei um Angaben der Probandin oder des Probanden, die Angaben sind zwar personenbeziehbar, sie werden jedoch unter Pseudonym erhoben und gespeichert (Probanden-ID). Diese Angaben werden im Zusammenhang mit anderen Datenkategorien zu wissenschaftlichen Zwecken genutzt.

Angaben zur Nutzung zur Gestaltung der App	Zufriedenheit mit der Häufigkeit des Einsatzes, Bedienungsqualität der App und die Nutzbarkeit der App-Funktionen, Kritik und Verbesserungsvorschläge. Es handelt sich hierbei um Angaben der Probandin oder des Probanden, die Angaben sind zwar personenbeziehbar, sie werden jedoch unter Pseudonym erhoben und gespeichert (Probanden-ID). Diese Angaben werden im Zusammenhang mit anderen Datenkategorien zu wissenschaftlichen Zwecken genutzt.
Angaben zum Projektablauf	Allgemeine Zufriedenheit mit der Erhebung und der Wegeerfassung, Kritik, Verbesserungsvorschläge, Bewertung der Kommunikationsqualität. Es handelt sich hierbei um Angaben der Probandin oder des Probanden, die Angaben sind zwar personenbeziehbar, sie werden jedoch unter Pseudonym erhoben und gespeichert (Probanden-ID). Die Angaben zum Projektablauf werden im Zusammenhang mit anderen Datenkategorien zu wissenschaftlichen Zwecken und zur Verbesserung der Projektgestaltung genutzt.

Die Interviewdaten werden durch das DLR protokolliert und auf passwortgeschützten Speichersystemen des DLR abgelegt. Zugriff auf diese Daten haben die Projektmitarbeiter des DLR, die die Interviews durchführen und auswerten.

Weitergabe der Interviewdaten

Die Interviewdaten können zum Zweck der Validierung und Reproduzierung von Forschungsergebnissen an andere, nicht im Vorhinein bekannte Wissenschaftlerinnen und Wissenschaftler weitergegeben werden. Der Zeitpunkt und der Umfang der Offenlegung der Daten ist durch die Anforderungen der Leitlinien guter wissenschaftlicher Praxis der Deutschen Forschungsgemeinschaft in der jeweils aktuellen Fassung zur Dokumentation von den für das Zustandekommen eines Forschungsergebnisses relevanten Informationen begrenzt. Die Daten werden dementsprechend nur dann und nur insoweit offengelegt, wie dies zur Validierung und Reproduzierung der Forschungsergebnisse erforderlich ist.

Dauer der Speicherung, Anonymisierung und Veröffentlichung der Interviewdaten

Die Interviewdaten werden bis zum Ende der Projektlaufzeit gespeichert. Die Speicherung erfolgt nur unter Pseudonym (Probanden-ID).

Nach Abschluss des Projektes werden die Interviewdaten so anonymisiert, dass eine direkte und indirekte Zuordnung zu den personenbezogenen Daten unmöglich gemacht wird. Zuordnungstabellen werden irreversibel gelöscht.

Die anonymisierten Daten werden entsprechend den Regeln des DLR zur Sicherung guter wissenschaftlicher Praxis auf Grundlage der „Vorschläge zur Sicherung guter wissenschaftlicher Praxis“ der DFG von 1998 i. d. F. von 2019 zehn Jahre lang nach Ende des Projektes, also bis zum 31.12.2033, auf einem Server des DLR gespeichert.

Interviewdaten werden ausschließlich in aggregierter und anonymisierter Form veröffentlicht. Eine Veröffentlichung personenbezogener Daten (z. B. in Form von Zitaten unter Namensnennung) erfolgt nicht.

Abschließende Risikoeinschätzung zur Verarbeitung der Interviewdaten

Die Interviewdaten sind nicht grundsätzlich von erhöhter Sensibilität. Aufgrund der potentiell offenen Fragestellungen, die auch auf subjektive Einschätzungen abzielen, müssen jedoch auch die Interviewdaten unter Einhaltung sachgerechter technischer und organisatorischer Maßnahmen durch das DLR verarbeitet werden. Die Verarbeitung erfolgt unter Beachtung des Trennungsgebotes und strikter Einhaltung der Zweckbindung. Die Transparenz der Erhebung und Verarbeitung der Interviewdaten wird durch die gesonderte Information bei der Einladung zu den Interviews und Gruppendiskussionen sichergestellt. In diesem Zusammenhang wird auch die Freiwilligkeit der Teilnahme ausdrücklich erläutert werden. Die Betroffenen können ihre datenschutzrechtlichen Rechte gegenüber dem DLR geltend machen und eine entsprechende Umsetzung der Rechte bei Eingang einer Anfrage ist auch operativ sichergestellt (insbesondere Auskunft anhand Probanden-ID).

c. Datentyp III: Wegedaten

Um die Erfassung von Wegedaten zu ermöglichen, stehen den Probandinnen und Probanden die App und die Website zur Verfügung. Über die App können Wegedaten sowohl automatisch als auch manuell erfasst werden. Über die Website können Wegedaten nur manuell erfasst werden.

Die App wird auch im Rahmen der Hauptphase im Auftrag des DLR durch einen externen Dienstleister weiterentwickelt. Die Entwicklerin oder der Entwickler liefert nur Updates für die App, eine Berührung mit den während des Forschungsprojektes erhobenen und verarbeiteten Wegedaten ist ausgeschlossen. Die GPS-Daten-Logger senden über eine Mobilfunk-Schnittstelle Daten ausschließlich an Datenserver im DLR.

Datenkategorie „Wegedaten“	**Erläuterungen und Zwecke**
Verkehrswegedaten	Start- und Zielpunkte, Routen, Etappen und ggf. POI; jeweils mit Start- und Zielzeitpunkten Anzahl und Länge der zurückgelegten Wege, GPS-Positionierung auf diesen Wegen und Angaben zu den genutzten Verkehrsmitteln. Es handelt sich bei den Wegedaten um Angaben, die sich auf die Probandin oder den Probanden beziehen. Die Angaben werden nur unter Pseudonym gespeichert (Nutzer-ID). Die Wegedaten werden im Zusammenhang mit anderen Datenkategorien zu wissenschaftlichen Zwecken genutzt.

Die MovingLab App wird über die regulären App-Stores (Google Play Store und Apple App-Store) öffentlich zur Verfügung gestellt und mittels eines teilnehmerindividuellen ID-Tokens (der die Probandin oder den Probanden durch das DLR bei der Rekrutierung mitgeteilt wird) bei der Initialisierung freigeschaltet. Dadurch wird sichergestellt, dass die Datenerfassung durch die App jeweils einem Datensatz einer Probandin oder einem Probanden zugeordnet werden kann. Probandinnen und Probanden nutzen zur Anmeldung an der App einen Anmeldenamen und ein Startpasswort, dass Ihnen im Zuge der Einladung zur Teilnahme mitgeteilt wird. Die App erzwingt bei der Erstanmeldung das Neusetzen des Startpasswortes. Die App ist so ausgestaltet, dass die Funktionen und die damit verbundene Datenverarbeitung für die Nutzerin oder den Nutzer intuitiv und transparent sind und die

Datenverarbeitung durch die Nutzerin oder den Nutzer autonom gesteuert werden kann. Ist die Erfassung der Standortdaten aktiv, wird dies transparent angezeigt. Die Nutzerin oder der Nutzer kann überdies die Erfassung jederzeit beenden und einen erfassten Weg in einer Kartenansicht nachvollziehen.

Die Nutzung der App dient der Erhebung weiterer Angaben über die zurückgelegten Wege und Nutzung des jeweiligen Verkehrsmittels. Die Funktionen der App und die damit verbundene Datenverarbeitung werden in der appspezifischen Datenschutzerklärung transparent aufgeschlüsselt. Es wird insbesondere die Erhebung und Verarbeitung der Wegedaten erläutert und erklärt, wie diesbezüglich eine Trennung von den unmittelbar personenbezogenen Angaben realisiert wird.

Die Wegedaten werden anhand der Probanden-ID gespeichert, kein anderer Beteiligter außer den Projektmitarbeitern des DLR hat grundsätzlich Zugriff auf die Wegedaten. Die Ablage der Wegedaten erfolgt auf passwortgeschützten Speichersystemen des DLR.

Anfragen von Probandinnen und Probanden gehen beim DLR ein und werden anhand der Probanden-ID durch das DLR inhaltlich umgesetzt. So können insbesondere sowohl Löschungs- als Auskunftsansprüche erfüllt werden.

Die Wegedaten werden vom DLR ausschließlich zu Forschungszwecken verwendet.

Weitergabe der Wegedaten

Die Wegedaten können zum Zweck der Validierung und Reproduzierung von Forschungsergebnissen an andere, nicht im vorhinein bekannte Wissenschaftlerinnen und Wissenschaftler weitergegeben werden. Der Zeitpunkt und der Umfang der Offenlegung der Daten ist durch die Anforderungen der Leitlinien guter wissenschaftlicher Praxis der Deutschen Forschungsgemeinschaft in der jeweils aktuellen Fassung zur Dokumentation von den für das Zustandekommen eines Forschungsergebnisses relevanten Informationen begrenzt. Die Daten werden dementsprechend nur dann und nur insoweit offengelegt, wie dies zur Validierung und Reproduzierung der Forschungsergebnisse erforderlich ist.

Dauer der Speicherung, Anonymisierung und Veröffentlichung der Daten

Die Wege- und Validierungsdaten werden bis zum Ende der Projektlaufzeit gespeichert. Die Speicherung erfolgt nur unter Pseudonym.

Nach Abschluss des Projektes werden die Wegedaten so anonymisiert, dass eine direkte und indirekte Zuordnung zu den personenbezogenen Daten unmöglich gemacht wird.

Die anonymisierten Daten werden entsprechend den Regeln des DLR zur Sicherung guter wissenschaftlicher Praxis auf Grundlage der „Vorschläge zur Sicherung guter wissenschaftlicher Praxis“ der DFG von 1998 i. d. F. von 2019 zehn Jahre lang nach Ende des Projektes, also bis zum 31.12.2033, auf einem Server des DLR gespeichert.

Die Wegedaten werden ausschließlich in aggregierter und anonymisierter Form veröffentlicht.

Abschließende Risikoeinschätzung zur Verarbeitung der Wegedaten

Die Wegedaten werden direkt bei den Probandinnen und Probanden erhoben. Die Informiertheit der Probandinnen und Probanden und allgemeine Transparenz der Datenverarbeitung wird gewährleistet. Die Tatsache, dass die Probandinnen und Probanden des Forschungsvorhabens unterschiedlichen Nutzertypologien zuzuordnen sind, ist im Rahmen der datenschutzrechtlichen Ausgestaltung der Informationstexte und der App- und Websitegestaltung sachgerecht berücksichtigt worden. Die Probandinnen und Probanden werden ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen. Auf

die Sensibilität der sich aus den Wegedaten potentiell ergebenden Bewegungsprofile wird in den Datenschutzhinweisen ausdrücklich hingewiesen.

Die Einhaltung sachgerechter technischer und organisatorischer Maßnahmen durch das DLR ist gewährleistet. Die Zweckbindung und der Erforderlichkeitsgrundsatz werden eingehalten. Die Betroffenen können ihre datenschutzrechtlichen Rechte gegenüber dem DLR geltend machen und eine entsprechende Umsetzung der Rechte bei Eingang einer Anfrage ist auch operativ sichergestellt (insbesondere Auskunft anhand Probanden-ID).

Die App ist datenschutzfreundlich ausgestaltet, sie lässt insbesondere die aktiv ablaufende Erfassung der Standortdaten gut erkennen und erlaubt dem Nutzer jederzeit die Beendigung der Erhebung. Die Datenschutzerklärung stellt die transparente Information der Nutzer sicher.

d. Datentyp IV: Validierungsdaten

Validierungsdaten beziehen sich auf die in vorstehendem Absatz (c.) beschriebenen Wegedaten. Sie dienen zu deren Verifizierung und ggf. Ergänzung bzw. Korrektur. Validierungsdaten werden von der Probandin oder von dem Probanden per App oder Website eingegeben.

Die App wird im Auftrag des DLR durch einen externen Dienstleister weiterentwickelt. Der Entwickler liefert nur Updates für die App, eine Berührung mit den während des Forschungsprojektes erhobenen und verarbeiteten Wegedaten ist ausgeschlossen.

Datenkategorie „Validierungsdaten“	**Erläuterungen und Zwecke**
Validierungsdaten	Manuell von der Probandin oder vom Probanden per App oder Website oder im Rahmen von Validierungen vorgenommene manuelle Ergänzungen oder Korrekturen der bereits erfassten Wege sind Validierungsdaten. Es handelt sich bei den Validierungsdaten um Angaben, die sich auf die Probandin oder auf den Probanden beziehen. Die Angaben werden nur unter Pseudonym gespeichert (Nutzer-ID). Die Validierungsdaten werden im Zusammenhang mit anderen Datenkategorien zu wissenschaftlichen Zwecken genutzt.

Die MovingLab App wird über die regulären App-Stores (Google Play Store und Apple App-Store) öffentlich zur Verfügung gestellt und mittels eines teilnehmerindividuellen ID-Tokens (der den Probandinnen und Probanden durch das DLR bei der Rekrutierung mitgeteilt wird) bei der Initialisierung freigeschaltet. Dadurch wird sichergestellt, dass die Datenerfassung durch die App jeweils einem Datensatz einer Probandin oder eines Probanden zugeordnet werden kann. Probandinnen und Probanden nutzen zur Anmeldung an der App einen Anmeldenamen und ein Startpasswort, dass Ihnen im Zuge der Einladung zur Teilnahme mitgeteilt wird. Die App erzwingt bei der Erstanmeldung das Neusetzen des Startpasswortes. Die App ist so ausgestaltet, dass die Funktionen und die damit verbundene Datenverarbeitung für die Nutzerin oder den Nutzer intuitiv und transparent sind und die Datenverarbeitung durch den Nutzer autonom gesteuert werden kann. Ist die Erfassung der Standortdaten aktiv, wird dies transparent angezeigt. Die Nutzerin oder der Nutzer kann überdies die Erfassung jederzeit beenden und einen erfassten Weg in einer Kartenansicht nachvollziehen.

Die Nutzung der App dient der Erhebung weiterer Angaben über die zurückgelegten Wege und Nutzung des jeweiligen Verkehrsmittels. Die Funktionen der App und die damit verbundene Datenverarbeitung werden in der appspezifischen Datenschutzerklärung transparent aufgeschlüsselt. Es wird insbesondere die Erhebung und Verarbeitung der Wegedaten erläutert und erklärt, wie diesbezüglich eine Trennung von den unmittelbar personenbezogenen Angaben realisiert wird. Da sich die Validierungsdaten auf die Wegedaten beziehen, wird durch die Information über die Wegedaten gleichzeitig über den Zweck der Verarbeitung der Validierungsdaten informiert.

Die Validierungsdaten werden anhand der Probanden-ID gespeichert, keine andere Beteiligte oder kein anderer Beteiligter außer den Projektmitarbeiterinnen und Projektmitarbeitern des DLR hat grundsätzlich Zugriff auf die Validierungsdaten. Die Ablage der Validierungsdaten erfolgt auf passwortgeschützten Speichersystemen des DLR.

Anfragen von Probandinnen und Probanden gehen beim DLR ein und werden anhand der Probanden-ID durch das DLR inhaltlich umgesetzt. So können insbesondere sowohl Löschungs- als Auskunftsansprüche erfüllt werden.

Die Validierungsdaten werden vom DLR ausschließlich zu Forschungszwecken verwendet.

Dauer der Speicherung, Anonymisierung und Veröffentlichung der Daten

Die Validierungsdaten werden bis zum Ende der Projektlaufzeit gespeichert. Die Speicherung erfolgt nur unter Pseudonym.

Nach Abschluss des Projektes werden die Validierungsdaten so anonymisiert, dass eine direkte und indirekte Zuordnung zu den personenbezogenen Daten unmöglich gemacht wird.

Die anonymisierten Daten werden entsprechend den Regeln des DLR zur Sicherung guter wissenschaftlicher Praxis auf Grundlage der „Vorschläge zur Sicherung guter wissenschaftlicher Praxis“ der DFG von 1998 i. d. F. von 2019 zehn Jahre lang nach Ende des Projektes, also bis zum 31.12.2033, auf einem Server des DLR gespeichert.

Die Validierungsdaten werden ausschließlich in aggregierter und anonymisierter Form veröffentlicht.

Abschließende Risikoeinschätzung zur Verarbeitung der Validierungsdaten

Die Validierungsdaten werden direkt bei den Probandinnen und Probanden erhoben. Die Informiertheit der Probandinnen und Probanden und allgemeine Transparenz der Datenverarbeitung wird gewährleistet. Die Tatsache, dass die Probandinnen und Probanden des Forschungsvorhabens unterschiedlichen Nutzertypologien zuzuordnen sind, ist im Rahmen der datenschutzrechtlichen Ausgestaltung der Informationstexte und der App- und Websitegestaltung sachgerecht berücksichtigt worden. Die Probandinnen und Probanden werden ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen.

Die Einhaltung sachgerechter technischer und organisatorischer Maßnahmen durch das DLR ist gewährleistet. Die Zweckbindung und der Erforderlichkeitsgrundsatz werden eingehalten. Die Betroffenen können ihre datenschutzrechtlichen Rechte gegenüber dem DLR geltend machen und eine entsprechende Umsetzung der Rechte bei Eingang einer Anfrage ist auch operativ sichergestellt (insbesondere Auskunft anhand Probanden-ID).

Die Projekt-App ist datenschutzfreundlich ausgestaltet, sie lässt insbesondere die aktiv ablaufende Erfassung der Standortdaten gut erkennen und erlaubt der Nutzerin oder dem Nutzer jederzeit die Beendigung der Erhebung. Die Datenschutzerklärung stellt die transparente Information der Nutzerinnen und Nutzer sicher.

e. Datentyp V: Zugangsdaten

Es handelt sich um Daten, die aus technischen Gründen benötigt werden, damit die Probandin oder der Proband auf sein persönliches Teilnehmerkonto zugreifen kann bzw. mit denen sie oder er sich auf der Website oder in der App anmelden kann, hier Benutzernamen und Passwörter.

Die Probandinnen und Probanden werden im Rahmen der Rekrutierung bei der Initialisierung der Projekt-App durch transparente Dokumente unterstützt. Das DLR teilt der Probandin oder dem Probanden einen teilnehmerindividuellen Benutzernamen zu. Die Zuordnung des Benutzernamens zu den Teilnehmerdaten wird getrennt von den Wegedaten gespeichert (siehe Ziffer 5.a.). Das DLR stellt der Probandin oder dem Probanden ein Startpasswort zur Verfügung. Die Probandin oder der Proband wählt bei der Initialisierung ein eigenes Passwort aus, dass den übrigen Beteiligten nicht bekannt ist, es wird nicht im Klartext gespeichert. Eine weitere Verarbeitung der Zugangsdaten erfolgt nicht. Kommuniziert die Probandin oder der Proband unter Verwendung seiner E-Mail-Adresse mit dem DLR (wenn er sich an movinglab@dlr.de wendet), um ein Problem bei der Verwendung der App zu klären, wird die E-Mail-Adresse zu diesem Zweck von dem DLR verarbeitet. Eine Weitergabe erfolgt nicht.

Dauer der Speicherung, Anonymisierung und Veröffentlichung der Daten

Die Zugangsdaten (Passwort, ID-Token, E-Mail-Adresse) werden bis zum Abschluss der Hauptphase gespeichert und danach gelöscht. Es gelten die Maßgaben zum Pseudonymisierungskonzept gem. Ziffer 5 a). Zur Speicherdauer von Zugangsdaten, die im Rahmen von technischen Rückfragen erhoben und gespeichert werden, siehe sogleich Ziffer 5 e).

Abschließende Risikoeinschätzung zur Verarbeitung der Zugangsdaten

Das Konzept zum Umgang mit den Zugangsdaten ist durch Nutzerautonomie und Datensparsamkeit geprägt. Die Vergabe des Startpasswortes und anschließende eigene Wahl eines nutzereigenen Passwortes entspricht einer sachgerechten und nutzerfreundlichen Gestaltung, die zugleich ein hohes Maß an Zugriffsschutz bietet.

Die Verarbeitung der E-Mail-Adresse im Rahmen der Klärung von (technischen) Rückfragen zur App-Nutzung ist transparent ausgestaltet. Die Probandin oder der Proband kann nachvollziehen, an wen sie oder er sich wendet; das anschließende Weitergabekonzept gewährleistet, dass stets nur der erforderliche Teil einer Anfrage an die weiteren Beteiligten weitergegeben wird.

Die Verarbeitung der Zugangsdaten erfolgt nur im unbedingt erforderlichen Umfang. Eine Verwendung der Zugangsdaten zu anderen Zwecken als der Umsetzung des Forschungsprojektes erfolgt nicht.

f. Datentyp VI: Servicedaten

Zum Zwecke der Klärung von Rückfragen und technischen Problemen können sich Probandinnen und Probanden über die E-Mail-Adresse movinglab@dlr.de an das DLR wenden. Technische Supportanfragen werden dann anonymisiert an die Technikerinnen und Techniker der IT-Systeme weitergegeben und von diesen bearbeitet und protokolliert. Diese anonymen Protokolle dienen der Identifizierung von Optimierungsbedarf des Gesamtsystems des MovingLab, und sie werden im Hinblick auf die Mobilitätsanalyse auch zu wissenschaftlichen Zwecken ausgewertet. Die Technikerinnen und Techniker haben im Rahmen der Klärung von technischen Rückfragen keinerlei Berührung mit den sonstigen Datenkategorien. Die Ablage der Protokolle erfolgt auf passwortgeschützten Speichersystemen des DLR (gesonderte Extranet-Teamsite). Zugriff haben die Projektmitarbeiterinnen und Projektmitarbeiter des DLR.

Dauer der Speicherung, Anonymisierung und Veröffentlichung der Daten

Die ggf. mit den Servicedaten zusammenhängende Kommunikation mit den Probandinnen und Probanden wird bis zur Erledigung des Supportfalls gespeichert und danach gelöscht.

Die Protokolle werden bis zum Ende der Projektlaufzeit gespeichert. Die Speicherung erfolgt nur unter Pseudonym. Nach Abschluss des Projektes werden die Protokolle so anonymisiert, dass eine direkte und indirekte Zuordnung zu den personenbezogenen Daten unmöglich gemacht wird.

Die anonymisierten Daten werden entsprechend den Regeln des DLR zur Sicherung guter wissenschaftlicher Praxis auf Grundlage der „Vorschläge zur Sicherung guter wissenschaftlicher Praxis" der DFG von 1998 i. d. F. von 2019 zehn Jahre lang nach Ende des Projektes, also bis zum 31.12.2033, auf einem Server des DLR gespeichert.

Abschließende Risikoeinschätzung zur Verarbeitung der Servicedaten

Die Servicedaten dienen der möglichst reibungslosen operativen Durchführung der Projektteilnahme. Eine Zusammenführung der Servicedaten mit den sonstigen Datenkategorien ohne Mithilfe des DLR ist nicht möglich. Mögliche Kommunikationsdaten (z. B. E-Mail-Verkehr zu einzelnen technischen Problemen, die Namen und Kontaktdaten enthalten können) werden umgehend nach Abschluss des Supportfalls gelöscht. Die schriftliche Verpflichtung der Mitarbeiterinnen und Mitarbeiter des DLT auf die Einhaltung der datenschutzrechtlichen Grundsätze und die Wahrung der Vertraulichkeit im Umgang mit personenbezogenen Daten flankiert die Sicherung eines hohen Datenschutzniveaus.

6. Abschließende Risikoeinschätzung zur Datenverarbeitung im Rahmen des Forschungsprojektes „Freemove"

Die Datenverarbeitung im Rahmen des Projektes „Freemove" ist streng an den datenschutzrechtlichen Grundprinzipien ausgerichtet. Die Grundsätze der Erforderlichkeit, Datensparsamkeit und Transparenz gegenüber den Beteiligten werden konsequent eingehalten. Alle Verarbeitungsschritte sind datenschutzrechtlich durch den Forschungszweck gerechtfertigt; es werden stets sachgerechte technische und organisatorische Maßnahmen umgesetzt, die auch in den Vereinbarungen mit den Beteiligten verbindlich vereinbart wurden. Die Möglichkeiten zur Identifizierung der Probanden sind durch die Verwendung von Pseudonymen und Anonymisierungsschritten soweit technisch und organisatorisch möglich begrenzt. Diese sachgerechten technischen und organisatorischen Maßnahmen stellen geeignete Garantien für die Rechte und Freiheiten der Betroffenen dar. Das Anonymisierungskonzept entspricht insofern vollumfänglich den gesetzlichen Vorgaben.

Die Rechte der Betroffenen sind gewahrt. Insbesondere wird durch die bereitgestellten Informationsmaterialien gewährleistet, dass die Betroffenen die Datenverarbeitung schon vor Beginn der Erhebung nachvollziehen können. Bei der Gestaltung der App und der Website wurde sichergestellt, dass alle zu erhebenden Daten dem Forschungszweck dienen und die Verarbeitung jederzeit transparent erfolgt.

Die Veröffentlichung von Forschungsergebnissen oder Forschungsdaten erfolgt ausschließlich in anonymer Form. Personenbezogene Daten der Beteiligten werden nicht veröffentlicht, es sei denn die jeweiligen Betroffenen haben gesondert und ausdrücklich in die Veröffentlichung eingewilligt.

Die Rechte und Freiheiten der Betroffenen im Rahmen des Forschungsprojektes „Freemove" sind somit sachgerecht gewahrt.

***