

Datenschutzkonzept der Forschungsstudie PIPS

Partizipative Interaktionen in Pflege- und Schlafsituationen

Projektleitung: Prof. Dr. Karsten Krauskopf
Prof. Dr. Frauke Hildebrandt

Projektmitarbeitende: Christine Mager
Annika Hänsch
Hannah Merkel

Stand: September 2025

Inhalt

1 Präambel	2
2 Akquise und Einverständnis einholen	3
2.1 Verarbeitung von Kontaktdaten im Akquiseprozess	4
2.2 Inhalt und rechtlicher Bezug des Informationspakets für Eltern und Fachkräfte....	4
2.2.1 Informationen und Einverständniserklärungen für Eltern	4
2.2.2 Informationen und Einverständniserklärungen für Fachkräfte	6
3 Studiendurchführung	7
3.1 Vorbereitung der Durchführung	7
3.1.1 Belehrung und Selbstverpflichtung der Mitarbeitenden im Forschungsteam	7
3.2 Beschreibung der Erhebungsabläufe.....	7
3.2.1 Erhebung einrichtungsbezogener Kontextdaten	7
3.2.1 Fragebögen	8
3.2.2 Videografie	9
3.2.3 Live-Beobachtungen	11
3.2.4 Interviews.....	11
3.2.5 Eye-Tracking	11
4 Datenspeicherung, -auswertung, -aufbewahrung und -löschung	12
4.1 Datenspeicherung und -aufbewahrung	12
4.2 Datenauswertung	13
4.3 Datenlöschung	15
4.3.1 Datenlöschung bei Widerruf der Einwilligung	15
5 Datennutzung	16
5.1 Nutzung von Daten für wissenschaftliche Veröffentlichungen.....	16
5.2 Nutzung von Daten durch Studierende	16
5.3 Veröffentlichung von Daten und Nachnutzung der Daten durch Dritte	16
5.3.1 Veröffentlichung von Videodaten	17
5.4 Nachnutzung der Daten für Fortbildungszwecke	17
Anhang.....	19
1 Umgang mit Datenschutzvorfällen	19
2 Dokumentierte Vorgehensweisen bei unerwünschten Aufnahmen	20
2.1 Vorlage Löschprotokoll im Datenschutzfall	22
3 Child Safeguarding und Kinderschutz.....	23

1 Präambel

Partizipative Interaktionen in Pflege- und Schlafsituationen (PIPS) ist ein Forschungsprojekt unter der Leitung von Prof. Dr. Karsten Krauskopf und Prof. Dr. Frauke Hildebrandt an der Fachhochschule Potsdam. Die AWO Kinder- und Jugendhilfe Potsdam gGmbH fungiert dabei als Praxispartner. Gefördert wird das Vorhaben vom Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ).

Im Zentrum der Studie steht die Untersuchung der aktuellen Praxis in der Betreuung von Kindern unter drei Jahren, mit besonderem Fokus auf die partizipative Gestaltung von Pflege- und Schlafsituationen im Krippenalltag. Ziel des Projekts ist es, ein wissenschaftlich fundiertes Konzept zu entwickeln, das Fachkräfte in der Umsetzung partizipativer Interaktionen in sensiblen Alltagssituationen unterstützt.

Hierfür werden bundesweit Fachkraft-Kind-Interaktionen videobasiert erfasst und analysiert. Ergänzt wird die Untersuchung durch Fragebögen, Interviews sowie den Einsatz von mobilem Eye-Tracking zur Erhebung professioneller Wahrnehmungsprozesse. Methodisch lehnt sich das Projekt an die BiKA-Studie an und erweitert diese um innovative Perspektiven der Blickbewegungsforschung sowie der responsiven pädagogischen Haltung.

Ein zentrales Anliegen von PIPS ist die praxisnahe Weiterentwicklung professionellen Handelns in der frühkindlichen Bildung. Die Ergebnisse der Studie fließen in die Entwicklung von offenen Bildungsmaterialien (Open Educational Resources) und videobasierten Fortbildungseinheiten ein, die langfristig in die Aus- und Weiterbildung pädagogischer Fachkräfte integriert werden sollen.

PIPS verbindet wissenschaftliche Forschung mit technologischer Innovation und leistet damit einen Beitrag zur Stärkung der Partizipation von Kleinkindern in der Kindertagesbetreuung.

Vor dem Hintergrund der in PIPS eingesetzten Methoden und der Nähe zur pädagogischen Praxis ist es ein zentrales Anliegen aller Beteiligten, mit den erhobenen Daten verantwortungsvoll und sorgfältig umzugehen. Dies umfasst insbesondere den vertraulichen Umgang mit sensiblen Informationen innerhalb des Projekts sowie die verpflichtende Schulung sämtlicher Mitarbeitenden, Studierenden und Honorarkräfte, die im Rahmen der PIPS-Studie mit Studiendaten in Kontakt kommen, im Bereich des Child-Safeguardings und Kinderschutzes (siehe Anhang 4). Darüber hinaus zählen die transparente Gestaltung aller relevanten Prozesse, die nachvollziehbare Dokumentation der Datennutzung sowie – in Fällen, in denen eine Einsichtnahme durch Externe nicht möglich oder zulässig ist – eine begründete Einschränkung von Zugriffsrechten zu den grundlegenden Prinzipien des Projekts. Die Erhebung soll dabei so sparsam wie möglich erfolgen, sinnvoll sein und die Wahrung der Persönlichkeitsrechte des Einzelnen sicherstellen. In diesem Sinne wird nachfolgend aufgeführt, welche internen Vorgehensweisen beschlossen wurden, um die Erhebung, Auswertung und Nutzung von Daten in der PIPS-Studie verantwortungsvoll zu gestalten.

Dieses Datenschutzkonzept beschreibt das grundlegende Vorgehen der Projektgruppe PIPS und wurde im Mai 2025 verfasst. Es wurde dem Datenschutzbeauftragten Herrn Sven Hirsch am 23.05.2025 vorgelegt und am 06.06.2025 sowie 12.09.2025 überarbeitet.

2 Akquise und Einverständnis einholen

Die Teilnahme an der PIPS-Studie ist freiwillig und setzt das explizite Einverständnis aller beteiligten Personen (pädagogische Fachkräfte, Eltern/ Sorgeberechtigte stellvertretend für die Kinder) sowie der Kitaverantwortlichen (Leitung und ggf. Träger) voraus. Dieses Einverständnis umfasst auch die datenschutzrechtliche Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO zur Verarbeitung personenbezogener Daten im Rahmen der Studie. Alle Teilnehmenden werden zuvor umfassend über Zweck, Umfang und Dauer der Datenverarbeitung sowie ihre Rechte, insbesondere das Recht auf Widerruf der Einwilligung, informiert.

Folgendes Vorgehen ist für die Akquise von Teilnehmenden geplant:

1. Versand eines schriftlichen Erstanschreibens mit Informationen zur PIPS-Studie an die Leitungen zufällig ausgewählter Kindertageseinrichtungen in Deutschland, mit der Bitte um Teilnahme sowie dem Hinweis auf ein bevorstehendes telefonisches Informationsgespräch.
2. Telefonisches Informationsgespräch (bei Bedarf mehrere) mit den kontaktierten Einrichtungsleitungen zur Klärung der grundsätzlichen Teilnahmebereitschaft, offener Fragen und der Einbindung weiterer Entscheidungsträger (z. B. Träger, Elternbeirat). Auf Wunsch wird angeboten, die Kommunikation mit dem Träger zu übernehmen und Informationsmaterialien für weitere Entscheidungsträger zur Verfügung zu stellen.
3. Bei grundsätzlicher Zustimmung zur Studienteilnahme durch die Kitaleitung und ggf. weitere Entscheidungsträger erfolgt der Versand eines Informationspakets für Fachkräfte und Sorgeberechtigte. Auf dieser Grundlage kann die Leitung im Konsens mit dem Team und ggf. den Eltern über eine Teilnahme beraten. Auch ein Vorschlag zu relevanten Kindergruppen und beteiligten pädagogischen Fachkräften soll im Team freiwillig und gemeinsam abgestimmt werden, sodass die Entscheidungsfindung im vertraulichen Rahmen der Einrichtung bleibt. Das Informationspaket enthält folgende Materialien (Anhang 3), die in Abschnitt 2.2 genauer dargestellt werden:
 - Studieninfoschreiben für Eltern/Sorgeberechtigte
 - Datenschutzzinfoschreiben für Eltern/ Sorgeberechtigte
 - Einverständniserklärungen für Eltern/ Sorgeberechtigte
 - Studieninfoschreiben für Fachkräfte
 - Datenschutzzinfoschreiben für Fachkräfte
 - Einverständniserklärungen für Fachkräfte

Die Unterlagen des Informationspakets stellen den rechtlichen Rahmen für die Teilnahme dar, da sie die datenschutzrechtliche Aufklärung sowie die freiwillige, informierte Einwilligung aller beteiligten Personengruppen sicherstellen.

4. Telefonische/ E-Mail-Rückfrage, zur Teilnahmebereitschaft im Team/ bei den Eltern und Vereinbarung eines Erhebungstermins
5. Übermittlung der Zugangsdaten für die Fragebogenerhebung für die teilnehmenden pädagogischen Fachkräfte und Sorgeberechtigten an die teilnehmenden Einrichtungen.

2.1 Verarbeitung von Kontaktdaten im Akquiseprozess

Die Gewinnung der Kontaktdaten der Einrichtungen erfolgt auf Grundlage öffentlich zugänglicher Informationen (Websites der Einrichtungen oder Träger). Diese Daten (Name der Einrichtung, Name der Leitung, Altersstruktur der Einrichtung, Telefonnummer, E-Mail-Adresse, Adresse) werden zur Steuerung des Kontaktprozesses in einer tabellari-schen Übersicht dokumentiert, um nachvollziehen zu können, welche Einrichtungen bereits kontaktiert wurden, welche noch ausstehen und welche ihr Interesse an einer Teil-nahme bekundet oder abgelehnt haben. Die Verarbeitung dieser Kontaktdaten erfolgt auf Grundlage von Art. 6 Abs. 1 lit.e DSGVO i.V.m. § 3 Brandenburgisches Hochschulgesetz (BbgHG) (öffentliches Interesse). Das öffentliche Interesse liegt in der Organisation und Durchführung der wissenschaftlichen Studie sowie der bedarfsgerechten Kommunika-tion mit potenziellen Teilnehmenden.

Die Akquise von teilnehmenden Einrichtungen erfolgt über die dienstlichen Telefone und E-Mail-Adressen der Mitarbeitenden des PIPS-Projekts sowie auf postalischem Weg. Für weiterführende Informationsgespräche werden bei Bedarf Videokonferenzen über Zoom X angeboten. Bei Zoom X handelt es sich um einen Dienst, der auf zwischen dem Deut-schen Forschungsnetz (DFN) stellvertretend für die Hochschulen und der Firma Zoom Inc. abgeschlossenen Rahmenverträgen beruht und u.a. ein höheres Datenschutzniveau ermöglicht. In diesem Fall gelten ergänzend die Datenschutzbestimmungen von Zoom X^{1, 2}.

Die Daten von Einrichtungen, die eine Teilnahme ablehnen, werden ausschließlich bis zum Ende der Akquisephase gespeichert, um Mehrfachkontaktierungen zu vermeiden und anschließend gelöscht. Eine Weiterverarbeitung oder Weitergabe dieser Daten er-folgt nicht.

Die Daten jener Einrichtungen, die ihre grundsätzliche Teilnahmebereitschaft erklärt ha-ben, werden separat von den eigentlichen Studiendaten in einem Ordner auf dem Server der Fachhochschule Potsdam gespeichert, zu dem nur berechtigte Projektmitarbeitende Zugang haben. Eine Verwendung der Akquisedaten zu anderen als den genannten Zwe-cken ist ausgeschlossen.

2.2 Inhalt und rechtlicher Bezug des Informationspakets für Eltern und Fachkräfte

2.2.1 Informationen und Einverständniserklärungen für Eltern

Studieninfoschreiben für Eltern/Sorgeberechtigte (siehe Anhang 3.1)

Das Studieninfoschreiben informiert Eltern bzw. Sorgeberechtigte in verständlicher Spra-che über die Zielsetzung, den Ablauf sowie die Inhalte der PIPS-Studie. Es erläutert u. a. den wissenschaftlichen Hintergrund, welche Daten im Rahmen der Studie erhoben wer-den (z. B. durch Fragebögen), in welchem Zeitraum dies geschieht und welche Rolle die Kinder bzw. die Sorgeberechtigten selbst einnehmen. Ziel dieses Dokuments ist es, Transparenz zu schaffen und die Grundlage für eine informierte Entscheidung über die

¹ <https://www.fh-potsdam.de/campus-services/it-service/softwarelizenzen/zoom>

² Näheres zu Zoom X und den spezifischen Datenschutzbestimmungen findet sich unter <https://www.fh-potsdam.de/campus-services/it-service/softwarelizenzen/zoom>

Teilnahme zu bieten. Es erfüllt damit zentrale Anforderungen an die Transparenzpflicht gemäß Art. 12 ff. DSGVO und bildet die inhaltliche Basis für eine informierte Einwilligung.

Datenschutzinfoschreiben für Eltern/Sorgeberechtigte (siehe Anhang 3.2)

Das Datenschutzinfoschreiben richtet sich speziell an Eltern bzw. Sorgeberechtigte und dient der Erfüllung der Informationspflichten gemäß Art. 13 DSGVO. Es klärt darüber auf, welche personenbezogenen Daten von Eltern und Kindern im Rahmen der Studie erhoben und verarbeitet werden, zu welchen Zwecken dies geschieht, auf welcher Rechtsgrundlage die Datenverarbeitung basiert, wie lange die Daten gespeichert werden und welche Rechte die Betroffenen haben (z. B. Auskunft, Berichtigung, Löschung, Widerruf). Darüber hinaus enthält es Informationen zur verantwortlichen Stelle, Kontaktmöglichkeiten sowie zum Datenschutzbeauftragten.

Einverständniserklärung für Eltern/Sorgeberechtigte (siehe Anhang 3.3)

Die Einverständniserklärung dokumentiert die freiwillige und informierte Zustimmung der Eltern bzw. Sorgeberechtigten zur Teilnahme ihres Kindes an der PIPS-Studie. Sie bildet die datenschutzrechtliche Grundlage für die Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. a DSGVO. Da keine besonderen Kategorien personenbezogener Daten erhoben werden, greift Art. 9 Abs. 2 lit. a DSGVO in diesem Fall nicht.

Konkret umfasst die Erklärung:

- die Einwilligung zur Videografie des Kindes und der damit verbundenen Verarbeitung audiovisueller Daten zu wissenschaftlichen Zwecken,
- die Einwilligung zur Verarbeitung der im Elternfragebogen erhobenen personenbezogenen Daten,
- sowie eine optionale Zustimmung zur Nutzung der Daten zu Fortbildungszwecken (z. B. in Lehre und Weiterbildung).

Die Einwilligung erfolgt erst nach vorheriger schriftlicher Information über Zweck, Umfang und Dauer der Datenverarbeitung sowie über die Rechte der Betroffenen. In der Einverständniserklärung wird ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen. Zudem werden die Eltern bzw. Sorgeberechtigten darüber informiert, dass die Einwilligung jederzeit widerrufen werden kann (Art. 7 Abs. 3 DSGVO) und dass eine Nichtteilnahme keinerlei Nachteile für das Kind mit sich bringt. Die Erklärung enthält außerdem den Hinweis, dass die erhobenen Daten ausschließlich zu den genannten Zwecken verwendet und nicht an Dritte weitergegeben werden.

2.2.2 Informationen und Einverständniserklärungen für Fachkräfte

Studieninfoschreiben für Fachkräfte (siehe Anhang 3.4)

Dieses Schreiben informiert die pädagogischen Fachkräfte über Ziel, Ablauf, Inhalte und Methodik der PIPS-Studie. Es erläutert, welche Rolle die Fachkräfte in der Studie einnehmen in welchem Umfang ihre Mitwirkung erforderlich ist und welche Themenfelder die Studie umfasst. Ziel ist es, eine fundierte Entscheidungsgrundlage für die freiwillige Teilnahme zu schaffen und den Kontext der Erhebung wissenschaftlich einzuordnen. Es unterstützt damit die ethische und rechtliche Verpflichtung zur transparenzbasierten Forschungsteilnahme.

Datenschutzinfoschreiben für Fachkräfte (siehe Anhang 3.5)

Das Datenschutzinfoschreiben für Fachkräfte enthält alle gemäß **Art. 13 DSGVO** erforderlichen Informationen zur Erhebung und Verarbeitung ihrer personenbezogenen Daten im Rahmen der Studie. Dazu gehören Angaben zum Zweck der Datenverarbeitung, zur Rechtsgrundlage (i. d. R. Art. 6 Abs. 1 lit. a DSGVO), zur Dauer der Datenspeicherung sowie zu ihren Rechten als betroffene Personen. Ebenso werden die verantwortliche Stelle, Kontaktinformationen und der Datenschutzbeauftragte benannt. Ziel ist die rechtssichere und nachvollziehbare Information, die für eine **wirksame Einwilligung** zwingend erforderlich ist.

Einverständniserklärung für pädagogische Fachkräfte (siehe Anhang 3.6)

Die Einverständniserklärung für pädagogische Fachkräfte bildet die datenschutzrechtliche Grundlage für ihre freiwillige Teilnahme an der PIPS-Studie. Sie dient der dokumentierten, informierten Einwilligung in die Erhebung und Verarbeitung personenbezogener Daten im Sinne von Art. 6 Abs. 1 lit. a DSGVO. Da keine besonderen Kategorien personenbezogener Daten erhoben werden, greift Art. 9 Abs. 2 lit. a DSGVO in diesem Fall nicht.

Die Erklärung umfasst:

- die Einwilligung zur Videografie im Rahmen der Studie und zur damit verbundenen Verarbeitung audiovisueller Daten zu wissenschaftlichen Zwecken,
- die Einwilligung zur Verarbeitung personenbezogener Daten, die über Fragebögen erhoben werden,
- die Einwilligung zur Teilnahme an einem Interview,
- eine optionale Einwilligung zur Teilnahme an der Eye-Tracking Erhebung,
- sowie eine Einwilligung zur Nutzung der erhobenen Daten zu Fortbildungszwecken (z. B. für Lehre, Training und Weiterbildung im pädagogischen Kontext).

In der Einverständniserklärung wird explizit auf die Freiwilligkeit der Teilnahme hingewiesen. Die Fachkräfte werden darüber informiert, dass sie ihre Einwilligung jederzeit und ohne Angabe von Gründen widerrufen können (Art. 7 Abs. 3 DSGVO) und ihnen durch eine Nichtteilnahme keinerlei Nachteile entstehen. Die Erklärung enthält zudem den Hinweis, dass die Daten ausschließlich zu den angegebenen Zwecken verwendet und nicht an Dritte weitergegeben werden.

3 Studiendurchführung

3.1 Vorbereitung der Durchführung

3.1.1 Belehrung und Selbstverpflichtung der Mitarbeitenden im Forschungsteam

Vor Beginn der Datenerhebung werden alle Mitarbeitenden, Studierenden und Honorarkräfte, die im Rahmen der PIPS-Studie in Berührung mit Studiendaten kommen, zum Umgang mit sensiblen Daten sowie zum Datenschutz geschult (Schulungspräsentation „Safeguarding, Datenschutz und Datenmanagement“ (in Überarbeitung)) und verpflichten sich schriftlich zur Einhaltung der Datenschutzbestimmungen. (Selbstverpflichtung s. Anlage 4). Die Datenschutzeschulung umfasst zudem eine Einführung in den sicheren Umgang mit den eingesetzten Softwaretools.

Für alle Personen, die im Zuge ihrer Tätigkeit Kontakt mit Kindern haben, ist zusätzlich die Vorlage eines eintragsfreien erweiterten Führungszeugnisses gemäß § 30a Abs. 2 BZRG erforderlich (nicht älter als sechs Monate), sowie die Unterzeichnung einer Selbstverpflichtung zur Einhaltung der Child-Safeguarding-Richtlinien (siehe Anlage 4).

Da die genannten Selbstverpflichtungen projektübergreifend für alle an der Forschung von Frau Prof. Dr. Hildebrandt sowie Frau Prof. Dr. Große beteiligten Personen (AG frühkindliche Bildungsforschung) gelten, trägt der Briefkopf die Logos der Projekte „PINA“ und eine unterschriebene Version wird in den Lab-Räumlichkeiten der o.g. Professuren dauerhaft aufbewahrt.

Eingereichte Führungszeugnisse werden ausschließlich im Panzerschrank der Institutsleitung aufbewahrt und wird nach dem Ausscheiden des Forschenden innerhalb von sechs Wochen datenschutzkonform vernichtet. Eine anderweitige Speicherung der Zeugnisse, erfolgt ausdrücklich nicht. Ebenfalls werden die Führungszeugnisse nicht für andere Zwecke genutzt, es sei denn, es liegt eine ausdrückliche Einwilligung vor.

Zur Sicherstellung der datenschutzkonformen Umsetzung innerhalb des Projekts erhalten Studierende, die im Rahmen des PIPS-Projekts eine Prüfungsleistung oder sonstige studienbezogene Tätigkeit erbringen, eine zusätzliche schriftliche Belehrung zum Umgang mit Studiendaten. Diese wird von den Studierenden unterzeichnet und in den Projektunterlagen abgelegt.

3.2 Beschreibung der Erhebungsabläufe

3.2.1 Erhebung einrichtungsbezogener Kontextdaten

Im Vorfeld an die Erhebungstermine erfolgt die Erhebung einrichtungsbezogener Kontextdaten. Diese erfolgt im Rahmen der vorbereitenden Recherche für die Akquise (Bundesland, auf der SGB-II Quote des Einrichtungsortes basierende Kategorisierung der sozialen Belastungslage, Trägerform, Einrichtungsart) sowie im Rahmen einer Befragung der Einrichtungsleitung (Anzahl betreuter Kinder, Anzahl Fachkräfte im Krippen-/Elementar-/Hort-Bereich). Dabei handelt es sich nicht um Kontaktdaten oder personenbezogene Informationen, die Rückschlüsse auf einzelne Einrichtungen oder beteiligte Personen zulassen würden. Die Angaben werden in einer Excel-Tabelle dokumentiert.

Der gemäß Art. 88 DSGVO erforderliche Datenschutz hinsichtlich der Datenverarbeitung im Beschäftigtenkontext ist hinreichend erfüllt, da die Zustimmung zur Studienteilnahme

nicht einrichtungsübergreifend oder durch Abhängigkeitsverhältnisse zum Träger begründet ist, sondern von den einzelnen teilnehmenden Fachkräften selbst erfolgt.

3.2.1 Fragebögen

Die Erhebung der Fragebogendaten erfolgt über die Online-Umfrageplattform Tivian (ehemals Unipark). Tivian erfüllt die Anforderungen der DSGVO und speichert die Daten ausschließlich auf zertifizierten Servern innerhalb Deutschlands³. Die Übertragung der Daten erfolgt verschlüsselt und die Datenverarbeitung entspricht höchsten Sicherheitsstandards.

Vor dem vereinbarten Videografie-Termin erhalten die Einrichtungen die unter Punkt 2 genannten Zugangsdaten zur Teilnahme an der Fragebogenerhebung. Diese werden in Form individualisierter QR-Codes an die Einrichtungen verschickt. Die QR-Codes befinden sich in farblich gekennzeichneten Umschlägen, deren Beschriftung eindeutig verdeutlicht, für welche Personengruppe der jeweilige Code bestimmt ist (Eltern, videografierte Fachkraft, Team-Fachkraft, Leitung). Im Fragebogen selbst wird nochmals darauf hingewiesen, für welche Zielgruppe er bestimmt ist. Zu Beginn des Fragebogens erhalten die Teilnehmenden eine datenschutzrechtliche Aufklärung. Die Einwilligung zur Teilnahme an der Online-Befragung wird anschließend im selben Online-Formular digital eingeholt.

Zur datenschutzkonformen Zuordnung der Fragebogendaten zu den übrigen Erhebungsdaten wird eine passwortgeschützte Tabelle mit den teilnehmenden Einrichtungen und den zugehörigen Codes geführt.

Im Rahmen des Kontakts mit der Einrichtungsleitung (insbesondere zur Rückmeldung des Rücklaufs der Einverständniserklärungen) kann die Leitung gebeten werden, die teilnehmenden Personen an das Ausfüllen der Fragebögen zu erinnern. Am Tag der Videografie wird ein Tablet mitgebracht, auf dem Fachkräfte bei Bedarf den Fragebogen digital vor Ort ausfüllen können.

³ <https://www.unipark.com/faq-datenschutz/>

Folgende Fragebögen werden eingesetzt:

1. Elternfragebogen
2. Fachkraftfragebogen für videografierte Fachkräfte
3. Fachkraftfragebogen für das Team
4. Fragebogen für die Kitaleitung

Die inhaltlichen Erhebungsbereiche sind wie folgt verteilt:

Inhaltliche Dimension	Eltern	Videografierte Fachkräfte	Team-Fachkräfte	Leitung
Demografische Angaben: Alter, Schulabschluss, höchster Berufs-/Bildungsabschluss	x	x	x	x
Demografische Angaben: Erstsprache	x	x	x	x
Demografische Angaben: derzeitige berufliche Stellung	x			
Demografische Angaben: Dauer der Berufstätigkeit als Pädagog*in		x	x	x
Einstellungen zur Partizipation (Pflege/Schlaf)	x	x	x	x
Biografische Erfahrungen (Pflege/Schlaf)	x	x	x	x
Teamklima und Arbeitsbelastung		x	x	x
Motivation		x	x	x
Elternzusammenarbeit (Pflege/Schlaf)		x	x	x
Arbeitszeit am Erhebungstag		x		
Skalen zur Emotionserkennung		x		
Beziehung zum Kind, weitere Bezugspersonen des Kindes	x			
Kommunikation mit Fachkräften zum Thema Pflege und Schlaf	x			
Erwartungen an die Kita	x			

Die von den Fachkräften erhobenen Angaben zu Arbeitszeiten und Arbeitsbelastung beruhen auf Freiwilligkeit, weshalb der gemäß Art. 88 DSGVO erforderliche Datenschutz hinsichtlich der Datenverarbeitung im Beschäftigtenkontext hinreichend erfüllt ist.

3.2.2 Videografie

Am vereinbarten Videografie-Termin in den Einrichtungen überprüfen die anwesenden Erheber*innen gemeinsam mit den pädagogischen Fachkräften zunächst, ob für alle anwesenden Kinder eine schriftliche Einverständniserklärung der Eltern bzw. Sorgeberechtigten vorliegt. Ebenso muss für alle teilnehmenden pädagogischen Fachkräfte eine entsprechende Einverständniserklärung vorliegen.

Nur Kinder und pädagogische Fachkräfte, deren Teilnahme an der Videografie schriftlich genehmigt wurde, dürfen sich während der Aufnahmen in den videografierten Räumlichkeiten aufhalten. Um dies zu gewährleisten, ist eine enge Zusammenarbeit mit den pädagogischen Fachkräften erforderlich, da ein eigenständiger und zuverlässiger Personenabgleich durch die Studienmitarbeiter*innen nicht möglich ist. Die Fachkräfte sind daher ausdrücklich dazu angehalten, auch während der Videografie aufmerksam zu bleiben und die Erheber*innen unverzüglich zu informieren, falls sich ein Kind oder Erwachsener ohne vorliegende Einverständniserklärung im videografierten Bereich aufhält.

Für Kinder, deren Erziehungsberechtigte der Teilnahme nicht zugestimmt haben oder für die aus anderen Gründen zu Beginn des Erhebungstages keine Einverständniserklärung vorliegt, ist die Anfertigung von Foto-, Video- oder Tonaufnahmen unzulässig. Da Kinder gemäß Erwägungsgrund 38 der Datenschutz-Grundverordnung (DSGVO) als besonders schützenswerte Personengruppe gelten, wird im gesamten Erhebungsprozess besonderer Wert auf altersgerechte Schutzmaßnahmen und die sorgfältige Einhaltung datenschutzrechtlicher Vorgaben gelegt. Um sicherzustellen, dass Kinder ohne vorliegende Einverständniserklärung nicht unbeabsichtigt aufgezeichnet werden, sind die Erheber*innen verpflichtet, vor Beginn der Aufnahmen potenzielle visuelle Reflexionsflächen – wie Fenster, Glastüren, Spiegel, spiegelnde Bilder oder Sichtfenster – sorgfältig abzudecken.

Die Kameras sind jederzeit personell besetzt, sodass ein situationsbezogenes Ein- und Ausschalten möglich ist. Dies ist insbesondere in Gemeinschaftsbereichen relevant, in denen Personen ohne Einverständnis nicht zuverlässig ausgeschlossen werden können (z. B. Badezimmer). Sofern nicht sichergestellt werden kann, dass ein gemeinschaftlich genutzter Bereich während der Videografie ausschließlich von Personen mit vorliegender Einverständniserklärung betreten wird, darf die Kamera dort nur situationsbezogen eingeschaltet werden. Dies erfolgt ausschließlich in Begleitung einer pädagogischen Fachkraft, sobald die entsprechende Voraussetzung erfüllt ist. Die Kamera darf hierbei nicht auf den Eingangsbereich des Raums gerichtet sein, sodass beim Eintreten einer Person ohne Einverständnis die Aufnahme augenblicklich beendet werden kann, bevor diese in das videografierte Feld eintritt. Die Kamera verbleibt nicht dauerhaft im Raum.

Die Videografie kann jederzeit unterbrochen oder abgebrochen werden, insbesondere dann, wenn Kinder, Fachkräfte oder andere Beteiligte Anzeichen von Unwohlsein zeigen oder der geschützte Rahmen nicht mehr gewährleistet ist. Die Aufzeichnung wird außerdem unverzüglich durch die Erheber*innen beendet, sobald im Verlauf der Beobachtung ein Vorkommnis festgestellt wird, das gemäß der Kinderschutzleitlinie (siehe Anhang) als relevant eingestuft werden muss. In einem solchen Fall steht der Schutz des Kindeswohls uneingeschränkt im Vordergrund, und die vorgesehenen Schritte werden umgehend eingeleitet.

Die Aufnahmen erfolgen mit Kameras des Typs (?). Zudem erhalten die videografierten Fachkräfte jeweils ein angestecktes Personenmikrofon des Typs (?). Die Speicherung erfolgt zunächst auf verschlüsselten SD-Karten, die für Transportwege zusätzlich in einer verschlossenen Kassette aufbewahrt werden. Zum nächstmöglichen Zeitpunkt werden die Daten gemäß der im Konzept beschriebenen Vorgehensweise zur Datenspeicherung (siehe Kapitel 4) durch die Erheber*innen gesichert und anschließend von der SD-Karte gelöscht.

3.2.3 Live-Beobachtungen

Ergänzend zur Videoaufzeichnung werden während der Erhebung zusätzliche Aspekte des Kita-Alltags durch die beobachtende Person live erfasst und schriftlich dokumentiert.

Die Live-Beobachtung umfasst folgende Elemente:

- Raum-Checkliste: Erfasst wird die räumliche Gestaltung der Einrichtung mit Blick auf partizipationsfördernde oder -hinderliche Bedingungen in Pflege- und Schlafsituationen.
- Beobachtung impliziter Regeln: Falls im Verlauf der Erhebung implizite Regeln oder Routinen beobachtbar sind, die das Verhalten der Fachkräfte oder Kinder in Pflege- und Schlafsituationen prägen, werden diese notiert. Sie dienen als Grundlage für gezielte Nachfragen im anschließenden Interview mit der Fachkraft.

3.2.4 Interviews

Im Anschluss an die Videoerhebung wird mit der videografierten Fachkraft ein leitfadengestütztes, etwa 15- bis 30-minütiges Interview durchgeführt. Das Interview wird mithilfe eines Diktiergeräts des Typs (?) aufgezeichnet und dient der ergänzenden Erfassung subjektiver Perspektiven auf den Erhebungstag.

Erfragt werden:

- die individuelle Einschätzung des Tagesverlaufs,
- welche Situationen als besonders herausfordernd erlebt wurden und wie der persönliche Umgang damit eingeschätzt wird,
- sowie bestehende Regeln, Routinen oder Absprachen im Team, die die Partizipation von Kindern in Pflege- und Schlafsituationen betreffen. Ggf. werden, falls in der Live-Beobachtung implizite Regeln beobachtet wurden, dazu Nachfragen gestellt.

3.2.5 Eye-Tracking

Ergänzend zu den oben beschriebenen Erhebungsmethoden ist der Einsatz von Eye-Tracking mit pädagogischen Fachkräften vorgesehen. Ziel dieser ergänzenden Untersuchung ist es, visuelle Aufmerksamkeitsmuster in alltäglichen Interaktionen mit Kindern unter drei Jahren zu analysieren.

Die Erhebung soll mit ca. 20 pädagogischen Fachkräften durchgeführt werden. Zum Einsatz kommen die Eye-Tracking-Brille des Typs (?) und die zugehörige Software von Pupil Labs (Modelle: Neon und Invisible). Pupil Labs erfüllt die datenschutzrechtlichen Vorgaben der DSGVO; alle erfassten Daten werden ausschließlich auf zertifizierten Servern innerhalb Deutschlands gespeichert.⁴ Vor Beginn der Erhebung wird ein zusätzliches, schriftliches Einverständnis zur Teilnahme an der Eye-Tracking-Erhebung eingeholt (siehe Anhang 3).

⁴ <https://pupil-labs.com/legal/privacy>

Der Ablauf der Eye-Tracking-Erhebung gestaltet sich wie folgt:

- Vor Beginn der Aufzeichnung wird den teilnehmenden Fachkräften die Eye-Tracking-Brille ausführlich erklärt und demonstriert. Auch den anwesenden Kindern wird die Brille kindgerecht vorgestellt, um Transparenz und Vertrauen zu fördern.
- Die Brille zeichnet ausschließlich das Sichtfeld der Fachkraft auf, nicht deren Gesicht.
- Geplant sind ca. drei-fünf kurze Aufzeichnungseinheiten pro Fachkraft, jeweils mit einer Dauer von ca. zehn Minuten.
- Die aufgezeichneten Videodaten werden auf einem mobilen Endgerät der Fachhochschule Potsdam gespeichert, unter Nutzung der App "Invisible Companion" von Pupil Labs.

Für die Eye-Tracking-Erhebung gelten die gleichen datenschutzrechtlichen Maßnahmen wie bei klassischer Videografie: Die teilnehmenden Fachkräfte werden ausdrücklich dazu angehalten, während der Aufzeichnung aufmerksam zu bleiben und das Erhebungsteam unverzüglich zu informieren, sollte sich eine Person (Kind oder Erwachsener) ohne vorliegende Einwilligung im Sichtfeld der Brille befinden. Kinder, für die keine unterschriebene Einverständniserklärung durch die Eltern bzw. Sorgeberechtigten vorliegt, dürfen unter keinen Umständen videografisch erfasst werden – weder durch klassische Kameras noch durch das Sichtfeld der Eye-Tracking-Brille.

4 Datenspeicherung, -auswertung, -aufbewahrung und -löschung

4.1 Datenspeicherung und -aufbewahrung

Alle erhobenen Daten werden so gespeichert, dass ein unbefugter Zugriff ausgeschlossen ist. Zentrale Maßnahmen hierfür sind insbesondere die physische sowie digitale Sicherung und Verschlüsselung der erhobenen Daten.

Die digitale Datenablage erfolgt auf den hochschuleigenen Servern der Fachhochschule Potsdam (FHP). Diese ermöglichen nicht nur eine regelmäßige Datensicherung (Backups), sondern bieten durch Firewalls Schutz vor unautorisiertem Zugriff (z. B. durch Hacking), Datenverlust und Schäden durch Umwelteinflüsse.

Die Speicherung der pseudonymisierten Daten – einschließlich der Fragebogendaten, Live-Erhebungsdaten, Transkripte von Video- und Interviewmaterialien sowie Codierdatensätze – erfolgt unter Einhaltung gängiger Sicherheitsstandards ausschließlich auf den Servern der FHP. Die Zuordnung der Einrichtungen erfolgt über eine separate Subjekt-Schlüssel-Liste, in der jeder Einrichtung ein Pseudonym (Einrichtungs-ID) zugewiesen ist. Innerhalb dieser Liste sind außerdem die pseudonymisierten Teilnehmenden-IDs jeweils der zugehörigen Einrichtung zugeordnet. Die Liste wird getrennt von den übrigen Forschungsdaten in einer geschützten Containerdatei aufbewahrt.

Für die Speicherung besonders sensibler Daten wie Video-, Audio- und Eye-Trackingmaterialien werden erweiterte Schutzmaßnahmen umgesetzt: Diese Dateien werden ausschließlich innerhalb einer mit VeraCrypt verschlüsselten Containerdatei auf dem FHP-Server gespeichert. Das zugehörige Passwort wird ausschließlich mündlich an zur Auswertung autorisierte Projektmitarbeiter*innen weitergegeben. Eine schriftliche Form des

Passworts wird gesichert in einem Safe verwahrt, auf den ausschließlich die hochschul-eigene IT und Frau Prof. Dr. Hildebrandt und Herr Prof. Dr. Karsten Krauskopf Zugriff haben. Zehn Jahre nach der Datenerhebung werden Frau Prof. Dr. Hildebrandt und Herr Prof. Dr. Karsten Krauskopf kontaktiert, um über eine Verlängerung der Aufbewahrung oder eine Löschung zu entscheiden.

Die Video-, Audio- und Eye-Trackingdaten werden unmittelbar nach der Erhebung in die geschützte Containerdatei übertragen und anschließend auf dem Aufnahmegerät sowie eventuell genutzten Zwischenträgern vollständig gelöscht.

Der Zugriff auf diese besonders sensiblen Daten ist ausschließlich auf von der Fachhochschule Potsdam bereitgestellten oder verwalteten Dienstrechnern zulässig, dies gilt Standort unabhängig, insofern sichergestellt ist, dass die Datensicherheitsstandards eingehalten werden. Für temporäre Auswertungszwecke dürfen die genannten Daten wenn zwingend erforderlich in verschlüsselten Containerdateien auch lokal auf diesen Rechnern oder auf verschlüsselten externen Speichermedien gespeichert werden. Im Anschluss an die Auswertung sind die Materialien unverzüglich vom entsprechenden Medium zu löschen, um eine unkontrollierte Vervielfältigung des Materials auszuschließen. Als sichere Löschrprogramme werden "DBAN" und "Eraser" (Methode: DoD 3 Passes) genutzt⁵

Die Subjekt-Schlüssel Listen zur Zuordnung der pseudonymisierten Personen-IDs und Einrichtungs-IDs zu den Klarnamen der Einrichtungen wird in einer gesonderten, ebenfalls verschlüsselten Containerdatei auf dem FHP-Server gespeichert. Für diese gelten dieselben Zugriffs- und Schutzrichtlinien wie für das audiovisuelle Datenmaterial.

Die Einverständniserklärungen werden ausschließlich in Papierform archiviert. Sie enthalten keine Zuordnung zu digitalen Daten und werden für die Dauer von zehn Jahren in einem abschließbaren Panzerschrank in den Räumen des PINA-Labors verwahrt. Der Zugang ist ausschließlich autorisierten Mitarbeiter*innen vorbehalten. Nach Ablauf der Frist erfolgt die datenschutzkonforme Vernichtung.

Nach Projektabschluss werden vollständig anonymisierte bzw. pseudonymisierte Forschungsdatensätze zur Nachnutzung und Qualitätssicherung auf der Plattform Open Science Framework (OSF) veröffentlicht. Die Veröffentlichung erfolgt unter Einhaltung der Open-Data-Prinzipien und entspricht den Maßgaben der DSGVO hinsichtlich wissenschaftlicher Archivierungszwecke gemäß Art. 89 DSGVO.

4.2 Datenauswertung

Die im Rahmen der Studie erhobenen Daten werden unter Einhaltung datenschutzrechtlicher Vorgaben verarbeitet und ausschließlich pseudonymisiert ausgewertet. Die Verarbeitung von Primärdaten erfolgt ausschließlich auf dienstlich gesicherten Geräten der Fachhochschule Potsdam. Dabei kommen folgende Verfahren und Softwarelösungen zum Einsatz:

⁵siehe auch: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/DBAN/dban_node.html

Transkription

Für alle Interview- und Videodaten erfolgt die Transkription von Audiodaten mittels f4 oder der Open-Source Software NoScribe. Die automatische, KI-unterstützte Transkription von f4 wird ausschließlich über Server in Deutschland realisiert und ist DSGVO-konform⁶. NoScribe wird als Desktopversion genutzt.

Alle Transkripte werden vor der Analyse pseudonymisiert (Entfernung bzw. Ersetzung personenbezogener Angaben, z. B. Klarnamen).

Videobearbeitung

Die Videoaufnahmen werden mit Adobe Premiere Pro 2025 bearbeitet. Die Software ermöglicht unter anderem Bild-in-Bild-Schnitt (z. B. zur Darstellung zweier Kameraperspektiven) sowie die Verfremdung identifizierbarer Personenmerkmale. Adobe Premiere wird von der Fachhochschule Potsdam bereitgestellt und es findet keine Übertragung von Daten an Adobe-Server statt⁷.

Übertragung von Eye-Tracking-Daten

Die Eye-Tracking-Videodaten werden zunächst auf einem mobilen Endgerät gespeichert, unter Nutzung der App Invisible Companion von Pupil Labs. Nach der Übertragung in die zugehörige KI-unterstützte Auswertungssoftware auf einem gesicherten Hochschulgerät werden die Daten aus der mobilen App gelöscht. Nach der Aufbereitung (z. B. Extraktion von Blickverläufen) und dem Export relevanter Kennwerte (z. B. als Excel-Dateien) werden auch die Daten aus der Softwareumgebung vollständig entfernt.

Inhaltliche Analyse

Die inhaltliche Analyse findet mit der Analysesoftware MAXQDA statt, wobei auch KI-unterstützte Tools der Software verwendet werden. Diese Tools sind DSGVO-konform, nutzen nur minimal notwendige Daten, nutzen diese nicht für KI-Trainingszwecke und werden nicht von KI-Dienstleistern gespeichert.⁸ Darüber hinaus wird – ausschließlich für einzelne Reliabilitätsanalysen – auch die MAXQDA TeamCloud verwendet. MAXQDA TeamCloud-Projekte werden ausschließlich auf DSGVO-konformen Servern in Deutschland gespeichert⁹. Gleiches gilt für die personenbezogenen Daten des MAXQDA-Accounts; die Speicherung erfolgt in einer verschlüsselten Datenbank auf Servern von AWS in Deutschland. Die Bedingungen der DSGVO werden eingehalten. Die Anschaffung der MAXQDA-Lizenzen erfolgte in Abstimmung mit der Fachhochschule Potsdam, womit die Nutzung datenschutzrechtlich abgesichert ist.

Um für ausgewählte Videoausschnitte zusätzlich die nonverbale affektive Grundstimmung zu erfassen (Basis-Emotionen) wird ergänzend der Noldus FaceReader (Desktop-Software) zur Analyse eingesetzt. Hierbei liegt der Fokus auf der Analyse von Ekel der Fachkräfte in Pflegesituationen. Die Anschaffung der Software erfolgte bereits vor unserem Projekt in Abstimmung mit den verantwortlichen Stellen der FHP. Die eingesetzte Software nutzt standardisierte Modelle mimischer Basisemotionen, die in der Forschung

⁶ <https://www.audiotranskription.de/f4/f4-dsgvo/>

⁷ <https://www.fh-potsdam.de/campus-services/it-service/softwarelizenzen/adobe-creative-cloud>

⁸ <https://www.maxqda.com/de/ki-und-datenschutz>

⁹ <https://help.maxqda.com/de/support/solutions/articles/80001135559-wo-werden-die-daten-gespeichert-ist-der-datenschutz-gew%C3%A4hrleistet>

als methodisch und kulturell begrenzt gelten. Um diese Einschränkungen zu berücksichtigen, wird die Software nur ergänzend verwendet. Ergebnisse werden mit Beobachtungs- und Interviewdaten abgeglichen, um Fehldeutungen zu vermeiden. Die automatisierte Analyse wird nicht für Trainingszwecke externer KI-Systeme genutzt, sondern bleibt vollständig innerhalb der Projektumgebung.

Statistische Auswertung

Die quantitativen Daten aus Fragebögen, der inhaltlichen Analyse und der Eye-Tracking-Erhebung werden mit Excel, SPSS, R oder JASP statistisch analysiert.

4.3 Datenlöschung

Die Löschung personenbezogener Daten erfolgt gemäß den datenschutzrechtlichen Vorgaben sowie den Empfehlungen der Deutschen Gesellschaft für Psychologie (DGPs) zur Aufbewahrung und Archivierung wissenschaftlicher Forschungsdaten¹⁰.

Die Projektleitungen verpflichten sich, die im Rahmen des Projekts erhobenen nicht-anonymisierten Rohdaten für die Dauer von zehn Jahren aufzubewahren. Diese Frist orientiert sich an den Empfehlungen der DGPs und dient der Sicherstellung wissenschaftlicher Nachvollziehbarkeit. Nach Ablauf dieser Frist erfolgt eine vollständige Löschung bzw. datenschutzkonforme Vernichtung der betroffenen Daten.

Die Einverständniserklärungen der Teilnehmenden sowie Verpflichtungserklärungen und eingereichte Führungszeugnisse der Mitarbeitenden werden ebenfalls spätestens zehn Jahre nach Projektende vernichtet.

4.3.1 Datenlöschung bei Widerruf der Einwilligung

Studienteilnehmende bzw. ihre gesetzlichen Vertreter*innen können ihre Einwilligung zur Verarbeitung personenbezogener Daten jederzeit widerrufen. In einem solchen Fall wird das entsprechende Videomaterial verfremdet (verpixelt/geschwärzt). Dieses Vorgehen wird dem Bedürfnis der StudienteilnehmerInnen bzw. deren VertreterInnen nach Unkenntlichmachung gerecht und steht in einem angemessenen Verhältnis zum hohen Aufwand der Datengewinnung (insbes. Videografie) des Projekts. Weitere Datensätze (Fragebögen u.a.) werden gelöscht.

Sowohl für die Verpixelung als auch für die Löschung von Datensätzen wird ein an Anhang 2.1 angelehntes Löschprotokoll angefertigt und in den Projektunterlagen aufbewahrt.

Bereits erfolgte Analysen und Veröffentlichungen können auch nach Widerruf nicht zurückgezogen werden – in diesem Sinne gilt ein Widerruf für die Verwendung der Daten stets für zukünftige Analysen u.a. Verwendungszwecke.

Team-Fachkräfte und Kitaleitungen, die nicht videografiert wurden, sondern ausschließlich an der Fragebogenerhebung teilgenommen haben, erhalten über ihren individuellen Fragebogen-Zugang (z. B. QR-Code) die Möglichkeit, jederzeit die Löschung ihrer erhobenen Daten zu beantragen. Auf dieses Recht werden sie bereits bei der Übergabe der Zugangsinformationen ausdrücklich hingewiesen.

¹⁰ Schönbrodt, F., Gollwitzer, M., & Abele-Brehm, A. (2017). Der Umgang mit Forschungsdaten im Fach Psychologie: Konkretisierung der DFG-Leitlinien. *Psychologische Rundschau*.

5 Datennutzung

5.1 Nutzung von Daten für wissenschaftliche Veröffentlichungen

Im Rahmen des Forschungsprojekts ist die Veröffentlichung eines Projektberichts sowie von Fachartikeln in wissenschaftlichen Zeitschriften vorgesehen. Darüber hinaus werden Forschungsergebnisse ggf. auf Fachtagungen präsentiert. Dabei wird strikt darauf geachtet, dass alle veröffentlichten Inhalte keine Rückschlüsse auf einzelne Teilnehmende oder beteiligte Einrichtungen zulassen.

Zur Veranschaulichung ausgewählter Befunde können (sofern erforderlich) Standbilder aus den Videografien verwendet werden. Die bevorzugte Darstellungsform sind abstrahierte Zeichnungen, die zentrale Situationen ohne identifizierende Merkmale visualisieren. Sollte dies im Einzelfall nicht möglich sein, können alternativ stark verfremdete Bildausschnitte verwendet werden, bei denen durch Zuschnitt, Schwärzung oder den Einsatz von abstrahierten Zeichnungen potenziell identifizierbare Umgebungsmerkmale unkenntlich gemacht wurden.

5.2 Nutzung von Daten durch Studierende

Studierende der Fachhochschule Potsdam, insbesondere aus der Arbeitsgruppe Frühkindliche Bildungsforschung, sollen im Sinne forschungsnaher Lehre und Qualifizierung in angemessener Weise in die Tätigkeiten des PIPS-Projekts eingebunden werden. Zu diesem Zweck wird ein niedrighschwelliger Zugang zu ausgewählten Projektbestandteilen ermöglicht (vgl. Abschnitt 4.2.1).

Über den Zugang zu sensiblen Projektmaterialien, insbesondere den Primärdatensätzen, entscheiden die im Projekt hauptverantwortlich tätigen Wissenschaftler*innen. Für alle Personen, die mit den sensiblen Erhebungsdaten arbeiten, gilt die in Abschnitt 3.1.1 beschriebene Belehrung und Selbstverpflichtung.

Sollten im Rahmen von Studien- oder Abschlussarbeiten sowie hochschulbezogenen Präsentationen Standbilder aus Videografien verwendet werden müssen, gelten hierfür die gleichen datenschutzrechtlichen Anforderungen wie für wissenschaftliche Publikationen (s. Abschnitt 5.1).

5.3 Veröffentlichung von Daten und Nachnutzung der Daten durch Dritte

Es ist vorgesehen, die Primärdatensätze der Erhebungsinstrumente nach Projektende in einem vertrauenswürdigen öffentlichen Repositorium zur Nachnutzung bereitzustellen. Dazu wird gemäß der Empfehlung der Deutschen Gesellschaft für Psychologie darauf geachtet, dass dies datenschutzrechtlich und inhaltlich sinnvoll ist.

Die Daten werden auf der Plattform Open Science Framework (OSF)¹¹ bereitgestellt. OSF ist ein interdisziplinäres, nicht-kommerzielles Repositorium, das von dem US-amerikanischen Center for Open Science betrieben wird. Die Plattform unterstützt Forschende

¹¹ <https://www.osf.io>

weltweit beim Management, der Veröffentlichung und der Archivierung wissenschaftlicher Daten und erfüllt dabei internationale Standards zu Datenschutz und -sicherheit¹². Für alle veröffentlichten Inhalte können differenzierte Zugriffsrechte und Nutzungsbedingungen vergeben werden (z. B. Embargo, geschützter Zugriff, Lizenzvergabe). Die Speicherung erfolgt verschlüsselt.

Folgende Datentypen sollen – nach Prüfung auf ausreichende Anonymisierung bzw. Pseudonymisierung – zur Veröffentlichung freigegeben werden:

- Tabelle mit einrichtungsbezogenen Kontextdaten (z. B. Einrichtungstyp, Gruppengröße, Altersstruktur),
- Antworten auf die Fragebögen (Eltern, Fachkräfte, Leitung), ausgenommen urheberrechtlich geschützter Items,
- Verhaltenskodierungen aus Videoanalysen
- Dokumentation der Live-Beobachtungen
- Kodierungen der Interviews
- Eye-Tracking-Daten

Videodaten werden nicht im Repositorium veröffentlicht. Diese enthalten personenbezogene Daten besonders schutzwürdiger Gruppen und können grundsätzlich nicht anonymisiert werden. Daher wird auf eine Veröffentlichung im Repositorium verzichtet.

5.3.1 Veröffentlichung von Videodaten

Ein Zugang zu Videodaten durch Dritte ist nur in begründeten Einzelfällen möglich, ausschließlich bei einem klar definierten, vorrangig wissenschaftlichen Erkenntnisinteresse. Über eine solche Zugangsvergabe entscheiden die verantwortlichen Projektleiter*innen gemeinsam und in enger Abstimmung. Die Entscheidung wird dokumentiert und an Bedingungen (z. B. unterschriebene Datenschutzerklärung, Nutzungskontext, Zugangskontrolle) geknüpft.

5.4 Nachnutzung der Daten für Fortbildungszwecke

Die Ergebnisse der PIPS-Studie sollen über die wissenschaftliche Auswertung hinaus auch in die Aus- und Fortbildung pädagogischer Fachkräfte einfließen. Zu diesem Zweck können ausgewählte Video- und Tonaufnahmen aus der Datenerhebung in Lehrveranstaltungen sowie Fortbildungsformaten eingesetzt werden. Die Zustimmung zur Verwendung der Aufnahmen für diesen Zweck wird im Rahmen der allgemeinen Einverständniserklärung sowohl bei den teilnehmenden Fachkräften als auch bei den Eltern bzw. Sorgeberechtigten der aufgenommenen Kinder eingeholt. Ergänzend erhalten alle Beteiligten im Vorfeld entsprechende Informationen zum Datenschutz und zur konkreten Verwendung der Aufnahmen in Aus- und Fortbildungskontexten (siehe Anhang 3).

Die Nutzung der entsprechenden Videosequenzen in Lehr- und Fortbildungssettings ist zeitlich begrenzt und darf nur zweckgebunden erfolgen. Für den Transport der benötigten Dateien an externe Fortbildungsorte werden ausschließlich verschlüsselte Datenträger verwendet. Nach Abschluss der jeweiligen Fortbildungsveranstaltung bzw. -reihe werden die verwendeten Dateien gemäß den Regelungen zur Datenspeicherung und -löschung vollständig und sicher entfernt (siehe Abschnitt 4.1 und 4.3).

¹² <https://help.osf.io/article/391-security-and-privacy>

Es wird darauf hingewiesen, dass bei der Verwendung von Videomaterial in Lehrkontexten eine vollständige Anonymisierung der aufgenommenen Personen nicht immer gewährleistet werden kann. Da Mimik, Gestik, Sprache und situative Kontexte zentrale Beobachtungsgrundlage der Studie darstellen, würde eine nachträgliche Verfremdung der Aufnahmen die Aussagekraft und den didaktischen Nutzen der Szenen erheblich einschränken. Daher wird bei der Auswahl der Videosequenzen besonders sorgfältig darauf geachtet, dass personenbezogene Informationen nicht unnötig rückverfolgbar sind. Dies betrifft insbesondere die Beschränkung auf kurze Ausschnitte sowie die gezielte Auswahl relevanter Interaktionssituationen. Personen, die im Bild zu sehen sind, aber für den jeweiligen Lehrkontext nicht relevant sind, werden unkenntlich gemacht.

Teilnehmenden von Fortbildungen und Lehrveranstaltungen wird vorab ausdrücklich mitgeteilt, dass etwaige Wiedererkennungen von Personen in den gezeigten Aufnahmen vertraulich zu behandeln sind und darüber Stillschweigen zu bewahren ist.

Anhang

1 Umgang mit Datenschutzvorfällen

Bei einem Datenschutzvorfall ist die Forschungsleitung, die Hochschulleitung und der Datenschutzbeauftragte zu informieren. Über die Feststellung eines Datenschutzvorfalls entscheiden die Forschungsleitung, die Hochschulleitung und der Datenschutzbeauftragte. Vorstufen von Datenschutzvorfällen, wie der Verlust eines gesicherten Datenträgers, müssen besprochen und vermieden werden.

Falltyp	Maßnahmen
1. Kind wird gefilmt, obwohl keine Einverständniserklärung der Eltern vorliegt <i>z. B. Kommt kurz in den Raum oder am Erhebungstag wird fälschlicherweise angenommen, dass Einverständnis vorliegt</i>	Bei vollständiger Kontrolle über das Datenmaterial durch Mitarbeiter*innen (kein Verlust, ausschließlich Nutzung verschlüsselter Datenträger, kein unbefugter Zugriff durch Dritte) Meldung an: <ul style="list-style-type: none">• die Hochschulleitung (Kanzlerin Frau Gerlinde Reich),• und den Datenschutzbeauftragten (Herr Sven Hirsch) Bei zusätzlichem Datenverlust, unbefugtem Zugriff oder einer anderweitigen Verletzung des Schutzes personenbezogener Daten: <ul style="list-style-type: none">• zusätzlich gemäß Art. 33 DSGVO Meldung an die zuständige Landesdatenschutzbehörde
2. Verlust von Datenträgern <i>z. B. USB-Stick, externe Festplatte, SD-Karte oder Laptop mit noch ungesicherten Aufnahmen oder Fragebogendaten geht verloren</i>	Nach Art. 33 DSGVO sofortige Meldung an: <ul style="list-style-type: none">• die Hochschulleitung (Kanzlerin Frau Gerlinde Reich),• Datenschutzbeauftragten (Herr Sven Hirsch),• sowie an die zuständige Landesdatenschutzbehörde. Prüfung ob personenbezogene Daten betroffen sind, Sicherstellen zukünftiger Verschlüsselung und Zugangsschutz
3. Unverschlüsselte Übertragung oder Speicherung <i>Daten wurden z. B. per E-Mail oder Cloud ohne Verschlüsselung übermittelt oder auf ungesicherten Geräten gespeichert</i>	Benachrichtigung des Datenschutzbeauftragten (Herr Sven Hirsch), nachträgliche Absicherung, ggf. Löschung, IT-Sicherheitsprüfung, Prüfung interner Prozesse
4. Unbefugter Zugriff (intern oder extern) <i>Eine nicht berechnigte Person erhält Zugriff auf Video-/Audio-/Fragebogendaten</i>	Sofortige Sperrung des Zugriffs, Benachrichtigung des Datenschutzbeauftragten (Herr Sven Hirsch), ggf. Meldung nach DSGVO
5. Fehlender Widerruf/Löschbegehren ignoriert <i>Eine betroffene Person fordert Löschung der Daten,</i>	Benachrichtigung des Datenschutzbeauftragten (Herr Sven Hirsch), Nachträgliche Löschung, Löschprotokoll, Prüfung interner Prozesse

<i>diese wird aber nicht korrekt umgesetzt</i>	
6. Veröffentlichung identifizierbarer Daten <i>z. B. versehentliche Veröffentlichung eines Videos/Bildes mit erkennbaren Kindern in Vortrag oder Publikation</i>	Sofortige Rücknahme, Benachrichtigung des Datenschutzbeauftragter (Herr Sven Hirsch), Kontakt zu betroffener Einrichtung, DSGVO-Prüfung, Maßnahmen zur künftigen Vermeidung
7. Einwilligung fehlerhaft dokumentiert <i>Ein Formular fehlt, ist unvollständig oder wurde nicht korrekt zugeordnet</i>	Benachrichtigung des Datenschutzbeauftragten (Herr Sven Hirsch), Korrektur, Nachholung der Einwilligung (wenn möglich), ggf. Löschung der Daten, Löschprotokoll

2 Dokumentierte Vorgehensweisen bei unerwünschten Aufnahmen

Die folgende Vorgehensweise basiert auf einem Datenschutzvorfall aus einer Vorgängerstudie (03.04.2019), bei dem in einer Kindertageseinrichtung ein Kind videografiert wurde, ohne dass eine Einverständniserklärung der Eltern vorlag. Dieser Fall wurde umfassend dokumentiert und dient als Referenzmodell für vergleichbare Situationen. Sollte es zu anderen, in Anhang 1 genannten oder weiteren Formen von Datenschutzverstößen kommen, erfolgt eine Einzelfallprüfung und Abstimmung mit dem Datenschutzbeauftragten der Fachhochschule Potsdam, Herrn Sven Hirsch.

Nach Bekanntwerden eines Datenschutzvorfalls erfolgt folgendes mehrstufiges Verfahren:

1) Interne Dokumentation des Vorfalls

Eine schriftliche Darstellung zum Ablauf und zur Entstehung des Vorfalls wird bei den unmittelbar beteiligten Personen (Erhebungsteam, ggf. Rückmeldung der Einrichtung) eingeholt. Die Dokumentation enthält:

- eine sachliche Beschreibung des Ablaufs,
- Angaben zu Datum, Uhrzeit und beteiligten Personen,
- ggf. eine Gegendarstellung durch die Einrichtung.

Die vollständige Dokumentation wird digital gesichert sowie physisch in einem abschließbaren, zugangsbeschränkten Archiv (z. B. Panzerschrank) aufbewahrt.

2) Prüfung der Meldepflicht, ggf. Meldung

Die Meldung des Vorfalls erfolgt unverzüglich an:

- die Hochschulleitung (Kanzlerin Frau Gerlinde Reich),
- und den Datenschutzbeauftragter (Herr Sven Hirsch).

Wenn das Datenmaterial analog zum Modellfall vollständig unter Kontrolle der Mitarbeiter*innen war ausschließlich auf gesicherten, verschlüsselten Datenträgern transportiert wurde und kein unbefugter Zugriff oder Verlust stattgefunden hat, ist eine Meldung an die Landesdatenschutzbehörde nicht erforderlich. Sollte es jedoch zu einem Datenverlust, unberechtigtem Zugriff oder einer anderweitigen Verletzung des Schutzes personenbezogener Daten kommen, erfolgt unverzüglich eine Meldung gemäß Art. 33 DSGVO an die zuständige Landesdatenschutzbehörde.

3) Entscheidung zum weiteren Umgang mit den betroffenen Daten

Ziel ist eine datenschutzkonforme und Schaden minimierende Handhabung, differenziert nach dem Erkennungsgrad des betroffenen Kindes:

- *Kind ist nicht sichtbar / nicht hörbar*: weitere Nutzung zulässig
- *Kind ist nur von hinten sichtbar*: Nutzung für interne Auswertung zulässig, Weiternutzungssperre für Fortbildungen, Publikationen o. Ä.
- *Kind ist hörbar*: Audiospur wird ausgeblendet
- *Kind ist sichtbar*: Video-Masken werden eingefügt (Schwärzen von Bildausschnitten). Fotografien des Kindes werden ausgedruckt, geschwärzt und erneut kopiert. Der geschwärzte Ausdruck wird in der Datenschutztonne entsorgt.

Die Weiternutzungssperre wird in den Metadaten der betroffenen Videodaten vermerkt (z. B. verbundene Word-Datei oder Datenbank). Die technische Bearbeitung erfolgt mit dem Videoschnittprogramm Adobe Premiere Pro 2025. Die Verfremdung erfolgt so, dass das Original nicht mehr rekonstruiert werden kann. Die Originaldateien werden mittels „DBAN“ gelöscht (Methode: DoD Short – 3 Runden).

4) Technische und organisatorische Umsetzung der Löschung, Dokumentation

Die Löschung erfolgt auf allen Speichermedien (Kamera, Laptop, externe Datenträger). Ein Löschprotokoll wird erstellt, das mindestens folgende Angaben enthält:

- Datum der Löschung,
- Namen der beteiligten Personen (mindestens zwei),
- technische Vorgehensweise (Verfremdung),
- technische Vorgehensweise (Löschung Originaldaten)
- Unterschrift und Ablage im Projektarchiv. (Vgl. Anhang 2.1)

Die Einrichtung muss über das beschriebene Vorgehen informiert werden und diese Information an die betreffende Familie weiterleiten.

2.1 Vorlage Löschprotokoll im Datenschutzfall

Am (*Datum*) waren zwei Erheber*innen des PIPS-Projekts zur Durchführung einer Erhebung in der Einrichtung (*Name der Kita, Adresse*). Dort wurden von einem Kind Videoaufnahmen gemacht, für das kein elterliches Einverständnis zur Videografie vorlag. Der Name des Kindes ist bekannt und kann bei Notwendigkeit angegeben werden.

Im Folgenden wird beschrieben, welche Maßnahmen ergriffen wurden, um die Persönlichkeitsrechte des Kindes zu wahren. Das Vorgehen wurde im Vorfeld mit dem Datenschutzbeauftragten der Fachhochschule Potsdam, Herrn Sven Hirsch (datenschutz@fh-potsdam.de), abgesprochen.

Bei weiteren Fragen wenden Sie sich bitte an die wissenschaftlichen Mitarbeiterinnen des Projekts (pips@fh-potsdam.de)

In folgenden Ausschnitten des Videomaterials vom (*Datum*) war das Kind in der ursprünglichen Aufnahme zu sehen/zuhören.

Dateiname	Änderungen	Länge/Zeitmarke
Datum_Beispielsituation_1.mp4	Video-Masken	00:00 – 00:41
		01:30 – 16:43
		16:52 – 23:39
	Audio-Ausblendungen	01:47 – 01:53
		06:24 – 06:25
		06:27 – 06:29

Die Originalaufnahmen wurden von sämtlichen Datenträgern gelöscht und durch Kopien ersetzt, in denen das betroffene Kind nicht zu erkennen ist.

Die Verfremdung der Daten erfolgte im Programm „Adobe Premiere Pro“. Es erfolgte ein Rendering bei eingefügten Video-Masken und Audio-Ausblendungen, sodass das Original nicht mehr rekonstruiert werden kann. Fotografien des Kindes wurden ausgedruckt, geschwärzt und erneut kopiert. Der geschwärzte Ausdruck wurde in der Datenschutzone entsorgt.

Die Löschung der Daten erfolgte von sämtlichen Datenträgern (*Anzahl externe Festplatten*) mittels „DBAN“ (Methode: DoD Short – 3 Runden).

Die Unkenntlichmachung sowie die Löschung der Aufnahmen des Kindes wurde von (*Name*) vorgenommen und von (*Name wiss. Mitarbeiterin Pips Projekt*) begleitet.

Datum, Ort

Foto-/Videobearbeiter*in

Datum, Ort

Mitarbeiterin PIPS Projekt

3 Child Safeguarding und Kinderschutz

Es folgen:

- Verhaltensrichtlinien zum institutionellen Kinderschutz
- Verpflichtung Datenschutz

Verhaltensrichtlinien

zum institutionellen Kinderschutz (Safeguarding) für Erheber*innen

der Fachhochschule Potsdam und der Universität Potsdam

Ziel

Angehörige der Fachhochschule Potsdam und der Universität Potsdam (einschließlich Studierende, Hilfskräfte, Praktikant*innen sowie auch Honorarkräfte) sind dem Übereinkommen über die Rechte des Kindes (UN-KRK) verpflichtet. Kinderrechte sind nicht nur Gegenstand von Lehre und Forschung (z.B. im Studiengang Frühkindliche Bildungsforschung und im Master Child Rights Studies), sondern der Schutz der Rechte von Kindern sind auch im alltäglichen Handeln in Forschung und Lehre bestmöglich zu gewährleisten. Deshalb verpflichten sich Personen, die Studien mit Kindern durchführen, zu den nachstehenden Verhaltensrichtlinien. Diese sollen Handlungssicherheit geben und dabei unterstützen, ein für Kinder sicheres Umfeld im Rahmen unserer Forschung zu gewährleisten.

Verhaltensrichtlinien

1. Ich achte die Rechte von Kindern und beachte die hierfür geltenden rechtlichen Bestimmungen, das sind insbesondere
 - die Menschenrechtsverträge der Vereinten Nationen und darin insbesondere das Übereinkommen über die Rechte des Kindes (UN-KRK)
 - Gesetze der Bundesrepublik Deutschland zum Kinder- und Jugendschutz und darin insbesondere das Achte Buch des Sozialgesetzbuches zur Kinder- und Jugendhilfe
 - die europäische Datenschutz-Grundverordnung (DSGVO) sowie die geltenden Datenschutzverordnungen der Länder
2. Ich verpflichte mich, alles mir Mögliche zu tun, um Kinder vor Vernachlässigung, vor körperlicher, psychischer und sexueller Misshandlung und Ausbeutung zu bewahren.
3. Ich bin verantwortungsvoll in Bezug auf physische und psychische Nähe und Distanz zu Kindern, das heißt zum Beispiel, dass ich schädliche Formen von Beziehungen sowie unangemessenen Körperkontakt zu Kindern unterlasse.
4. Ich unterlasse verbal und nonverbal gewalttätiges, diskriminierendes, rassistisches und sexistisches Verhalten gegenüber sowie in Gegenwart von Kindern.
5. Ich behandle Kinder als eigenständige Persönlichkeiten und begegne ihnen mit Respekt, unabhängig von z. B. Alter, Geschlecht, Herkunft, Sprache, Religion, Hautfarbe, Behinderung oder politischen Ansichten.

Selbstverpflichtung Safeguarding

6. Ich achte die Meinungen und Äußerungen von Kindern und setze mich dafür ein, dass diese in allen sie berührenden Angelegenheiten entsprechend ihrem Alter und ihrer Reife angemessen berücksichtigt werden.
7. Ich achte darauf, dass Kinder persönliche Dinge, die sie alleine bewältigen können, selbst erledigen.
8. Ich trage dafür Sorge, dass bei dem Umgang mit Kindern stets eine zweite erwachsene Person anwesend oder in Reichweite ist („Zwei-Erwachsenen-Regel“).
9. Ich achte die Sorgeberechtigten der Kinder, respektiere sie in ihrer Verantwortung und gehe gegenüber Kindern, ihren Sorgeberechtigten sowie gegenüber Mitarbeitenden in Bildungs- und Betreuungseinrichtungen sorgsam und transparent mit meiner Rolle als Forschende/r um.
10. Ich stelle sicher, dass Kinder bzw. ihre Sorgeberechtigten sowie die Mitarbeitenden in Bildungs- und Betreuungseinrichtungen sowie anderen Erhebungsorten die Rechte der Kinder im Zusammenhang mit meinem Forschungsvorhaben kennen und über bestehende Melde-, Widerrufs- und Beschwerdemechanismen aufgeklärt sind.
11. Ich trage meinen Teil zu einer Kultur der gegenseitigen Verantwortlichkeit an der Hochschule bei, die ermöglicht, dass sämtliche an der Hochschule aufkommenden Verdachtsfälle von Kindeswohlgefährdung gemeldet und für alle Seiten vertraulich behandelt werden.
12. Ich melde sämtliche mir im Rahmen meiner Tätigkeit für die Fachhochschule Potsdam bzw. für die Universität Potsdam bekanntwerdenden Verdachtsfälle innerhalb von 24 Stunden vertraulich gegenüber der zuständigen Projektleitung.

Erklärung zur Selbstverpflichtung

Ich habe die Verhaltensrichtlinien gelesen und verstanden und verpflichte mich, gemäß diesen Richtlinien zu handeln. Mir ist bewusst, dass die Fachhochschule Potsdam und die Universität Potsdam jedem Verstoß nachgehen werden.

Name der oder des Verpflichteten

Abteilung/ Forschungsgruppe/ Tätigkeit

Ort,

Datum

Unterschrift der oder des Verpflichteten

Verpflichtung auf die Vertraulichkeit personenbezogener Daten

Angehörige der Fachhochschule Potsdam und der Universität Potsdam (einschließlich Studierende, Hilfskräfte, Praktikant*innen sowie auch Honorarkräfte) und insbesondere Personen, die im Rahmen der Lehre und der Forschung in Kontakt mit personenbezogenen Daten kommen, sind verpflichtet, das Datengeheimnis zu wahren.

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Angehörigen der Fachhochschule Potsdam und der Universität Potsdam auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Nach den Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zu unbefugter Offenlegung oder unbefugtem Zugang führt.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Beschäftigungsverhältnisses bzw. nach Abschluss des Studiums, des Praktikums, der Tätigkeit fort.

Frau/Herr

Abteilung/ Forschungsgruppe/ Tätigkeit

erklärt, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten.

Mit Ihrer Unterschrift bestätigen Sie zugleich den Empfang einer Kopie dieser Niederschrift nebst Anlage.

Ort,

Datum

Unterschrift der oder des Verpflichteten

Anlage zur Verpflichtung auf die Vertraulichkeit personenbezogener Daten

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „Personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene 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.

Art. 4 Nr. 2 DS-GVO: „Verarbeitung“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
 2. auf andere Art und Weise zugänglich macht
- und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
 2. durch unrichtige Angaben erschleicht
- und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Quelle: Gesellschaft für Datenschutz und Datensicherheit e.V. (25.05.2018) <https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo>, Stand: Dezember 2017



Partizipative Interaktionen in Pflege-
und Schlafsituationen in Krippen

Selbstverpflichtungserklärung zum Schutz von Kindern gemäß § 72a SGB VIII

Ich,

_____ (Nachname)

_____ (Vorname)

geboren am _____ in _____

achte die körperliche, psychische und geistige Unversehrtheit mir anvertrauter Kinder.
Hierfür gehe ich folgende Verpflichtungen ein:

1. Ich versichere, nicht wegen einer in § 72a Abs. 1 SGB VIII benannten Straftat rechtskräftig verurteilt worden zu sein und keine Kenntnis davon zu haben, dass ein Strafverfahren oder ein staatsanwaltschaftliches Ermittlungsverfahren wegen einer solchen Straftat gegen mich anhängig sind.
2. Ich versichere ferner, nicht in einem anderen Staat außerhalb der Bundesrepublik Deutschland wegen Straftaten verurteilt worden zu sein oder Kenntnis von Ermittlungsverfahren zu haben, die mit den in § 72a SGB VIII benannten Straftaten (Anlage) vergleichbar sind.
3. Ich bin darüber informiert, dass eine nicht wahrheitsgemäße Angabe beziehungsweise ein Verstoß gegen die Mitteilungspflicht personalrechtliche Konsequenzen haben können, die bis zur Beendigung meines Beschäftigungsverhältnisses führen können.
4. Die Inhalte der Selbstverpflichtung habe ich verstanden. Ich stimme mit ihnen überein, werde nach ihnen handeln und sie nach innen und außen vertreten.

Ort, Datum

Unterschrift