PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Leitlinien zu ethischen und rechtlichen Fragen des Datenschutzes in der IKT-Forschung und -Innovation.

BIOMETRIK

Dieses Werk ist lizenziert unter einer Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Dieses Projekt wurde aus Mitteln des Forschungs- und Innovationsprogramms Horizont 2020 der Europäischen Union unter der Finanzhilfevereinbarung Nr. 788039 finanziert. Die Verantwortung für den Inhalt dieses Dokuments tragen allein die Verfasser; die Agentur haftet nicht für die weitere Verwendung der darin enthaltenen Angaben.

Biometrische Daten in der IKT-Forschung und -Innovation

Alessandro Ortalnda, Carlotta Rigotti, Andrés Chomczyk Penedo, Paul De Hert (VUB)

Dieser Teil der Leitlinien wurde von Stefano Leucci (Europäischer Datenschutzbeauftragter), Ernestina Sacchetto (Universität Turin), Catherine Jasserand-Breeman (KU Leuven) und Lydia Belkadi (KU Leuven) überprüft.

Darüber hinaus wurde er von Prof. Gert Vermuelen (Universität Gent) überprüft und validiert.

1 Einleitung und Geltungsbereich des Abschnitts Leitlinien

Forschungstätigkeiten können mitunter die Verarbeitung biometrischer Daten beinhalten, sodass Forscher und Forschungseinrichtungen, die als Verantwortliche oder Auftragsverarbeiter tätig sind, die Datenschutzanforderungen berücksichtigen müssen. Da biometrische Daten innerhalb des EU-Rechtsrahmens einen besonderen Schutz genießen, sollten Forscher, die mit biometrischen Daten arbeiten, nicht nur die allgemeinen Datenschutzanforderungen und die besonderen Anforderungen gemäß Artikel 89 der Europäischen Datenschutz-Grundverordnung (DSGVO) in Bezug auf Forschungstätigkeiten[769] einhalten, sondern auch zusätzliche Garantien umsetzen, die auf die Besonderheiten biometrischer Daten und/oder der biometrischen Verarbeitung zugeschnitten sind.

Die folgenden Leitlinien geben Hinweise darauf, wie die in der europäischen Datenschutzregelung verankerten rechtlichen Verpflichtungen eingehalten werden können. Das Dokument befasst sich insbesondere mit IKT-Forschungstätigkeiten, die die Entwicklung von IKT-Systemen umfassen, die biometrische Daten verwenden. Die Autoren erkennen an, dass solche Systeme heutzutage üblicherweise Technologien der künstlichen Intelligenz verwenden. Da jedoch spezielle Leitlinien für künstliche Intelligenz in dem Dokument „Guidelines on legal and ethical issues regarding artificial intelligence in ICT research and innovation“ zu finden sind, befasst sich das vorliegende Dokument nicht mit künstlicher Intelligenz.

Dieses Dokument richtet sich an IKT-Forschungseinrichtungen, die als Verantwortliche mit biometrischer Technologie arbeiten, und zwar nicht nur an die Forscher, die sich der rechtlichen Verpflichtungen infolge ihrer Forschungstätigkeiten möglicherweise nicht bewusst sind, sondern auch an andere Beteiligte wie Rechtsabteilungen oder Ethikausschüsse, die sich zwar besser mit rechtlichen Aspekten, aber nicht unbedingt mit den besonderen Datenschutzregelungen für biometrische Daten und Forschungstätigkeiten auskennen. Damit beide Zielgruppen problemlos auf den Inhalt der Leitlinien zugreifen können, wird in dem Dokument versucht, ein Gleichgewicht zwischen technischen Details (sowohl in Bezug auf IKT und biometrische Technologie als auch auf das Datenschutzrecht) und allgemeiner Zugänglichkeit herzustellen.

[769] Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (2016)

2 Definitionen

2.1 Besondere Kategorien personenbezogener Daten

Vor der Definition biometrischer Daten sollten die „besonderen Kategorien personenbezogener Daten“ beachtet werden, die gemeinhin auch als „sensible Daten“ bekannt sind. In der Tat werden in Artikel 9.1 DSGVO biometrische Daten (oder zumindest einige von ihnen; siehe 2.2 Biometrische Daten) in dieser breiteren Gruppe zusammengefasst:

Besondere Kategorien personenbezogener Daten
Daten, aus denen die rassische und ethnische Herkunft hervorgeht
Daten, aus denen politische Meinungen hervorgehen
Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen
Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht
Genetische Daten
Biometrische Daten (zur eindeutigen Identifizierung einer natürlichen Person)
Gesundheitsdaten
Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person

Artikel 9 DSGVO untersagt standardmäßig die Verarbeitung besonderer Kategorien personenbezogener Daten, es sei denn, es liegt eine der in Artikel 9 Absatz 2 DSGVO aufgeführten Ausnahmen vor. Eine dieser Ausnahmen gilt, wenn die „Verarbeitung [...] für wissenschaftliche oder historische Forschungszwecke erforderlich ist“.

Es ist anzumerken, dass es für die Erfüllung nicht ausreicht, dass eine Verarbeitung besonderer Kategorien personenbezogener Daten eine der in Artikel 9 Absatz 2 DSGVO aufgeführten Ausnahmen erfüllt. Darüber hinaus muss der Verantwortliche vor Beginn der Verarbeitung eine geeignete Rechtsgrundlage für die Datenverarbeitung ermitteln (siehe Abschnitt 3.2.3 Ermittlung der am besten geeigneten Rechtsgrundlage)[770].

Die Verantwortlichen sollten sich auch darüber im Klaren sein, dass die Mitgliedstaaten gemäß Artikel 9 Absatz 4 DSGVO zusätzliche Bedingungen und Beschränkungen für die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten einführen bzw. anwenden können. Daher sollten Verantwortliche, die diese besonderen Kategorien verarbeiten wollen, immer prüfen, ob es anwendbare spezifische nationale Anforderungen gibt. Weitere Informationen finden Sie in den vom Panelfit-Konsortium erstellten nationalen Berichten (abrufbar unter https://www.panelfit.eu/national-reports/).

Obwohl bestimmte Daten für sich genommen keine besonderen Kategorien personenbezogener Daten darstellen, können sie in Verbindung mit anderen Daten besondere Kategorien personenbezogener Daten darstellen. So sind beispielsweise die Adresse und die

[770] Siehe auch: Ludmilla Georgieva and Christopher Kuner, Article 9. Processing of Special Categories of Personal Data, in *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford, United Kingdom: Oxford University Press, 2019), 376–77.

Muttersprache einer Person keine besondere Kategorie personenbezogener Daten. Wenn jedoch Name, Geburtsort und andere Daten der betroffenen Person dem Datensatz beigefügt werden, könnte die Kombination genügend Informationen bereitstellen, um die rassische oder ethnische Herkunft der betroffenen Person mit einem angemessenen Grad an Sicherheit zu ermitteln. In diesem Szenario sollten die Daten den gleichen Anforderungen und Beschränkungen wie besondere Kategorien personenbezogener Daten unterliegen, auch wenn sie es für sich genommen nicht sind.

Datensatz 1	**Datensatz 2**
Adresse: Washington D.C.	Adresse: Washington D.C.
Muttersprache: Französisch	Muttersprache: Französisch
	Name: Seydou Kablan Bakayoko
	Geburtsort: Abidjan
	Andere bekannte Sprache: Cebaara, Englisch
	Grundschule: École Konan Raphael, Abidjan
Datensatz 1 enthält keine Informationen über die rassische oder ethnische Herkunft der betroffenen Person	*Die von Datensatz 2 gelieferten Informationen könnten als ausreichend angesehen werden, um die rassische oder ethnische Herkunft der betroffenen Person (mit einem angemessenen Grad an Sicherheit) zu ermitteln.*

Es wird nochmals darauf hingewiesen, dass die Daten einen angemessenen Grad an Sicherheit bieten sollten. Dieser Grad an Sicherheit ist kontextabhängig und muss von Fall zu Fall bewertet werden.

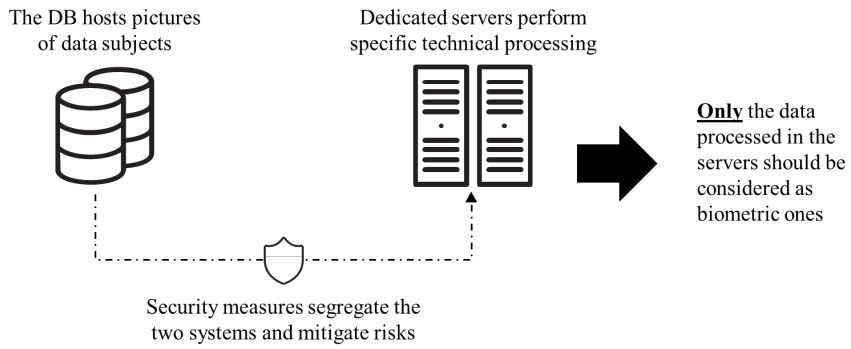
2.2 Biometrische Daten

Der Begriff „biometrische Daten“ ist in Artikel 4 Absatz 14 DSGVO definiert. Demnach sind biometrische Daten „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen“. Laut der Definition müssen personenbezogene Daten vier *Kriterien*[771] erfüllen, damit sie als „biometrisch“ gelten.

Erstens muss es sich um „personenbezogene Daten“ handeln, die in Artikel 4 Absatz 1 DSGVO als „Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ definiert sind. Zweitens erfordern sie „spezielle technische Verfahren“, um die Informationen aus der Rohdatenquelle zu gewinnen (z. B. die Extraktion von Gesichtszügen aus einem Bild). In Erwägungsgrund 51 DSGVO heißt es: „Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von

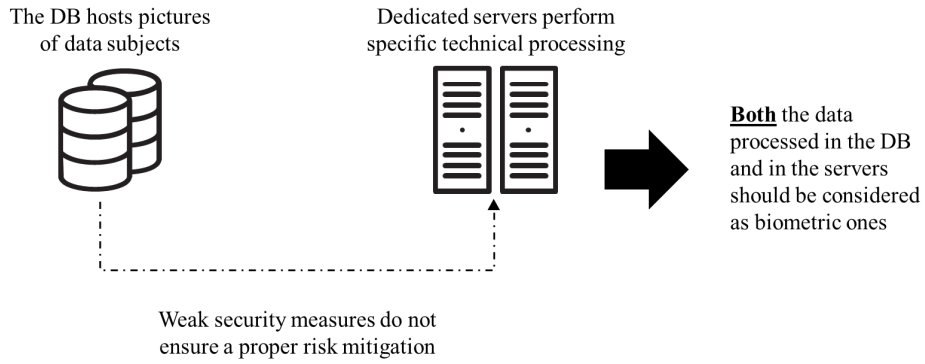
[771] Zur Analyse der Definition in der Datenschutz-Grundverordnung siehe: C. Jasserand, Legal Nature of Biometric Data: From “Generic” Personal Data to Sensitive Data, *European Data Protection Law Review* 2, Nr. 3 (2016): 297–311, https://doi.org/10.21552/EDPL/2016/3/6.

personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen“. Somit sind biometrische Daten ohne „spezielle technische Verfahren“ zu deren Gewinnung keine biometrischen Daten im Sinne der DSGVO[772]. Aber auch wenn Daten in einem bestimmten Stadium keine biometrischen Daten sind, können sie Teil einer Datenverarbeitung sein, die sie in einem späteren Stadium zu biometrischen Daten macht. So können beispielsweise in einer Datenbank Bilder gespeichert sein, die zu einem späteren Zeitpunkt durch ein spezielles technisches Verfahren zur biometrischen Identifizierung verwendet werden (sodass sie vorerst noch keine biometrischen Daten darstellen). Stellen Sie sich ein Szenario vor, in dem diese Datenbank direkt mit dem System verbunden ist, das die biometrische Identifizierung durchführt (siehe auch Abschnitt 2.3 Biometrisches System). In diesem Fall könnten Unbefugte diese Verbindung ausnutzen, um auf biometrische Daten zuzugreifen. Sie könnten beispielsweise die in der Datenbank gespeicherten (nicht biometrischen) Bilder exfiltrieren, in das System zur biometrischen Identifizierung eindringen, das Bild durchlaufen lassen und die biometrische Identifizierung durchführen, wodurch sie Zugang zu den biometrischen Daten erhalten. In diesem Szenario ermöglicht eine schwache Sicherheit, dass externe Parteien biometrische Daten erhalten können, auch wenn diese biometrischen Daten noch gar nicht existieren. Die Verantwortlichen sollten dies unter dem Gesichtspunkt des Risikomanagements betrachten. Wenn sie keine angemessene Risikominderung für die nicht-biometrischen Daten gewährleisten können (d. h. Auswertungsrisiken), sollten diese Datensätze als biometrische Daten betrachtet werden und allen rechtlichen Anforderungen unterliegen, auch wenn sie – für sich genommen – nicht die Kriterien für die Einstufung als biometrische Daten erfüllen.



Biometrische Daten Szenario 1

[772] In der Wissenschaft ist umstritten, ob dies auch auf technische Verarbeitungsverfahren angewandt werden sollte, die Voraussetzung für die Identifizierung sind, wie etwa die bloße Speicherung in Datenbanken. Siehe z. B.: Kindt, *Having yes, using no? About the new legal regime for biometric data*, Computer Law and Security Review, 34, 2018, Seiten 523–538. Eine Analyse der Probleme im Zusammenhang mit anderen Formaten als Lichtbildern finden Sie in: Andras Nautsch *et al.*, Preserving privacy in speaker and speech characterisation, Computer Speech & Language, 58, 2018, Seite 445.



Biometrische Daten Szenario 2

Das dritte *Kriterium* bezieht sich auf die Merkmale der betroffenen Personen, die durch die oben erwähnte speziellen technischen Verfahren erfasst werden. Diese Merkmale können „physisch", „physiologisch" oder „verhaltenstypisch" sein und unterscheiden sich von zufälligen Eigenschaften wie der Adresse der betroffenen Person, ihrem Standort zu einem bestimmten Zeitpunkt, Beschäftigungsdaten usw. Das vierte und letzte *Kriterium* besagt, dass personenbezogene Daten nur dann als biometrisch gelten, wenn sie die eindeutige Identifizierung einer natürlichen Person ermöglichen oder bestätigen. In der Tat identifizieren biometrische Daten Personen nicht unbedingt *per se* eindeutig. So könnten biometrische Daten beispielsweise verwendet werden, um zwischen Menschen und Tieren oder zwischen Männern und Frauen zu unterscheiden[773]. Anders als bei anderen Identifikatoren wie Namen oder Identifizierungscodes führt die Verarbeitung biometrischer Daten jedoch nicht zu einer eindeutigen Identifizierung. Vielmehr ermöglicht sie die Identifizierung von Personen mit einem gewissen Grad an Wahrscheinlichkeit. Nach gängiger Auffassung sind Daten als biometrisch zu betrachten, „auch wenn die in der Praxis angewandten Modelle für ihre technische Messung in gewissem Umfang auf Wahrscheinlichkeiten beruhen"[774].

2.3 Biometrisches System

In diesem Kapitel wird der Begriff „biometrisches System" definiert als ein System, das in der Lage ist, natürliche Personen (mit einem gewissen Grad an Wahrscheinlichkeit) eindeutig zu identifizieren, indem es spezielle technische Verfahren verwendet, die sich auf die physischen, physiologischen oder verhaltenstypischen Merkmale dieser natürlichen Personen beziehen[775]. Die Definition gilt sowohl für Komplettsysteme, die alle Schritte durchführen (z. B. Datenerhebung, Datenverarbeitung, Datenspeicherung usw.), als auch für Systemcluster, die jeweils einzelne Schritte durchführen (z. B. ein Netz von Datenerhebungsmodulen auf der Grundlage einer Kamera, einer biometrischen Zuordnungssoftware und einer Datenbank zur Speicherung). Wenn ein System, das einen oder mehrere Einzelschritte durchführt (nachstehend „System X"), an sich kein biometrisches System im Sinne der obigen Definition ist, aber dennoch Teil eines Systemclusters ist, zu denen auch biometrische Systeme gehören, sollte das System X als biometrisches System betrachtet werden, es sei denn, es kann – möglicherweise durch dokumentierte Belege –

[773] Siehe beispielsweise: 14 Misunderstandings with Regard to Identification and Authentication' (Agencia Espanola Proteccion Datos, European Data Protection Supervisor, Juni 2020), 3.

[774] Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", 2007, 8. Siehe auch: Artikel-29-Datenschutzgruppe, Stellungnahme 03/2012 zu Entwicklungen im Bereich biometrischer Technologien, 2012, 6.

[775] Obwohl die Internationale Organisation für Normung detaillierte Vokabularien im Zusammenhang mit der Biometrie erstellt hat, die auch die Definition des Begriffs „biometrisches System" enthalten, ziehen die Verfasser des vorliegenden Dokuments eine Definition vor, die auf den Bestimmungen der DSGVO beruht. Siehe: International Standardization Organization and International Electrotechnical Commission, ISO/IEC 2382-37 – Information Technology – Vocabulary – Part 37: Biometrics, 2017.

nachgewiesen werden, dass es keine biometrischen Daten verarbeitet und dass die Risiken wirksam gemindert werden (z. B. das Risiko, dass unbefugte Dritte das System X nutzen, um Zugang zu einem anderen, direkt mit dem System X verbundenen System zu erhalten, in dem biometrische Daten verarbeitet werden).

Biometrische Systeme stützen sich häufig auf die Technologie der künstlichen Intelligenz. Der Einsatz dieser künstlichen Intelligenz birgt weitere Datenschutzrisiken, mit denen sich die Verantwortlichen befassen müssen. Daher empfiehlt es sich, das Dokument „Guidelines on ethical and legal issues regarding artificial intelligence in ICT research and innovation“ zu konsultieren.

2.4 Arten von biometrischen Daten

Wie bereits erwähnt, können verschiedene biometrische Daten aus unterschiedlichen Merkmalen einer natürlichen Person abgeleitet werden – physische, physiologische und verhaltenstypische. In diesem Abschnitt werden diese verschiedenen Arten biometrischer Daten erläutert. Die folgende Taxonomie ist nicht als Standard festgelegt, wobei bestimmte Arten biometrischer Daten von verschiedenen Experten unterschiedlich kategorisiert werden können. Beispielsweise werden in Taxonomien manchmal physiologische biometrische Daten in die Kategorie der physischen biometrischen Daten zusammengefasst.

2.4.1 Physische biometrische Daten

Physische biometrische Daten können durch die Erfassung charakteristischer Körpermerkmale von Personen gewonnen werden. Die Unterscheidbarkeit dieser Merkmale kann dann als Identifikator genutzt werden. Zu den gebräuchlichsten physischen biometrischen Merkmalen gehören Fingerabdrücke, die Form der Hand, Gesichtsmerkmale (wie die Rundung des Gesichts, der Abstand zwischen den Augen usw.) und Merkmale der Iris.

2.4.2 Physiologische biometrische Daten

Physiologische biometrische Daten können durch die Beobachtung von Körperfunktionen und die Erfassung der mit ihnen verbundenen charakteristischen Muster gewonnen werden. Einige der gebräuchlichsten physiologischen biometrischen Daten werden aus Elektrokardiogrammen (EKG), Atmungsmustern und Elektroenzephalogrammen (EEG) gewonnen.

Obwohl physische biometrische Daten oft als Synonym für physiologische biometrische Daten verwendet werden (und umgekehrt), sind die Autoren der Meinung, dass eine Unterscheidung von Vorteil sein könnte, um die Diskussion besser zu strukturieren. Dies ist insbesondere in Anbetracht neuerer Studien über die Beziehung zwischen biometrischer Technologie und bestimmten physiologischen Funktionen wie z. B. neurophysiologischen Funktionen von Vorteil[776].

2.4.3 Verhaltenstypische biometrische Daten

Verhaltenstypische biometrische Daten können durch die Beobachtung des Verhaltens von Personen gewonnen werden, um charakteristische Muster in diesem Verhalten zu erkennen. Einige Verhaltensweisen sind den Personen inhärent (z. B. der Gang oder die Stimme), während andere nur durch die Interaktion mit bestimmten Hilfsmitteln an den Tag gelegt werden (z. B. Handschrift, Tastaturdynamik und Mausbewegungen).

[776] Siehe beispielsweise: Patrizio Campisi und Daria La Rocca, Brain Waves for Automatic Biometric-Based User Recognition, *IEEE Transactions on Information Forensics and Security* 9, Nr. 5 (Mai 2014): 782–800, https://doi.org/10.1109/TIFS.2014.2308640.

Im Gegensatz zu physischen biometrischen Daten erfordern verhaltenstypische biometrische Daten eine Beobachtung der Personen, was eine Zeitvariable in die Bewertung einführt[777]. Es wird oft vorgebracht, dass verhaltenstypische biometrische Daten trotz ihrer größeren Anfälligkeit für momentane Schwankungen und Veränderungen im Laufe des Lebens den Vorteil haben, dass sie weniger in die Privatsphäre eingreifen und kostengünstig sind.[778] Einige Wissenschaftler haben jedoch festgestellt, dass verhaltenstypische biometrische Daten im Vergleich zu anderen Arten biometrischer Daten größere Risiken für den Schutz der Privatsphäre mit sich bringen könnten,[779] da sie weitere Informationen über die Betroffenen preisgeben können, die mitunter sehr sensibel sind, wie z. B. der Gesundheitszustand.[780]

2.5 Forschungstätigkeiten

Der Begriff „Forschungstätigkeit" ist im Rechtsrahmen nicht eindeutig definiert. Gemäß Erwägungsgrund 159 DSGVO sollte „die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken weit ausgelegt werden und die Verarbeitung für beispielsweise die technologische Entwicklung und die Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen".

Der Europäische Datenschutzbeauftragte (EDSB) sieht das Hauptziel von Forschungstätigkeiten darin, „das kollektive Wissen und das Wohlergehen der Gesellschaft zu steigern und nicht in erster Linie einem oder mehreren privaten Interessen zu dienen"[781]. Die bloße Erforschung neuer kommerzieller Technologien stellt daher nach dem derzeitigen Rechtsrahmen anscheinend keine „Forschungstätigkeit" dar (siehe Abschnitt 4.1 „Data protection and scientific research" im Dokument „Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation").

3 Biometrische Technologie in der IKT-Forschung und -Innovation Leitlinien

Der folgende Abschnitt gibt einen Überblick über praktische Schritte, die bei der Entwicklung biometrischer Technologien oder beim Einsatz solcher Technologien im Rahmen der IKT-Forschung und -Innovation unternommen werden können. Diese Schritte können es Forschern erleichtern die Datenschutzverpflichtungen einzuhalten. Die Empfehlungen gelten für biometrische Systeme, unabhängig davon, welche biometrischen Daten sie erzeugen und verarbeiten (weitere Informationen siehe 2.3 „Biometrisches System").

---

[777] Siehe: Roman V. Yampolskiy und Venu Govindaraju, Behavioural Biometrics: A Survey and Classification, *International Journal of Biometrics* 1, Nr. 1 (2008): 81, https://doi.org/10.1504/IJBM.2008.018665.

[778] Siehe: Madeena Sultana, Padma Polash Paul und Marina Gavrilova, A Concept of Social Behavioral Biometrics: Motivation, Current Developments, and Future Trends, in *2014 International Conference on Cyberworlds* (2014 International Conference on Cyberworlds (CW), Santander, Cantabria, Spain: IEEE, 2014), 271–78, https://doi.org/10.1109/CW.2014.44.

[779] Siehe: Günter Schumacher, Behavioural Biometrics: Emerging Trends and Ethical Risks, in *Second Generation Biometrics: The Ethical, Legal and Social Context*, Herausgeber: Emilio Mordini und Dimitros Tzovaras (Springer, 2012).

[780] Siehe beispielsweise: Marcos Faundez-Zanuy et al., Handwriting Biometrics: Applications and Future Trends in e-Security and e-Healt', *Cognitive Computation* 12, Nr. 5 (September 2020): 940–53, https://doi.org/10.1007/s12559-020-09755-z.

[781] Europäischer Datenschutzbeauftragter, A Preliminary Opinion on Data Protection and Scientific Research (European Data Protection Supervisor, 6 Januar 2020).

3.1 Designphase

In der Designphase legen die Forscher den Rahmen fest, indem sie die Ziele und Bedürfnisse der Forschungstätigkeit bestimmen.

3.1.1 Identifizierung der Ziele, ob die Tätigkeit als „Forschung“ eingestuft werden kann sowie der Rollen der Beteiligten

Die Forscher sollten zunächst das Ziel ihrer Tätigkeit bestimmen (beispielsweise eine theoretische Studie durchführen, ein biometrisches System entwickeln, ein bestehendes System testen usw.). Dies ist ein wichtiger Schritt – nicht nur um die Zwecke festzulegen, für die personenbezogene Daten erhoben werden, sondern auch, um den Forschern die Ermittlung zu erleichtern, ob die Tätigkeit als „Forschung“ einzustufen ist und folglich die spezifischen rechtlichen Bestimmungen für Forschungstätigkeiten gelten. Artikel 89 Absatz 2 DSGVO beispielsweise sieht mehrere Ausnahmen in Bezug auf die Verarbeitung personenbezogener Daten zu Forschungszwecken vor. Insbesondere erkennt der Artikel an, dass bestimmte Rechte der betroffenen Personen (Recht auf Auskunft, Recht auf Berichtigung, Recht auf Einschränkung, Recht auf Widerspruch. Weitere Informationen finden Sie im Dokument „Rechte der betroffenen Personen“) die Verwirklichung der spezifischen Forschungszwecke beeinträchtigen oder unmöglich machen würden. Daher sieht er Ausnahmen von diesen Rechten vor, wenn zwei *Kriterien* erfüllt sind. Erstens muss die Ausnahme ausdrücklich im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehen sein. Forscher dürfen somit neben den Bestimmungen der DSGVO nur dann von der Verpflichtung zur Einhaltung dieser Rechte befreit werden, wenn es in einem nationalen Gesetz oder im EU-Recht andere spezifische Rechtsgrundlagen als die DSGVO gibt (siehe Abschnitt 3.2.3 „Ermittlung der am besten geeigneten Rechtsgrundlage“). Zweitens müssen die Forscher gemäß Artikel 89 Absatz 1 DSGVO geeignete technische und organisatorische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen ergreifen. Angesichts der potenziellen Auswirkungen der Forschungstätigkeit auf die Einhaltung der Vorschriften sollte unbedingt sofort ermittelt werden, ob die Tätigkeit als „Forschung“ einzustufen ist.

Ein korrektes Scoping der Tätigkeiten ist ebenfalls notwendig, damit die Forscher die mit der Forschung verbundenen Datenschutzrisiken verstehen. So erfordern beispielsweise Systeme, die im Gesundheitswesen oder bei der Strafverfolgung eingesetzt werden sollen, wahrscheinlich genauere Ergebnisse als Systeme, die für Freizeitaktivitäten wie beispielsweise Musik-Streaming-Dienste bestimmt sind. Da die Genauigkeit eines Systems in bestimmten Fällen von der Menge der zu verarbeitenden personenbezogenen Daten abhängen kann (z. B. beim Training eines KI-Algorithmus), könnte der Bedarf an größerer Genauigkeit zu mehr Datenschutzrisiken führen. Die Forscher sollten eindeutig bestimmen, welches Maß an Genauigkeit das System erfüllen muss, und Strategien zur Gewährleistung festlegen, dass diese Genauigkeit durch die Einführung eines möglichst niedrigen Risikoniveaus erreicht wird, zum Beispiel durch die Begrenzung der Menge der verarbeiteten personenbezogenen Daten (siehe Abschnitt 3.3. „Data Minimisation“ im Dokument „Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation“).

Fernen müssen die Forscher ihre eigene Rolle und die Rolle der anderen beteiligten Akteure verstehen. Forscher müssen ihre Mitwirkung an der erwarteten Datenverarbeitung prüfen, um zu verstehen, ob sie (d. h. die Einrichtung, für die sie arbeiten) die Hauptverantwortung für die Datenverarbeitung tragen (Verantwortlicher), ob sie die Rolle des Verantwortlichen gemeinsam mit anderen Einrichtungen ausüben (gemeinsam Verantwortliche) oder ob sie Daten im Auftrag anderer Einrichtungen verarbeiten (Auftragsverarbeiter). Die verschiedenen Rollen bringen eine unterschiedliche Verteilung der Verantwortlichkeiten und Haftungen mit sich.

3.1.2 Bestätigung der Notwendigkeit der Verarbeitung biometrischer Daten

Wie bereits erwähnt, untersagt die DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten – also auch biometrischer Daten – es sei denn, es gelten besondere Ausnahmen (siehe Abschnitt 3.2.3 „Ermittlung der am besten geeigneten Rechtsgrundlage“). Forscher müssen somit, wenn sie die Verarbeitung biometrischer Daten planen, sicher sein, dass die Verarbeitung dieser Daten notwendig ist, um das Ziel der Forschungstätigkeit zu erreichen. Das Forschungsziel könnte zum Beispiel in der Entwicklung und Prüfung einer neuen Methode bestehen, die die Genauigkeit von Systemen zur Erkennung von Gesichtsmerkmalen erhöhen soll. In diesem Fall besteht das Ziel nicht darin, die Genauigkeit der eindeutigen Identifizierung von Personen zu erhöhen, sondern nur die Genauigkeit der Erkennung von Gesichtsmerkmalen. Die Forscher könnten sich in diesem Fall auf computergenerierte Gesichtsbilder anstelle von Bildern einer bestehenden natürlichen Person stützen, sodass keine biometrischen Personendaten verarbeitet werden müssen. Bei der Systementwicklung sollten die Forscher auch berücksichtigen, wie das biometrische System nach seiner Einführung biometrische Daten verarbeiten wird. Die Forscher müssen im Voraus alle technischen und organisatorischen Maßnahmen ergreifen, um sicherzustellen, dass jedes potenzielle Risiko gemindert wird und die Datenverarbeitung nach der Einführung im Einklang mit dem rechtlichen Rahmen erfolgt.

3.2 Vorbereitungsphase

In der Vorbereitungsphase legen die Forscher die Grundlagen für die Forschung, indem sie alle vorbereitenden Arbeiten für die Forschungstätigkeit durchführen.

3.2.1 Benennung eines Datenschutzbeauftragten

Der Datenschutzbeauftragte (DSB) unterstützt den Verantwortlichen oder den Auftragsverarbeiter bei der Einhaltung der Datenschutznormen. Artikel 37 DSGVO schreibt die Benennung eines DSB in fünf konkreten Fällen vor.

Anforderungen für die Benennung eines Datenschutzbeauftragten	
Anforderung 1	„Die Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln”, Artikel 37 Absatz 1 DSGVO
Anforderung 2	„Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen”, Artikel 37 Absatz 1 DSGVO
Anforderung 3	„Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9”, Artikel 37 Absatz 1 DSGVO
Anforderung 4	„Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung […] von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10”, Artikel 37 Absatz 1 DSGVO
Anforderung 5	„Der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen”, Artikel 37 Absatz 4

	DSGVO

Die Anforderungen 1 und 3 sind für dieses Dokument besonders relevant. Anforderung 1 ist relevant, weil Forschungseinrichtungen häufig öffentliche Einrichtungen sind, wie z. B. öffentliche Krankenhäuser und öffentliche Universitäten. In einem solchen Fall sieht Artikel 37 Absatz 3 DSGVO vor, dass „ein gemeinsamer Datenschutzbeauftragter für mehrere solcher Behörden oder Stellen benannt werden kann". Öffentliche Krankenhäuser könnten beispielsweise keinen DSB benannt haben, sich aber auf einen solchen verlassen, um seine Dienste zu erbringen. Anforderung 3 ist insofern relevant, als sie die Verarbeitung besonderer Kategorien personenbezogener Daten – wie biometrischer Daten – als eines der drei Kriterien für die obligatorische Benennung eines DSB nennt. Die beiden anderen *Kriterien* kommen zum Tragen, wenn die Verarbeitung personenbezogener Daten im Rahmen einer Kerntätigkeit erfolgt und umfangreich ist. Die Begriffe „Kerntätigkeit" und „umfangreiche Verarbeitung" sind in der DSGVO nicht ausdrücklich definiert. Die Artikel-29-Datenschutzgruppe (WP29) gibt jedoch in ihren Leitlinien in Bezug auf Datenschutzbeauftragte Auslegungshilfen. Demnach sind Kerntätigkeiten „die wichtigsten Arbeitsabläufe, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters erforderlich sind"[782] und schließen somit unterstützende oder untergeordnete Tätigkeiten aus. Im Zusammenhang mit der IKT-Forschung und -Innovation könnte dies als jede Tätigkeit verstanden werden, die direkt mit der Durchführung von IKT-Forschung und der Verwirklichung von IKT-Innovation zusammenhängt, wie z. B. im Fall der Entwicklung eines biometrischen Systems. Was das *Kriterium* der umfangreichen Verarbeitung betrifft, so knüpft die WP29 es an „die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung; das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten; die Dauer oder Permanenz der Datenverarbeitungstätigkeit; [und] die geografische Ausdehnung der Verarbeitungstätigkeit"[783].

Wenn die Benennung eines DSB erforderlich ist, sollte dies so früh wie möglich geschehen. Denn gemäß Artikel 39 Absatz 1 Buchstabe a DSGVO gehört die Unterrichtung und Beratung des Verantwortlichen in allen Phasen der Forschung zu den Aufgaben des Datenschutzbeauftragten. Die frühestmögliche Einschaltung eines Datenschutzbeauftragten stellt daher sicher, dass die Forscher angemessen beraten werden, wie die Compliance-Anforderungen zu erfüllen sind.

Die Kontaktdaten des Datenschutzbeauftragten sollten veröffentlicht und den betroffenen Personen zugänglich gemacht werden.

3.2.2 Ermittlung des Datenerhebungsansatzes

Der nächste Schritt für die Forscher besteht in der Ermittlung, ob personenbezogene Daten direkt bei den betroffenen Personen oder indirekt (z. B. über andere Forscher, kommerzielle Datenbanken usw.) erhoben werden sollen. Dies verpflichtet die Forscher zwar nicht zwangsläufig zur Wahl einer bestimmten Rechtsgrundlage (siehe Abschnitt 3.2.3 „Ermittlung der am besten geeigneten Rechtsgrundlage"), könnte diese Entscheidung jedoch beeinflussen. Wenn Forscher beispielsweise beschließen, Daten direkt bei den betroffenen Personen zu erheben, könnten sie die Einwilligung als Rechtsgrundlage vorziehen, da ohnehin eine direkte Beziehung zu den betroffenen Personen hergestellt wird. Außerdem ändern sich gemäß Artikel 13 und 14 DSGVO je nachdem, ob ein direkter oder indirekter Ansatz für die Datenerhebung gewählt wird, die Informationen, die die Verantwortlichen den betroffenen Personen bereitstellen müssen.

[782] Artikel-29-Datenschutzgruppe, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), April 2017, 20.
[783] Artikel 29-Datenschutzgruppe, 21.

Informationen, die den betroffenen Personen je nach Erhebungsverfahren zur Verfügung gestellt werden müssen		
	Direkt	**Indirekt**
Identität und Kontaktdaten des Verantwortlichen	☐	☐
Gegebenenfalls Identität und Kontaktdaten des Vertreters des Verantwortlichen	☐	☐
Kontaktdaten des Datenschutzbeauftragten	☐	☐
Zwecke der Verarbeitung	☐	☐
Kategorien der betroffenen personenbezogenen Daten		☐
Rechtsgrundlage für die Verarbeitung	☐	☐
Gegebenenfalls berechtigte Interessen des Verantwortlichen oder eines Dritten	☐	☐
Empfänger oder Kategorien von Empfängern der personenbezogenen Daten	☐	☐
Die Absicht des Verantwortlichen, personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln	☐	☐
Im Falle einer Übermittlung das Vorhandensein oder Nichtvorhandensein eines Angemessenheitsbeschlusses der Kommission oder gegebenenfalls ein Hinweis auf die Garantien und die Mittel, um eine Kopie der Daten zu erhalten	☐	☐
Zeitraum, für den die personenbezogenen Daten gespeichert werden, bzw., falls dies nicht möglich ist, die Kriterien zur Festlegung dieses Zeitraums	☐	☐
Das Recht, Auskunft über die die betroffene Person betreffenden Daten und deren Berichtigung oder Löschung oder die Einschränkung der Verarbeitung zu verlangen oder der Verarbeitung zu widersprechen, sowie das Recht auf Datenübertragbarkeit	☐	☐
Im Falle der „ausdrücklichen Einwilligung" als Rechtsgrundlage für die Verarbeitung das Recht, die Einwilligung jederzeit zu widerrufen	☐	☐
Das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen	☐	☐
Die Quelle der personenbezogenen Daten und gegebenenfalls, ob sie aus öffentlich zugänglichen Quellen stammen		☐
Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder eine Voraussetzung für den Abschluss eines Vertrags ist und ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, sowie die Folgen einer Nichtbereitstellung dieser Daten	☐	

Das Vorliegen einer automatisierten Entscheidungsfindung, einschließlich Profiling	☐	☐
Im Falle einer automatisierten Entscheidungsfindung Angaben zur Logik, zur Bedeutung der Verarbeitung und zu den voraussichtlichen Folgen für die betroffene Person	☐	☐

Die DSGVO räumt ein, dass es Fälle geben kann, in denen diese Informationspflicht nicht anwendbar ist, und führt in Artikel 14 Absatz 5 Ausnahmen auf. Diese Ausnahmen sind anzuwenden, wenn:

- die betroffene Person bereits über die Informationen verfügt;
- die Erteilung dieser Informationen:
  - sich als unmöglich erweist;
  - einen unverhältnismäßigen Aufwand erfordern würde;
  - voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde.

In diesem Zusammenhang ist unbedingt zu beachten, dass diese Ausnahme insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien gilt.

Außerdem muss der Verantwortliche in solchen Fällen geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit ergreifen.

- Der Verantwortliche ist durch Rechtsvorschriften der Union oder der Mitgliedstaaten verpflichtet, die personenbezogenen Daten zu erlangen oder offenzulegen; oder
- die personenbezogenen Daten müssen gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden.

Unabhängig davon, wie die Daten erhoben werden, muss der Verantwortliche geeignete Maßnahmen zur Gewährleistung ergreifen, dass die Daten genau und auf dem neuesten Stand sind (z. B. regelmäßige Überprüfung der Genauigkeit). Die Erhebung von Daten direkt bei den betroffenen Personen kann dazu beitragen, das Risiko der Ungenauigkeit zu verringern (insbesondere bei biometrischen verhaltenstypischen Daten, die sich im Laufe der Zeit ändern können). Außerdem muss der Verantwortliche in jeder Prozessphase für Transparenz sorgen (siehe Abschnitt 3.1. „Lawfulness, fairness and transparency“ im Dokument „Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation“). Eine ausführlichere Erläuterung des Rechts auf Auskunft und seiner Nuancen finden Sie im Dokument „Rechte der betroffenen Personen“.

3.2.3 Ermittlung der am besten geeigneten Rechtsgrundlage

Einer der wichtigsten Schritte unter dem Gesichtspunkt des Datenschutzes ist die Ermittlung der Rechtsgrundlage für die Verarbeitung personenbezogener Daten, die in Artikel 6 DSGVO aufgeführt sind. Wie bereits erwähnt, ist die Verarbeitung biometrischer Daten jedoch untersagt und kann nur im Falle der Anwendbarkeit bestimmter Ausnahmen erfolgen. Diese sind in Artikel 9 Absatz 2 DSGVO vorgesehen und lassen sich in zwei Arten unterteilen. Solche, die sofort gültig und anwendbar sind, und solche, die zusätzliche Rechtsvorschriften der Union oder der Mitgliedstaaten erfordern, bevor sie zur Rechtfertigung einer Verarbeitung biometrischer Daten herangezogen werden können.

Verfügbare Rechtsgrundlagen für die Verarbeitung biometrischer Daten gemäß der DSGVO	
	Erfordert zusätzliches Unionsrecht oder Recht der Mitgliedstaaten
Ausdrückliche Einwilligung	
Arbeitsrecht, Recht der sozialen Sicherheit und Sozialschutz	?
Lebenswichtige Interessen	
Tätigkeiten von Vereinigungen oder sonstigen Organisationen ohne Gewinnerzielungsabsicht	
Die Daten wurden von der betroffenen Person öffentlich gemacht	
Rechtsansprüche oder Handlungen der Gerichte	
Erhebliches öffentliches Interesse	?
Versorgung im Gesundheits- oder Sozialbereich	?
Öffentliches Interesse im Bereich der öffentlichen Gesundheit	?
Archivzwecke, Forschungszwecke oder statistische Zwecke	?

Wenn eine dieser Ausnahmen zutrifft, kann der Verantwortliche eine der in Artikel 6 DSGVO aufgeführten Rechtsgrundlagen wählen und die personenbezogenen Daten entsprechend verarbeiten.

Von den zehn Ausnahmen nach Artikel 9 Absatz 2 DSGVO sind zwei für das vorliegende Dokument besonders relevant. Die erste ist die Anforderung einer „ausdrücklichen Einwilligung". Im Zusammenhang mit der Verarbeitung biometrischer Daten muss die Einwilligung der betroffenen Personen „ausdrücklich" sein, d. h. es muss sich um eine klare, auf den konkreten Fall bezogene und unmissverständliche Erklärung handeln, dass die betroffenen Personen in die Verarbeitung ihrer biometrischen Daten für die von dem Verantwortlichen angegebenen Zwecke einwilligen.[784] Bei der Verarbeitung biometrischer Daten, die aus Bildern gewonnen werden, reicht es beispielsweise nicht aus, die Einwilligung der betroffenen Personen in die Verarbeitung dieser Bilder einzuholen. Vielmehr müssen die betroffenen Personen darüber informiert werden, dass biometrische Merkmale extrahiert und verarbeitet werden, und es muss deren ausdrückliche Einwilligung eingeholt werden.

[784] In Erwägungsgrund 33 der DSGVO wird eingeräumt, dass der Zweck der Verarbeitung zum Zeitpunkt der Erhebung der personenbezogenen Daten möglicherweise nicht vollständig angegeben werden kann und dass es den betroffenen Personen daher erlaubt sein sollte, ihre Einwilligung für bestimmte „Bereiche wissenschaftlicher Forschung" zu geben. Der in Erwägungsgrund 33 angesprochene Punkt und eine Reihe von Auslegungsproblemen wurden in dem Dokument „Issues and gaps analysis on informed consent in the context of ICT research and innovation" untersucht.

Beispiel: Einwilligung versus ausdrückliche Einwilligung	
Einwilligung	**Ausdrückliche Einwilligung**
„Bitte stellen Sie ein Lichtbild von sich bereit, das in einer gut beleuchteten Umgebung von vorne aufgenommen wurde. Das Bild wird verwendet, um biometrische Merkmale für die Entwicklung eines neuen biometrischen Erkennungssystems zu gewinnen".	„A: Bitte stellen Sie ein Lichtbild von sich bereit, das in einer gut beleuchteten Umgebung von vorne aufgenommen wurde. B: Das Bild wird verwendet, um biometrische Merkmale für die Entwicklung eines neuen biometrischen Erkennungssystems zu extrahieren. C: Bitte kreuzen Sie vor dem Absenden des Lichtbilds das folgende Kästchen an, um anzuzeigen, dass Sie als betroffene Person darin einwilligen, dass Ihr Bild zum Zweck der Gewinnung biometrischer Merkmale verarbeitet wird, die zu dem unter Punkt B beschriebenen Zweck verarbeitet werden. Markieren Sie das Kästchen ☐"

Wenn es um die Einwilligung im Zusammenhang mit der Forschung geht, ist es auch wichtig, zwischen der Einwilligung zur Teilnahme an der Studie und der Einwilligung zur Verarbeitung personenbezogener Daten zu unterscheiden. Es handelt sich um zwei verschiedene Arten von Einwilligungen, die unabhängig voneinander erhoben werden müssen[785]. Das Forschungsteam kann sich auf eine einzige Einwilligungserklärung stützen, vorausgesetzt, diese unterscheidet klar zwischen den beiden Arten der Einwilligung und fasst sie nicht in einer einzigen Vereinbarung zusammen (weitere Informationen finden Sie im Dokument „Issues and gaps analysis on informed consent in the context of ICT research and innovation").

Eine weitere Ausnahmeregelung in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten, die für den Zweck dieses Dokuments von Bedeutung ist, ist die Ausnahme hinsichtlich der für Forschungstätigkeiten erforderlichen Verarbeitung. Damit diese Ausnahmeregelung Anwendung findet, müssen zwei *Kriterien* erfüllt sein. Erstens muss die Verarbeitung geeigneten technischen und organisatorischen Garantien gemäß Artikel 89 Absatz 1 DSGVO unterliegen. Zweitens sollte das Unionsrecht oder das Recht der Mitgliedstaaten Vorschriften vorsehen, die eine Rechtsgrundlage für die Verarbeitung im Zusammenhang mit einer Forschungstätigkeit bieten. Dieses letzte *Kriterium* bedeutet, dass die Ausnahmeregelung für Forschungszwecke möglicherweise nicht überall anwendbar ist. Daher müssen die Forscher die nationalen Rechtsvorschriften aller Staaten, in denen die Forschung durchgeführt werden soll, dahingehend überprüfen, ob solche Vorschriften vorgesehen sind (siehe Anhang III „Comparative study of national reports" im Dokument „Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation").

[785] Siehe: Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Mai 2020, 30; Europäischer Datenschutzausschuss, Stellungnahme 3/2019 zu den Fragen und Antworten zum Zusammenspiel der Verordnung über klinische Prüfungen und der Datenschutz-Grundverordnung (DSGVO) (Artikel 70 Absatz 1 Buchstabe b), 2019.

3.2.4 Einrichtung eines Repository für unterstützende Dokumentation

Laut der DSGVO müssen die Verantwortlichen nicht nur ihren Datenschutzpflichten nachkommen, sondern auch in der Lage sein, ihre Einhaltung dieser Pflichten und der in der Norm verankerten Grundsätze nachzuweisen. Der Verantwortliche muss somit angemessene Aufzeichnungen und Unterlagen über die Datenverarbeitung und die Steuerung dieser Verarbeitung aufbewahren.

Abgesehen von einer begrenzten Anzahl von Dokumenten, die eindeutig vorgeschrieben sind (z. B. das in Artikel 30 DSGVO geforderte Verzeichnis von Verarbeitungstätigkeiten), muss der Verantwortliche ermitteln, welche Dokumente für den Nachweis der Einhaltung der Vorschriften erforderlich sind. Die nachstehenden Tabellen enthalten eine Liste der laut DSGVO vorgeschriebenen Unterlagen mit der entsprechenden Stelle im Text. Sie sollten als Mindestanforderung und nicht als erschöpfende Checkliste betrachtet werden. Auch wenn sie nicht vorgeschrieben sind, können zusätzliche Unterlagen zum Nachweis der Einhaltung erforderlich sein (z. B. Berichte über eine vorherige Konsultation der Aufsichtsbehörden, Beschreibung der getroffenen technischen und organisatorischen Maßnahmen usw.)

Unterlagen: Checkliste		
1	Geeignete Datenschutzvorkehrungen	Artikel 24 Absatz 2.
2	Datenschutzhinweis	Artikel 12, 13, 14
3	Datenspeicherungserklärung	Artikel 5, 13, 17 und 30
4	Datenspeicherungsplan	Artikel 30
5	Verzeichnis von Verarbeitungstätigkeiten (ggf.)	Artikel 30
6	Einwilligungserklärung (ggf.)	Artikel 6, 7, 9
7	Datenverarbeitungsvertrag mit Lieferanten	Artikel 28, 32, 82
8	Datenschutz-Folgenabschätzung	Artikel 35
9	Benennung eines EU-Vertreters (ggf.)	Artikel 27
10	Verfahren zur Reaktion auf und Meldung von Datenschutzverletzungen	Artikel 4, 33, 34
11	Meldung von Datenschutzverletzungen an die Aufsichtsbehörde (ggf.)	Artikel 33
12	Benachrichtigung der von einer Datenschutzverletzung betroffenen Person (ggf.)	Artikel 34

Einige Unterlagen sind nur erforderlich, wenn bestimmte *Kriterien* zutreffen.

Bedingt vorgeschriebene Unterlagen	
Verzeichnis von Verarbeitungstätigkeiten	Bei 250 oder mehr Beschäftigten, es sei denn, die vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien bzw. von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.

Einwilligungserklärung	Wenn sich die Verarbeitung auf eine Einwilligung als Rechtsgrundlage stützt und die Daten in schriftlicher Form erhoben wurden[786]
Benennung eines EU-Vertreters	Wenn die Verarbeitung betroffene Personen in der EU betrifft und von einem Verantwortlichen bzw. einem Auftragsverarbeiter durchgeführt wird, der nicht in der EU ansässig ist, es sei denn, die Verarbeitung erfolgt gelegentlich, schließt nicht die umfangreiche Verarbeitung besonderer Datenkategorien oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ein und führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.
Meldung von Datenschutzverletzungen an die Aufsichtsbehörde	Nur im Falle einer Verletzung einer Datenschutzverletzung, die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Benachrichtigung der von einer Datenschutzverletzung betroffenen Person	Im Falle einer Datenschutzverletzung, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, bzw. die voraussichtlich kein hohes Risiko zur Folge hat, die Aufsichtsbehörde dies jedoch verlangt.

Um das Führen von Aufzeichnungen zu erleichtern und einheitlich zu gestalten, sollte der Forscher geeignete Vorlagen für die zu dokumentierenden Schritte erstellen oder sich mit dem Datenschutzbeauftragten bzw. seiner Rechtsabteilung beraten, um zu prüfen, ob in der Organisation Vorlagen vorhanden sind.

Bevor die Forscher mit der Erhebung und Verarbeitung personenbezogener Daten beginnen, sollten sie die in ihrer Organisation bereits vorhandene Datenschutzdokumentation sammeln und ein spezielles *Dossier* mit allen relevanten Unterlagen erstellen. Neue Dokumente sollten bei Erstellung dem *Dossier* hinzugefügt werden. Zweck des *Dossiers* ist es, die von den Forschern und anderen an der Forschungstätigkeit beteiligten Datenschutzakteuren unternommenen Schritte und getroffenen Entscheidungen aufzuzeichnen und genügend Informationen zum Nachweis vorzulegen, dass die Vorschriften während des gesamten Prozesses eingehalten wurden.

Das Forschungsteam sollte das *Dossier* jedoch nicht als reine Aufzeichnungspflicht betrachten. Das *Dossier* sollte vielmehr als Formalisierung der praktischen Schritte dienen, die das Forschungsteam unternimmt, um den Schutz der personenbezogenen Daten zu gewährleisten. So reicht es beispielsweise nicht aus, ein Verfahren zur Reaktion auf und Meldung von Datenschutzverletzungen zu haben. Die Forscher sollten nachweisen können, dass das Verfahren im Bedarfsfall schnell und effektiv in Gang gesetzt werden kann.

3.2.5 Prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist

Laut der Artikel-29-Datenschutzgruppe ist eine Datenschutz-Folgenabschätzung (DPIA) „ein Verfahren, anhand dessen die Verarbeitung beschrieben, ihre Notwendigkeit und Verhältnismäßigkeit bewertet und die Risiken für die Rechte und Freiheiten natürlicher Personen, die die Verarbeitung personenbezogener Daten mit sich bringt, durch eine

[786] Tatsächlich schreibt die DSGVO nicht vor, dass die Einwilligung in schriftlicher Form eingeholt werden muss. Weitere Informationen finden Sie unter: Europäischer Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 16.

entsprechende Risikoabschätzung und die Ermittlung von Gegenmaßnahmen besser kontrolliert werden sollen“[787].

Gemäß Artikel 35 Absatz 1 DSGVO müssen die Verantwortlichen eine Datenschutz-Folgenabschätzung durchführen, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Daher ist eine Datenschutz-Folgenabschätzung nicht immer zwingend erforderlich. Die Verantwortlichen sind jedoch verpflichtet, vorab stets eine Risikobewertung durchzuführen, um festzustellen, ob die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Diese vorbereitende Bewertung ist ein integraler Bestandteil des DPIA-Prozesses. Bestimmte Elemente der Datenschutz-Folgenabschätzung sind somit obligatorisch, um zumindest deren Erforderlichkeit zu bestimmen.

Die Risiken für die Rechte und Freiheiten der betroffenen Personen werden in Erwägungsgrund 75 der DSGVO genannt. Dabei handelt es sich um Risiken, die zu einem physischen, materiellen oder immateriellen Schaden für die betroffene Person führen könnten (z. B. die Verweigerung des Zugangs zu einem Dienst nach einer falsch-negativen Identifizierung).

Beispiele für Risiken für die Rechte und Freiheiten	
Diskriminierung	Identitätsdiebstahl oder -betrug
Finanzieller Verlust	Rufschädigung
Verlust der Vertraulichkeit von dem Berufsgeheimnis	Unbefugte Aufhebung der Pseudonymisierung
Wirtschaftliche oder gesellschaftliche Nachteile	Hinderung, personenbezogene Daten zu kontrollieren

In der DSGVO wird der Begriff „hohes Risiko“ nicht definiert. Die Artikel-29-Datenschutzgruppe hat jedoch eine Liste mit neun *Kriterien* erstellt, anhand derer die Verantwortlichen erkennen können, ob die Verarbeitung als mit einem hohen Risiko behaftet einzustufen ist[788].

***Kriterien* einer mit einem hohen Risiko behafteten Verarbeitung**	
Kriterium 1	Evaluierung oder Bewertung (z. B. Profiling)
Kriterium 2	Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher signifikanter Wirkung
Kriterium 3	Systematische Überwachung
Kriterium 4	Sensible Daten oder Daten von sehr persönlicher Natur
Kriterium 5	Daten werden in großem Umfang verarbeitet

[787] Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, Oktober 2017, 4.
[788] Artikel 29-Datenschutzgruppe, 9–11.

Kriterium 6	Matching oder Kombination von Datensätzen (über die vernünftigen Erwartungen der betroffenen Person hinaus)
Kriterium 7	Daten zu gefährdeten Personen
Kriterium 8	Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
Kriterium 9	Die Verarbeitung an sich verhindert, dass betroffene Personen ein Recht ausüben oder eine Dienstleistung oder einen Vertrag in Anspruch nehmen

Forscher, die Forschungstätigkeiten durchführen, sollten alle diese Kriterien berücksichtigen, um zu verstehen, ob eine Datenschutz-Folgenabschätzung erforderlich ist. Für den Zweck dieses Dokuments sind jedoch insbesondere die *Kriterien* vier und acht besonders relevant. *Kriterium* vier ist von Bedeutung, wenn biometrische Daten während der Forschungstätigkeit verarbeitet werden. *Kriterium* acht ist im Zusammenhang mit der IKT-Forschung wichtig, da bei dieser Tätigkeit möglicherweise neue Datenverarbeitungstechnologien eingeführt werden (z. B. innovative Methoden zur Erfassung und Analyse von Stimmproben).

Gemäß Artikel 35 Absatz 4 DSGVO müssen die nationalen Aufsichtsbehörden die Liste der Verarbeitungsvorgänge veröffentlichen, für die eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist[789]. Dies könnte weitere Anhaltspunkte dafür liefern, was eine Verarbeitung darstellt, die eine Datenschutz-Folgenabschätzung erfordert, wobei die Forscher die Position der zuständigen Aufsichtsbehörden beachten sollten. In Anbetracht der Komplexität der Aufgabe sollten Forscher auch den Datenschutzbeauftragten ihrer Organisation um Rat fragen.

Um die Einhaltung der Vorschriften nachweisen zu können, sollte die Bewertung, ob die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, dokumentiert und aufbewahrt werden.

3.2.6 Durchführung einer Datenschutz-Folgenabschätzung (ggf.)

Es gibt kein Standardverfahren für die Durchführung einer Datenschutz-Folgenabschätzung. Artikel 35 Absatz 7 DSGVO fordert jedoch bestimmte Elemente, die immer vorhanden sein müssen. Diese sind:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und
- der Zwecke der Verarbeitung;
- eine Bewertung der Notwendigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen;
- die zur Bewältigung der Risiken geplanten technischen und organisatorischen Abhilfemaßnahmen.

[789] In diesem Zusammenhang haben die nationalen Aufsichtsbehörden auf ihren Websites eine entsprechende Liste veröffentlicht. In einigen Fällen hat der EDSA bereits eine Stellungnahme zu den in den einzelnen Listen aufgeführten Tätigkeiten abgegeben. Weitere Informationen finden Sie unter: European Data Protection Board, Opinion 6/2019 on the Draft List of the Competent Supervisory Authority of Spain Regarding the Processing Operations Subject to the Requirement of a Data Protection Impact Assessment (Article 35.4 GDPR), März 2019.

Die Forscher können weitere Elemente hinzufügen, um die Verarbeitung und die zugrunde liegenden Risiken besser zu beschreiben. Stellt der Verantwortliche nach Durchführung einer Datenschutz-Folgenabschätzung fest, dass die Risiken für die Rechte und Freiheiten der betroffenen Person durch die geplanten Maßnahmen zur Eindämmung dieser Risiken nicht angemessen gemindert werden, muss er gemäß Artikel 36 DSGVO die Aufsichtsbehörde konsultieren.

Das Gesetz schreibt kein bestimmtes Format für die Datenschutz-Folgenabschätzung vor. Dieses kann von dem Verantwortlichen frei gewählt werden. Einige Datenschutzbehörden haben jedoch Vorlagen erstellt, die die Verantwortlichen verwenden können.[790]

Die Datenschutz-Folgenabschätzung ist keine punktuelle Tätigkeit, sondern ein kontinuierlicher Prozess. Daher müssen im Laufe der Zeit unter Umständen mehrere Bewertungen durchgeführt werden, beispielsweise wenn sich der Kontext ändert oder wenn neue Informationen verfügbar werden.

Die Ergebnisse der Datenschutz-Folgenabschätzungen sind aufzuzeichnen und als Teil der Datenschutzdokumentation aufzubewahren.

3.2.7 Umsetzung risikomindernder Maßnahmen

Gemäß Erwägungsgrund 78 der Datenschutz-Grundverordnung „ist es zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen [der DSGVO] erfüllt werden.“ Diese Bestimmung, die einen Eckpfeiler des Rechtsrahmens darstellt, wird für den besonderen Fall der Verarbeitung zu Forschungszwecken weiter ausgeführt. Erwägungsgrund 156 und Artikel 89 DSGVO fordern die Umsetzung „geeigneter Garantien“ und betonen die Bedeutung des Schutzes der Rechte und Freiheiten natürlicher Personen.

Die DSGVO enthält keine umfassende Liste technischer und organisatorischer Maßnahmen, sondern überlässt es dem Verantwortlichen, diese zu ermitteln und ihre Wirksamkeit zur Minderung der Risiken für die betroffenen Personen zu bewerten. Außerdem sollten die Forscher eine externe Sicherheits- und Datenschutzüberprüfung zwecks Bestätigung in Betracht ziehen, dass die Sicherheits- und Compliance-Maßnahmen solide sind, und um die Einhaltung des Grundsatzes der Rechenschaftspflicht nachzuweisen.

Beispiele für technische und organisatorische Maßnahmen.	
Technische Maßnahmen	**Organisatorische Maßnahmen**
Anonymisierung oder Pseudonymisierung der Daten[791]	Sicherheitsrichtlinien
Verschlüsselung der Kommunikation	Datenmanagementpläne
Schutz der Daten vor unbefugtem Zugriff	Schulungsprogramm für das Personal
Schwachstellenanalyse/Penetrationstests	Regelmäßige Überprüfungen und Bewertungen

[790] Siehe beispielsweis: }Commision Nationale Informatique & Libertés, Privacy Impact Assessment (PIA). Templates, Februar 2018.

[791] Weitere Informationen zur Anonymisierung finden Sie in Abschnitt 3.3.5 Löschung oder Vernichtung von Daten. Weitere technische Informationen finden Sie unter PANELFIT DOCUMENT ON ANONYMISATION

3.3 Ausführungsphase

Nachdem die Forschungstätigkeit angemessen vorbereitet wurde, können die Forscher mit ihrer Arbeit und den damit verbundenen Datenverarbeitungsvorgängen beginnen. Diese Phase beginnt mit der Erhebung der Daten gemäß dem in der Vorbereitungsphase festgelegten Plan.

3.3.1 Verarbeitung biometrischer Daten

Sobald die Forscher die erforderlichen biometrischen Daten erhalten haben, können diese zwecks Gewinnung der für die Forschung benötigten biometrischen Merkmale verarbeitet werden. Obwohl eine „manuelle" Verarbeitung theoretisch möglich ist (z. B. die manuelle Zuordnung von Gesichtsmerkmalen auf Bildern, wie der Abstand zwischen den Augen, die Form des Gesichts, die Höhe der Ohren usw.),[792] wird ein solcher Ansatz heute im Allgemeinen als nicht durchführbar angesehen und durch automatisierte Mittel ersetzt, die häufig auf der Technologie der künstlichen Intelligenz beruhen (spezifische Hinweise finden Sie im Dokument „Guidelines on ethical and legal issues regarding artificial intelligence in ICT research and innovation"). Unabhängig von dieser Unterscheidung muss jeder Verarbeitungsvorgang unter Einhaltung aller in der Vorbereitungsphase festgelegten Garantien und Vorsichtsmaßnahmen durchgeführt werden.

3.3.2 Entwicklung des biometrischen Systems und der Benutzeroberfläche

Wenn das Ziel der Forschung in der Entwicklung eines biometrischen Systems besteht, sollten die Forscher besondere Sorgfalt auf die Gestaltung der Benutzeroberfläche verwenden, vor allem dann, wenn das System von der Öffentlichkeit genutzt werden soll. Die UI sollte so benutzerfreundlich wie möglich gestaltet werden, um die Transparenz zu fördern und den betroffenen Personen die Ausübung ihres Rechts auf Auskunft zu erleichtern. In diesem Sinne sollten die Forscher drei Hauptaspekte berücksichtigen. Und zwar die über die Benutzeroberfläche verfügbaren Informationen, die über die Benutzeroberfläche zugänglichen Funktionen und die allgemeine Benutzerfreundlichkeit der Oberfläche.

Erstens muss der Verantwortliche sicherstellen, dass alle Informationen, die den betroffenen Personen gemäß Artikel 13 und 14 DSGVO zur Verfügung gestellt werden, über die Benutzeroberfläche verfügbar sind. Sie sollten leicht zugänglich sein und in einer klaren und leicht verständlichen Weise dargestellt werden. So könnte das System beispielsweise eine sichtbare Schaltfläche enthalten, auf die die betroffenen Personen klicken können, um ein Pop-up-Fenster mit den Informationen zu öffnen. Es empfiehlt sich, die Informationen direkt im System zur Verfügung zu stellen und nach Möglichkeit Links zu externen Repositorys oder Websites zu vermeiden. So wird das Risiko minimiert, dass die Informationen z. B. aufgrund von Verbindungsproblemen nicht zugänglich sind. Die Benutzeroberfläche sollte auch die Fähigkeiten des Geräts nutzen, über das auf die Informationen zugegriffen wird. Läuft das System beispielsweise auf einem Smartphone, könnte es die Möglichkeit bieten, den Datenschutzbeauftragten mit einem einfachen Klick direkt anzurufen oder ihm eine E-Mail zu senden.[793]

Zweitens sollte die Benutzeroberfläche eine Reihe von Funktionen bieten, anhand der die betroffenen Personen ihre Rechte leichter ausüben können (vorausgesetzt, es gibt keine Ausnahmeregelung für die Anwendung dieser Rechte). Siehe Abschnitt 3.2.2 Ermittlung des Datenerhebungsansatzes). Beispielsweise sollte die Benutzeroberfläche den betroffenen

---

[792] Einige biometrische Erkennungsverfahren wurden zuerst als manuelle Technik entdeckt und waren sogar schon vor der Entwicklung von Computersystemen vorhanden. Siehe beispielsweise: Mark Maguire, The Birth of Biometric Security', *Anthropology Today* 25, Nr. 2 (April 2009): 9–14, https://doi.org/10.1111/j.1467-8322.2009.00654.x..

[793] Ungeachtet dessen müssen die Kontakte ebenfalls angezeigt werden. Das System darf zudem keine bestimmte Art der Kommunikation vorschreiben.

Personen die Möglichkeit bieten, auf ihre personenbezogenen Daten zuzugreifen und sie zu berichtigen oder zu löschen (sofern dies nicht dazu führt, dass der Zweck der Verarbeitung nicht mehr erfüllt werden kann). Wenn die betroffenen Personen Zugang zu spezifischen Funktionen haben, können diese ihre Rechte nicht nur leichter ausüben, sondern es dürfte auch die Belastung der Verantwortlichen verringern, da viele dieser Anfragen direkt von den betroffenen Personen gestellt werden. So kann beispielsweise der Fall eintreten, dass Nutzer von Gesichtserkennungssystemen ihre Bilder aktualisieren müssen (z. B. nach einer Operation). Wenn man ihnen die Möglichkeit bereitstellt, dies direkt zu tun, anstatt sich an den Verantwortlichen wenden zu müssen, könnte dies ein Anreiz sein, die Daten auf dem neuesten Stand zu halten und somit auch die Einhaltung des Grundsatzes der Genauigkeit zu gewährleisten. Die Einführung dieser Funktionalitäten kann jedoch auch die Risiken für die Rechte und Freiheiten der betroffenen Personen erhöhen. Wird beispielsweise das Konto eines Nutzers gehackt, gibt diese „Selbstbedienungsoption" Angreifern die volle Kontrolle über die personenbezogenen Daten der betroffenen Personen. Daher müssen Verantwortliche stets sicherstellen, dass jedes zusätzliche Risiko infolge spezifischer Funktionen durch geeignete Sicherheitsmaßnahmen (z. B. Mehrfaktorauthentifizierung, obligatorische Passwortaktualisierung usw.) angemessen gemindert wird. Können die Forscher die Risiken nach der Einführung neuer Funktionen nicht angemessen mindern, so müssen vorher die zuständige Aufsichtsbehörde konsultieren oder die Einführung der Funktionen so lange vermeiden, bis sie einen praktikablen Ansatz zur Risikominderung gefunden haben.

Drittens muss die allgemeine Benutzerfreundlichkeit der Oberfläche die Transparenz fördern und vermeiden, dass den betroffenen Personen bei der Ausübung ihrer Rechte unnötige Lasten aufgebürdet werden. Eine angemessene Benutzeroberfläche sollte Elemente wie die Merkmale der betroffenen Personen (z. B. Sprache, Demografie usw.), die Art und Weise, wie die Benutzer mit dem System interagieren (z. B. auf einem PC, einem Smartphone, einer speziellen Hardware usw.), den Ort, an dem die Benutzer mit dem System interagieren (z. B. zu Hause, in einem öffentlichen Raum usw.), Rückfalloptionen (z. B. wenn Benutzer versehentlich bestimmte Einstellungen ändern) und viele andere Elemente berücksichtigen. Die Entwickler sollten auch bedenken, dass das System von schutzbedürftigen Personen wie Kindern oder sehbehinderten Menschen genutzt werden könnte. Daher sollte die Oberfläche so gestaltet sein, dass diesen Personen die Nutzung des Systems erleichtert wird (z. B. Sprache-zu-Text, Textvergrößerung usw.).

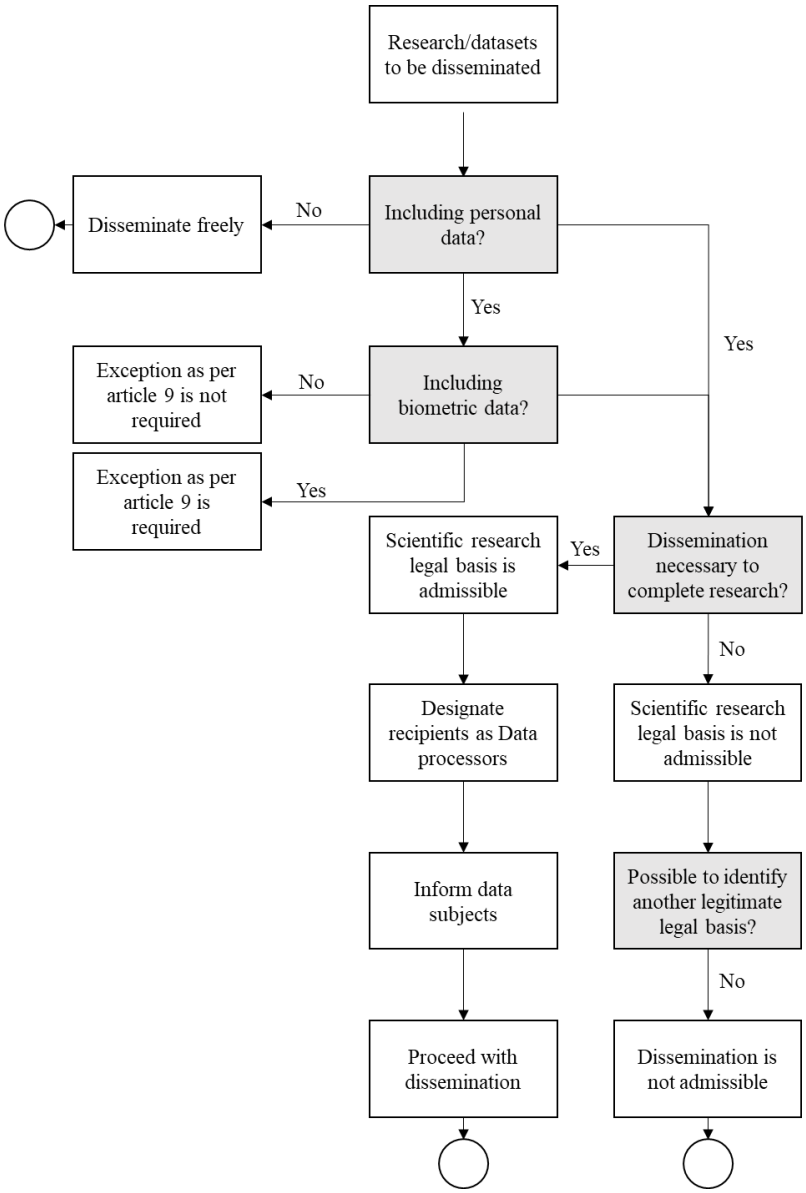
3.3.3 Testen des biometrischen Systems

Der letzte Schritt vor dem Einsatz des biometrischen Systems besteht darin, es zu testen und seine Ergebnisse zu validieren. In diesem Zusammenhang gibt es zwei mögliche Szenarien. Im ersten Szenario müssen neue Daten erhoben werden, während im zweiten Szenario die Forscher die bereits in der Entwicklungsphase verarbeiteten Daten verwenden. Das erste Szenario tritt ein, wenn beispielsweise neue Personen speziell zum Testen des Systems hinzugezogen werden. In diesem Fall muss der Verantwortliche die bereits bezüglich der Vorbereitungsphase erwähnten Schritte durchführen. Im zweiten Szenario müssen die Forscher prüfen, ob diese weiteren Tests in den ursprünglichen Zwecken enthalten sind (weitere Informationen finden Sie in Abschnitt 3.2. „Purpose limitation" im Dokument „Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation"). Das „Testen des Systems" stellt in der Tat eine andere Verarbeitung dar als die „Entwicklung des Systems" und könnte daher eine andere Rechtsgrundlage erfordern, insbesondere dann, wenn die beiden Verarbeitungsvorgänge unterschiedliche Datensätze erfordern. In solchen Fällen sollten die Forscher nicht davon ausgehen, dass sie, da sie die Pflichten im Zusammenhang mit der Entwicklung des Systems erfüllt haben, automatisch auch die Pflichten im Zusammenhang mit dem Testen erfüllen. Vielmehr müssen sie diesen Schritt

kritisch betrachten und sich vorrangig um die Minimierung der Risiken für die Rechte und Freiheiten der betroffenen Personen bemühen.

3.3.4 Verbreitung der Ergebnisse

Am Ende der Forschungstätigkeit können die Forscher beschließen, die Ergebnisse ihrer Arbeit zu verbreiten. Sofern die Verbreitung nicht die während der Forschung verarbeiteten personenbezogenen Daten umfasst, kann die Arbeit an andere interessierte Kreise weitergegeben werden. Schließt die Verbreitung dagegen die während der Forschung verarbeiteten Daten ein (z. B. indem die Daten der wissenschaftlichen Gemeinschaft zur Begutachtung zur Verfügung gestellt werden), sollten zusätzliche Maßnahmen ergriffen werden. Die Verbreitung personenbezogener Daten stellt einen Verarbeitungsvorgang gemäß Artikel 4 Absatz 2 DSGVO dar, wobei – wie oben beschrieben – jede Verarbeitung biometrischer Daten untersagt ist, sofern keine Ausnahmen gelten. Daher sollten Forscher die bereits unter 3.2.2 beschriebenen Schritte erneut durchführen, bevor sie mit der Verbreitung fortfahren. Stützt sich der Verantwortliche auf die Rechtsgrundlage „wissenschaftliche Forschung“ und sind alle Voraussetzungen für die Annahme einer solchen Rechtsgrundlage erfüllt (siehe Abschnitt 3.2.3 „Ermittlung der am besten geeigneten Rechtsgrundlage“), lassen sich zwei weitere Szenarien unterscheiden. Im ersten Fall hat das Forschungsteam (Team A) die Forschungstätigkeit abgeschlossen und beabsichtigt nun, die Daten zum Nutzen anderer Forschungsteams (Team B) zu verbreiten. In einem solchen Szenario ist die Verbreitung kein notwendiger Vorgang, um die Forschungszwecke von Team A zu erreichen, könnte aber für die Forschungszwecke von Team B notwendig sein. Somit kann sich Team A nicht auf die Rechtsgrundlage „wissenschaftliche Forschung“ berufen. Daraus folgt, dass Team A keine Rechtsgrundlage für die Weitergabe der Daten an Team B oder einen anderen Empfänger hat, sofern keine andere Rechtsgrundlage gefunden wird (z. B. kann Team A eine ausdrückliche Einwilligung für die Weitergabe der Daten an Team B einholen). Im zweiten Szenario stellt Team A nach der Erhebung der personenbezogenen Daten fest, dass es nicht über angemessene (z. B. technische) Kapazitäten verfügt, um die Daten zu verarbeiten und die Forschung fortzusetzen. Daher beschließt Team A, sich bei der Verarbeitung der Daten auf die Fähigkeiten von Team B zu stützen. In dieser Situation ist die Verbreitung der an Team B ein notwendiger Schritt, um die Forschungszwecke von Team A zu erreichen, wobei Team B muss gemäß Artikel 28 DSGVO als „Auftragsverarbeiter“ benannt werden muss. Artikel 4 Absatz 8 DSGVO definiert einen Auftragsverarbeiter als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Die Benennung und die Aufgaben des Auftragsverarbeiters sind der betroffenen Person vor der Übermittlung mitzuteilen und erfolgen auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das zumindest den Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sowie die Pflichten und Rechte des Verantwortlichen festlegt.



Falls personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums übermittelt werden müssen[794] und vorausgesetzt, dass eine solche Übermittlung nicht unter eine oder mehrere der in Artikel 49 DSGVO[795] aufgeführten Ausnahmen fällt, sollten zusätzliche Schritte unternommen werden. Die DSGVO sieht eine Reihe von Instrumenten für die internationale Übermittlung von Daten vor. Allerdings sind derzeit noch nicht alle von ihnen anwendbar, da die zuständigen Behörden noch an der Formalisierung einiger arbeiten.

Internationale Datenübermittlung	
Verfolgung eines Angemessenheitsbeschlusses	Anwendbar
Verfolgung von Standarddatenschutzklauseln	Anwendbar
Verfolgung von verbindlichen internen Datenschutzvorschriften	Anwendbar

[794] Dazu gehören alle EU-Mitgliedstaaten sowie Island, Liechtenstein und Norwegen.
[795] Weitere Informationen finden Sie unter: Europäischer Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, Mai 2018.

Verfolgung von Verhaltenskodizes	Geplant
Verfolgung von Zertifizierungsmechanismen	Geplant
Verfolgung eines rechtsverbindlichen Instruments zwischen öffentlichen Behörden oder Einrichtungen	Geplant[796]

Im ersten Fall (Verfolgung eines Angemessenheitsbeschlusses) können die Daten in weitere EU-Staaten übermittelt werden, wenn ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Ein Angemessenheitsbeschluss kann angenommen werden, wenn der andere Staat ein Datenschutzniveau bietet, das dem europäischen Standard entspricht.[797] Im zweiten Fall (Verfolgung von Standarddatenschutzklauseln) können die Daten übermittelt werden, wenn es eine Vereinbarung zwischen dem Datenexporteur und dem Datenimporteur gibt und wenn diese Vereinbarung eine Reihe von Standardklauseln zum Datenschutz enthält, die von der Europäischen Kommission vorab genehmigt wurden[798]. Im dritten Fall, wenn die extraterritoriale Übermittlung innerhalb derselben Einrichtung stattfindet (z. B. eine Übermittlung zwischen zwei Niederlassungen eines internationalen Konzerns), können die Daten übermittelt werden, wenn es verbindliche interne Datenschutzvorschriften gibt, die Garantien gemäß Artikel 47 DSGVO bieten und von der zuständigen Datenschutzaufsichtsbehörde genehmigt wurden.

3.3.5 Löschung oder Vernichtung von Daten

Nach Abschluss der Tests sollte der Verantwortliche den zu diesem Zweck verwendeten Datensatz löschen, es sei denn, es besteht eine rechtliche Notwendigkeit, die Daten beispielsweise für die Weiterentwicklung oder Bewertung des Systems oder für andere Zwecke zu speichern, die gemäß den Bestimmungen von Artikel 6 Absatz 4 DSGVO mit den Zwecken vereinbar sind, für die sie erhoben wurden.

Die Anonymisierung stellt eine Alternative zur Löschung dar.[799] Das Konsortium hat ein eigenes Dokument zu diesem Thema erstellt (https://www.datenschutzzentrum.de/uploads/projekte/IdentPseudoAnon-320-v1-0-web.pdf).

[796] Zum Juli 2021 sind diese drei Optionen für die internationale Übermittlung von Daten zwar geplant, aber noch nicht umgesetzt.

[797] Die Liste der Länder, die durch einen Angemessenheitsbeschluss anerkannt wurden, ist abrufbar unter: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[798] Die aktuellste Fassung der Standardklauseln finden Sie unter: Europäische Kommission, Durchführungsbeschluss (EU) 2021/914 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (2021), https://doi.org/10.5040/9781782258674.

[799] Es sei darauf hingewiesen, dass nach Ansicht einiger Wissenschaftler personenbezogene Daten, insbesondere biometrische Daten, nicht vollständig anonymisiert werden können. Siehe beispielsweise: Justin Banda, Inherently Identifiable: Is It Possible to Anonymize Health and Genetic Data?, *International Association of Privacy Professionals* (blog), November 2019, https://iapp.org/news/a/inherently-identifiable-is-it-possible-to-anonymize-health-and-genetic-data/.

4 Biometrische Technologie in der IKT-Forschung und -Innovation Fallstudie

Die folgende Fallstudie wenden den Inhalt von Abschnitt 3 „Biometrische Technologie in der IKT-Forschung und -Innovation. Leitlinien“ an. Die Fallstudie bezieht sich nicht auf eine reale Situation.

Ein Team von IKT-Entwicklern beschließt, ein Handerkennungssystem zu entwickeln, um den Identifizierungsprozess von Arbeitnehmern am Eingang von Arbeitsstätten zu rationalisieren. Die Forscher wollen einen datenschutzfreundlichen Ansatz vorschlagen, dessen Umsetzbarkeit verstehen, die entsprechende Technologie entwickeln und einen Artikel mit den Ergebnissen veröffentlichen.

Das Entwicklerteam hat beschlossen, den Schwerpunkt auf drei Aspekte zu legen:

- Das System muss vollständig den Datenschutznormen entsprechen
- Das System ist effektiv genug, um von Unternehmen übernommen zu werden
- Das System wird von den Benutzern – den Mitarbeitern – nicht als zu invasiv empfunden.

Alle Entwickler arbeiten für das gleiche private Unternehmen, Developing Inc., mit Sitz in dem fiktiven europäischen Staat Developonia. In dem Szenario handelt Developing Inc. als Verantwortlicher.

4.1 Designphase

4.1.1 Identifizierung der Ziele und ob die Tätigkeit als „Forschung“ eingestuft werden kann

Die Entwickler legen die folgenden Ziele fest:

- Entwurf eines Ansatzes, um die Identifizierung von Arbeitnehmern am Arbeitsplatz zu rationalisieren
- Verständnis der Umsetzbarkeit
- Entwicklung und Test der entsprechenden Technologie
- Veröffentlichung einer Publikation mit den Ergebnissen

Auf der Grundlage dieser Ziele bewerten die Entwickler anschließend, ob es sich bei dem Projekt um eine „wissenschaftliche Forschung“ handelt. Dazu ziehen sie die Definition des EDSB heran (siehe Abschnitt 2.5 „Forschungstätigkeit“) und prüfen, ob die Tätigkeit dazu beiträgt, „das kollektive Wissen und das Wohlergehen der Gesellschaft zu steigern und nicht in erster Linie einem oder mehreren privaten Interessen zu dienen“[800]. Die Entwickler kommen zu dem Schluss, dass die Antwort positiv ausfällt, da die Aktivität nicht nur darauf abzielt, eine neue kommerzielle Technologie zu schaffen, sondern einen Ansatz zur Wahrung der Privatsphäre der Arbeitnehmer einzuführen, der für Anwendungen zur Wahrung der Privatsphäre in anderen Kontexten aufschlussreich sein wird.

Rechtliche Regelung: Forschung			
Kann die Tätigkeit als „Forschung“ eingestuft werden?	Ja	?	Besondere Regelung für die Forschung gilt
	Nein		Besondere Regelung für die Forschung gilt nicht

[800] Europäischer Datenschutzbeauftragter, A Preliminary Opinion on Data Protection and Scientific Research.

4.1.2 Bestätigung der Notwendigkeit der Verarbeitung biometrischer Daten

Für die konkrete Forschung beschließen die Entwickler, weder auf eine kommerzielle Datenbank noch auf computergenerierte Bilder zurückzugreifen. Vielmehr wählen sie, alle zur Erreichung ihrer Forschungsziele erforderlichen Daten (Handflächenabdrücke) direkt von natürlichen Personen zu erheben. Die Entwickler sammeln Abdrücke der Handflächen und extrahieren daraus die charakteristischen physischen Merkmale (z. B. die Abmessungen der Hand).

Zur Ermittlung, ob es sich um biometrische Daten handelt, wenden die Entwickler die *Kriterien* von Artikel 4 Absatz 14 DSGVO an.

Checkliste biometrische Daten		
☐	Es handelt sich um personenbezogene Daten	Ja, da sich die Handflächenabdrücke auf eine „identifizierte natürliche Person" beziehen.
☐	Sie werden mit einem speziellen technischen Verfahren gewonnen	Ja, da die Unterscheidungsmerkmale durch technische Verarbeitung aus den Abdrücken der Handflächenabdrücke extrahiert werden.
☐	Sie beziehen sich auf physische, physiologische oder verhaltenstypische Merkmale	Ja, da sich die Handflächenabdrücke auf physische Merkmale beziehen.
☐	Sie ermöglichen oder bestätigen die eindeutige Identifizierung einer natürlichen Person	Ja, da das Ziel des Projekts darin besteht, Handflächenabdrücke zur Identifizierung natürlicher Personen zu verwenden.

Rechtliche Regelung: Besondere Kategorien personenbezogener Daten			
Betrifft die Tätigkeit biometrische Daten?	Ja	☐	Spezifische Regelung für besondere Kategorien personenbezogener Daten gilt
	Nein		Spezifische Regelung für besondere Kategorien personenbezogener Daten gilt nicht

4.2 Vorbereitungsphase

4.2.1 Benennung eines Datenschutzbeauftragten (DSB)

Zur Bewertung, ob ein DSB erforderlich ist, prüfen die Entwickler die Anforderungen laut Artikel 37 DSGVO. Da dort häufig das *Kriterium* des „umfangreichen Verarbeitung" genannt wird, beschließen die Entwickler, zunächst zu prüfen, ob die Verarbeitung als umfangreiche angesehen werden kann, wobei sie den Ansatz der Artikel-29-Datenschutzgruppe übernehmen.

Bewertung des Kriteriums „umfangreiche Verarbeitung”	
Anzahl der betroffenen Personen	Voraussichtlich 30 bis 50 betroffene Personen
Datenvolumen und/oder Bandbreite der unterschiedlichen, zu verarbeitenden Datenelemente	Es werden personenbezogene Daten (z. B. Name, Alter usw.) und besondere Datenkategorien (Handflächenabdrücke) verarbeitet
Dauer der Datenverarbeitungstätigkeit	Die Entwickler gehen davon aus, dass die Studie 1 Jahr dauern wird.
Geografische Ausdehnung der Datenverarbeitungstätigkeit	Die Entwickler gehen davon aus, dass die Studie eine lokale Ausdehnung hat (Gemeinde)

Nach der Bewertung entscheiden die Entwickler, dass die Verarbeitungstätigkeit als „umfangreich“ eingestuft werden kann. Auch wenn keine quantitativen *Kriterien* verfügbar sind und das Ergebnis der Bewertung daher nicht als schlüssig angesehen werden kann, kommen sie zu dieser Entscheidung, um einen vorsichtigeren Ansatz zu verfolgen.

Nach der Bewertung des *Kriteriums* der „umfangreichen Verarbeitung“ bewerten die Entwickler die Notwendigkeit, einen DSB zu benennen.

Anforderungen für die Benennung eines Datenschutzbeauftragten		
„Die Verarbeitung wird von einer Behörde oder öffentlichen Stelle durchgeführt, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln”	☐	Trifft nicht zu
„Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der Durchführung von Verarbeitungsvorgängen, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen”	☐	Trifft nicht zu (keine regelmäßige oder systematische Überwachung)
„Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9”	☐	Trifft zu (besondere Datenkategorien und „umfangreiche Verarbeitung”)
„Die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters besteht in der umfangreichen Verarbeitung […] von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10”	☐	Trifft nicht zu (keine personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten)

„Der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen"	?	Trifft nicht zu (kein spezifisches Recht der Union oder der Mitgliedstaaten)

Da eine der Anforderungen zutrifft, beschließen die Entwickler die Benennung eines DSB. Der Verantwortliche (Developing Inc.) hat keinen DSB ernannt. Daher entscheiden die Entwickler, einen solchen einzustellen.

Rechtliche Regelung: Besondere Kategorien personenbezogener Daten			
Erfüllt die Tätigkeit eine der Anforderungen für einen DSB?	Ja	?	Die Benennung eines DSB ist obligatorisch
	Nein		Die Benennung eines DSB ist nicht obligatorisch

4.2.2 Ermittlung des Datenerhebungsansatzes

Die Entwickler beschließen, die personenbezogenen Daten direkt bei den betroffenen Personen zu erheben. Diese werden in das Labor von Design Inc. eingeladen, wo Abdrücke der Handflächen genommen werden.

4.2.3 Ermittlung der am besten geeigneten Rechtsgrundlage

Bevor die Entwickler die am besten geeignete Rechtsgrundlage ermitteln können, müssen sie prüfen, ob eine der Ausnahmen für die Verarbeitung besonderer Kategorien personenbezogener Daten zutrifft.

Verfügbare Rechtsgrundlagen für die Verarbeitung biometrischer Daten gemäß der DSGVO		
Ausdrückliche Einwilligung	?	Trifft zu
Arbeitsrecht, Recht der sozialen Sicherheit und Sozialschutz	?	Trifft nicht zu (erfordert ein zusätzliches Gesetz; eine Prüfung der einschlägigen Vorschriften hat bestätigt, dass es in diesem Staat nicht existiert)
Lebenswichtige Interessen	?	Trifft nicht zu
Tätigkeiten von Vereinigungen oder sonstigen Organisationen ohne Gewinnerzielungsabsicht	?	Trifft nicht zu
Die Daten wurden von der betroffenen Person öffentlich gemacht	?	Trifft nicht zu
Rechtsansprüche oder Handlungen der Gerichte	?	Trifft nicht zu

Erhebliches öffentliches Interesse	?	Trifft nicht zu (erfordert ein zusätzliches Gesetz; eine Prüfung der einschlägigen Vorschriften hat bestätigt, dass es in diesem Staat nicht existiert)
Versorgung im Gesundheits- oder Sozialbereich	?	Trifft nicht zu (erfordert ein zusätzliches Gesetz; eine Prüfung der einschlägigen Vorschriften hat bestätigt, dass es in diesem Staat nicht existiert)
Öffentliches Interesse im Bereich der öffentlichen Gesundheit	?	Trifft nicht zu (erfordert ein zusätzliches Gesetz; eine Prüfung der einschlägigen Vorschriften hat bestätigt, dass es in diesem Staat nicht existiert)
Archivzwecke, Forschungszwecke oder statistische Zwecke	?	Trifft nicht zu (erfordert ein zusätzliches Gesetz; eine Prüfung der einschlägigen Vorschriften hat bestätigt, dass es in diesem Staat nicht existiert)

Da die einzige anwendbare Ausnahme die „ausdrückliche Einwilligung“ ist, beschließen die Entwickler auch, die „Einwilligung“ als Rechtsgrundlage für die Datenverarbeitung zu wählen.

Nach Prüfung der Rechtsgrundlage und in Anbetracht der Tatsache, dass die Daten direkt bei den betroffenen Personen erhoben werden (siehe 4.2.2 „Ermittlung des Datenerhebungsansatzes“), bereiten die Entwickler die Informationen vor, die den betroffenen Personen in der Einwilligungserklärung zur Verfügung gestellt werden.

Informationen, die den betroffenen Personen je nach Erhebungsverfahren zur Verfügung gestellt werden müssen	
Identität und Kontaktdaten des Verantwortlichen	Developing Inc. (Verantwortlicher) Developers Straße 99, 21010 Developonia +49 – 0123456, info@developinginc.com
Gegebenenfalls Identität und Kontaktdaten des Vertreters des Verantwortlichen	Nicht anwendbar
Kontaktdaten des Datenschutzbeauftragten	Max Mustermann (DSB von Developing Inc.) Developers Straße 99, 21010 Developonia +49 – 0123457, dpo@developinginc.com
Zwecke der Verarbeitung	Erforschung eines Ansatzes zur Verwendung von Handflächenabdrücken zur Identifizierung von Arbeitnehmern am Arbeitsplatz, Entwicklung und Test der entsprechenden Technologie sowie Veröffentlichung der Ergebnisse
Kategorien der betroffenen personenbezogenen Daten	Vorname, Nachname, Geburtsdatum, Adresse, Telefonnummer, E-Mail-Adresse, Handflächenabdruck
Rechtsgrundlage für die Verarbeitung	Ausdrückliche Einwilligung
Gegebenenfalls berechtigte Interessen des Verantwortlichen oder eines Dritten	Nicht anwendbar (keine Verfolgung berechtigter Interessen)
Empfänger oder Kategorien von Empfängern der personenbezogenen Daten	Developing Inc. (Verantwortlicher)
Die Absicht des Verantwortlichen, personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln	Nicht anwendbar (keine Übermittlung)
Im Falle einer Übermittlung das Vorhandensein oder Nichtvorhandensein eines Angemessenheitsbeschlusses oder gegebenenfalls ein Hinweis auf die Garantien und die Mittel, um eine Kopie der Daten zu erhalten	Nicht anwendbar (keine Übermittlung)
Zeitraum, für den die personenbezogenen Daten gespeichert werden, bzw., falls dies nicht möglich ist, die Kriterien zur Festlegung dieses Zeitraums	Dauer der Forschung (voraussichtlicher Beginn: 01.01.2022, Dauer: 1 Jahr), bis das System entwickelt und getestet ist

Das Bestehen des Rechts auf Auskunft, Berichtigung oder Löschung, Einschränkung der Verarbeitung, Widerspruch und Übertragbarkeit	Betroffene Personen können ihre Rechte gemäß Artikel 12–22 DSGVO ausüben
Im Falle der „ausdrücklichen Einwilligung" als Rechtsgrundlage das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen	Betroffene Personen können ihre Einwilligung widerrufen. In diesem Fall wird Developing Inc. neue betroffene Person ermitteln
Das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen	Beschwerden können bei der Datenschutzaufsichtsbehörde von Developonia eingereicht werden. Kontaktdaten werden bereitgestellt.
Ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder eine Voraussetzung für den Abschluss eines Vertrags ist und ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, sowie die Folgen einer Nichtbereitstellung	Die Bereitstellung ist weder gesetzlich noch vertraglich vorgeschrieben.
Das Vorliegen einer automatisierten Entscheidungsfindung, einschließlich Profiling	Die Verarbeitung umfasst keine automatisierte Entscheidungsfindung
Im Falle einer automatisierten Entscheidungsfindung Angaben zur Logik, zur Bedeutung und zu den voraussichtlichen Folgen für die betroffene Person	Nicht anwendbar

4.2.4 Einrichtung eines Repository für unterstützende Dokumentation

Der DSB von Developing Inc. erstellt ein Repository, in dem die Dokumentation über die Verarbeitung archiviert wird. Die Unterlagen werden lokal auf den Servern von Developing Inc. gespeichert. Die Speicherarchitektur von Developing Inc. ist redundant, um die Geschäftskontinuität zu gewährleisten, und der Inhalt der Server wird regelmäßig gesichert.

Die Entwickler ermitteln die folgenden zwingend vorgeschriebenen Unterlagen:

Unterlagen: Checkliste		
Geeignete Datenschutzvorkehrungen	☐	Trifft zu
Datenschutzhinweis	☐	Trifft zu
Datenspeicherungserklärung	☐	Trifft zu
Datenspeicherungsplan	☐	Trifft zu
Verzeichnis von Verarbeitungstätigkeiten (ggf.)	☐	Trifft zu (siehe unten)

Einwilligungserklärung (ggf.)	?	Trifft zu (Einwilligung als Rechtsgrundlage)
Datenverarbeitungsvertrag mit Lieferanten	?	Trifft nicht zu (keine Lieferanten mit Zugang zu personenbezogenen Daten)
Datenschutz-Folgenabschätzung	?	Trifft zu (siehe Abschnitt 4.2.5)
Vertragsklauseln für die Übermittlung personenbezogener Daten (falls zutreffend)	?	Trifft nicht zu (keine Übermittlung)
Benennung eines EU-Vertreters (ggf.)	?	Trifft nicht zu (Sitz von Developing Inc. mit Sitz ist in der Europäischen Union)
Verfahren zur Reaktion auf und Meldung von Datenschutzverletzungen	?	Trifft zu
Verzeichnis der Datenschutzverletzungen	?	Trifft nicht zu (keine Datenschutzverletzung aufgetreten)
Meldungsformular von Datenschutzverletzungen an die Aufsichtsbehörde	?	Trifft nicht zu (keine Datenschutzverletzung aufgetreten)
Formular zur Benachrichtigung der von einer Datenschutzverletzung betroffenen Person	?	Trifft nicht zu (keine Datenschutzverletzung aufgetreten)

In diesem Szenario verfügt die Design Inc. über ein Verzeichnis der Verarbeitungstätigkeiten. Obwohl es sich um ein kleines Unternehmen mit weniger als 250 Mitarbeitern handelt, werden die Mitarbeiter betreffende Daten verarbeitet (z. B. Gehaltsabrechnung, Organisation von Betriebsausflügen usw.). Developing Inc. hat keine eigene Vorlage für das Verzeichnis der Verarbeitungstätigkeiten erstellt und die von der französischen Aufsichtsbehörde bereitgestellte Vorlage übernommen[801].

4.2.5 Prüfen, ob eine Datenschutz-Folgenabschätzung erforderlich ist

Die DSGVO verlangt eine Datenschutz-Folgenabschätzung, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Entwickler sind sich nicht sicher, ob die Verarbeitung solche Risiken zur Folge hat. Sie beschließen daher, die Verarbeitung anhand der oben genannten neun von der Artikel 29-Datenschutzgruppe vorgeschlagenen *Kriterien* zu bewerten.

***Kriterien* einer mit einem hohen Risiko behafteten Verarbeitung**

[801] Die Vorlage ist abrufbar unter: Commision Nationale Informatique & Libertés, Record of Processing Activities, August 2019, https://www.cnil.fr/en/record-processing-activities.

Bewertung oder Bewertung (z. B. Profiling)	☐	Trifft nicht zu
Automatisierte Entscheidungsfindung mit rechtlicher oder ähnlicher signifikanter Wirkung	☐	Trifft nicht zu
Systematische Überwachung	☐	Trifft nicht zu
Sensible Daten oder Daten von sehr persönlicher Natur	☐	Trifft zu (siehe unten)
Daten werden in großem Umfang verarbeitet	☐	Trifft zu (siehe Abschnitt 4.2.1)
Matching oder Kombination von Datensätzen (über die vernünftigen Erwartungen der betroffenen Person hinaus)	☐	Trifft nicht zu
Daten zu gefährdeten Personen	☐	Trifft nicht zu
Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen	☐	Trifft nicht zu (siehe unten)
Die Verarbeitung an sich verhindert, dass betroffene Personen ein Recht ausüben oder eine Dienstleistung oder einen Vertrag in Anspruch nehmen	☐	Trifft nicht zu

Die Bewertung ergibt, dass die Verarbeitung mindestens zwei *Kriterien* erfüllt. Das erste Kriterium betrifft die Art der personenbezogenen Daten, die verarbeitet werden sollen. Da im Rahmen dieser Forschungstätigkeit Handflächenabdrücke als biometrische Daten ermittelt wurden, kommen die Entwickler zu dem Schluss, dass diese Daten das *Kriterium* der Sensibilität und der sehr persönlichen Natur erfüllen. Das zweite *Kriterium* betrifft den Umfang der Verarbeitung. Die Entwickler haben bereits ermittelt, dass die Verarbeitung als „umfangreich“ einzustufen ist (siehe 4.2.1 „Benennung eines Datenschutzbeauftragten (DSB)“).

Die Entwickler prüfen darüber hinaus das *Kriterium* „Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen“. Dieses Kriterium trifft nicht zu, da sich die Tätigkeit auf die Forschung konzentriert und eine konkrete Anwendung in einem organisatorischen Kontext bei der derzeitigen Tätigkeit nicht vorgesehen ist.

Datenschutz-Folgenabschätzung			
Ist die Verarbeitung mit einem „hohe Risiko” behaftet?	Ja	☐	Eine DSFA ist obligatorisch
	Nein		Eine DPIA ist optional

4.2.6 Durchführung einer Datenschutz-Folgenabschätzung

Da die Aufsichtsbehörde von Developonia keine Leitlinien für die Durchführung einer Datenschutz-Folgenabschätzung erstellt hat, führen die Entwickler auf Anraten des Datenschutzbeauftragten diese anhand der vom EDSA gebilligten Leitlinien der Artikel-29-

Datenschutzgruppe und der von der französischen Aufsichtsbehörde bereitgestellten Vorlage durch[802]. Das Ergebnis der Datenschutz-Folgenabschätzung zeigt, dass alle Risiken für die Rechte und Freiheiten der betroffenen Personen auf ein akzeptables Niveau gemindert werden, das für keine der identifizierten Risiken hoch ist.

Das Ergebnis der Datenschutz-Folgenabschätzung wird im Repository für unterstützende Unterlagen gespeichert.

4.2.7 Umsetzung risikomindernder Maßnahmen

Nach der Durchführung der Datenschutz-Folgenabschätzung stellen die Entwickler fest, dass die technischen und sicherheitsrelevanten Maßnahmen geeignet sind, die Rechte und Freiheiten der betroffenen Personen zu schützen, und als angemessene Garantien gemäß Artikel 89 DSGVO angesehen werden können.

4.3 Ausführungsphase

4.3.1 Verarbeitung biometrischer Daten

Nachdem das Forscherteam alle Informationen an die betroffenen Personen verteilt und deren ausdrückliche Einwilligung eingeholt hat, beginnt es mit der Erhebung der biometrischen Daten der betroffenen Personen. Die Forscher nehmen Abdrücke der Hände jedes Teilnehmers und speisen diese in ein System der künstlichen Intelligenz ein, um die biometrischen Merkmale zu extrahieren (z. B. Handformen, Erhebungen, Vertiefungen usw.). Alle Komponenten des Systems der künstlichen Intelligenz, einschließlich des zugrundeliegenden Algorithmus, werden von den Forschern selbst entwickelt und gewartet. Zudem sind keine anderen Personen beteiligt oder haben Zugriff auf die vom System der künstlichen Intelligenz verarbeiteten Daten. Die Komponenten der künstlichen Intelligenz des Systems werden gemäß den Schritten entwickelt, die in dem Dokument „Guidelines on ethical and legal issues regarding artificial intelligence in ICT research and innovation“ beschrieben sind.

4.3.2 Entwicklung der Benutzeroberfläche des biometrischen Systems

Das Forschungsteam beschließt, dass die Interaktion mit dem biometrischen System über zu diesem Zweck vorgesehene Kioske erfolgen soll. Während der Forschung werden die Kioske im Labor der Entwickler aufgestellt. Die Kioske sollen Daten erheben und lokal speichern, wobei die Benutzer mit den Kiosken in Anwesenheit des Forschungsteams interagieren. Der Einsatz der Kioske in der kontrollierten Umgebung des Labors wird den Entwicklern Aufschluss über die Umsetzbarkeit der Technologie geben und als Pilotversuch für den künftigen Einsatz an tatsächlichen Arbeitsplätzen dienen.

Eines der Ziele der Forschung ist die Rationalisierung der Authentifizierung von Arbeitnehmern. Dazu wollen die Forscher den Authentifizierungsprozess beschleunigen, indem sie die Benutzerfreundlichkeit erhöhen und so die Zeit, die jeder Benutzer am Kiosk verbringt, minimieren. Aus diesem Grund beschließen sie, die Funktionen in zwei verschiedene Arten von Kiosken aufzuteilen: einen für die Authentifizierung (Authentifizierungskiosk) und einen für andere Funktionen wie den Zugriff auf Informationen und die Aktualisierung personenbezogener Daten (Zusatzkiosk). Mitarbeiter, die andere

[802] Commision Nationale Informatique & Libertés, Privacy Impact Assessment (PIA). Templates.

Schritte als die Authentifizierung durchführen müssen, verlansamen so nicht die Authentifizierung der anderen Mitarbeiter.

Der Authentifizierungskiosk besteht aus zwei Hauptkomponenten: einem Scanner für die Hand und einem Monitor. Bei erfolgreicher Authentifizierung wird ein grünes Zeichen angezeigt, die Tür öffnet sich und der Mitarbeiter kann weitergehen. Die Authentifizierung wird nicht aufgezeichnet (da das Ziel nicht darin besteht, die Arbeitszeiten von Personen zu messen), und der Monitor zeigt keine Informationen über die Person an.

Der Zusatzkiosk umfasst die gleichen Elemente wie der Authentifizierungskiosk, der Monitor ist allerdings ein Touchscreen, um sicherzustellen, dass die Benutzer mit dem System interagieren können. Außerdem ist der zusätzliche Kiosk mit einer Umfassung versehen, um das Schulter-Surfen zu verhindern. Der Benutzer kann den Zusatzkiosk problemlos durch das Scannen seiner Handfläche aktivieren. Daraufhin wird auf dem Monitor ein Menü mit drei Optionen angezeigt:

- Informationen zur Datenverarbeitung anzeigen: Diese Option öffnet ein Pop-up-Fenster, in dem alle unter 4.2.3 „Ermittlung der geeignetsten Rechtsgrundlage“ aufgeführten Informationen bereitgestellt werden;
- Zugriff auf und Berichtigung von personenbezogenen Daten: Diese Option öffnet ein Pop-up-Fenster, in dem alle personenbezogenen Daten der betroffenen Personen angezeigt werden und in dem der Nutzer diese Daten berichtigen kann, einschließlich der Aufnahme neuer Handflächenabdrücke;
- Recht auf Berichtigung, Einschränkung, Datenübertragbarkeit oder Widerspruch ausüben: Diese Option ist derzeit im Kiosk-Prototypen deaktiviert. Wenn ein Nutzer diese Option auswählt, erhalten die Mitglieder des Forschungsteams eine Warnmeldung auf ihren mobilen Geräten. Sie müssen sich dann bei der betroffenen Person vergewissern, ob diese tatsächlich eines ihrer Rechte ausüben möchte.

4.3.3 Testen des biometrischen Systems

Sobald das System entwickelt ist, können die Forscher es testen und seine Leistung überprüfen (darunter Fehlerquote, Geschwindigkeit der Authentifizierung, Energieverbrauch usw.). Zu diesem Zweck bringen Sie die betroffenen Personen zusammen, um die Nutzung des Systems simulieren.

Da das Testen des Systems eine der Hauptaktivitäten der Forschung ist, die betroffenen Personen bereits ihre ausdrückliche Einwilligung zu den Tests gegeben haben und keine zusätzlichen personenbezogenen Daten verarbeitet werden, kommt das Forschungsteam zu dem Schluss, dass die Risiken für die Rechte und Freiheiten der betroffenen Personen angemessen berücksichtigt werden. Daher fährt es mit den Tests fort.

4.3.4 Verbreitung der Ergebnisse

Nach Abschluss der Tests und Erhebung aller Testdaten kann das Forschungsteam schließlich einen Artikel verfassen, in dem die Technologie beschrieben und die Ergebnisse vorgestellt werden. In der Zuversicht, dass das System einheitlich funktioniert, beschließen sie, die Technologie als Open-Source zu veröffentlichen, damit andere Forscher ihre eigenen Tests durchführen und die Ergebnisse validieren können. Im Anschluss an diese Entscheidung beschließen die Forscher, alle personenbezogenen Daten der Personen, die an der Forschungstätigkeit teilgenommen haben, zu löschen.

4.3.5 Löschung oder Vernichtung von Daten

Alle personenbezogenen Daten werden vollständig gelöscht.

Checkliste

Diese Checklisten sind nicht durch Externe überarbeitet und validiert worden. Nichtsdestotrotz hält PANELFIT sie für den Zweck, auf den diese Leitlinien abzielen, für angemessen.

Checkliste für die Designphase

Schritt
☐ Identifizieren Sie die Ziele der jeweiligen Aktivität.
☐ Überprüfen Sie ob die Aktivität unter "Forschung" fällt.
☐ Identifizieren Sie die Rollen des Forschungsteams und der von anderen Interessenvertretern.
☐ Vergewissern Sie sich, dass die Verarbeitung von biometrischen Daten notwendig ist um die Ziele der Aktivität erreichen zu können.

Checkliste für die Vorbereitungsphase

Schritt
☐ Überprüfen Sie ob eine der fünf Voraussetzungen für einen DPO gegeben ist.
☐ Wenn Sie eine öffentliche Behörde sind, überprüfen Sie ob ein DPO durch eine andere öffentliche Behörde ernannt wurde.
☐ Veröffentlichen Sie die Kontaktinformationen des DPO.
☐ Identifizieren Sie ob die Datenerhebung direkt über die betroffene Person (data subject) erfolgt, oder indirekt.
☐ Prüfen Sie, ob Sie für eine Ausnahme von der Informationspflicht gegenüber der betroffenen Person in Frage kommen.
☐ Erfassen Sie die Beurteilung, ob eine Befreiung von der Informationspflicht in Frage kommt.
☐ Definieren Sie ein internes Verfahren zur Gewährleistung der Richtigkeit der verarbeiteten Daten.
☐ Erfassen Sie, ob Ausnahmen für die Verarbeitung besonderer Kategorien personenbezogener Daten gelten.
☐ Falls ein zusätzliches Gesetz erforderlich ist, überprüfen Sie dessen Existenz. Falls nicht, geben Sie eine andere Ausnahme an.
☐ Falls Ausnahmen gelten, ist die Rechtsgrundlage für die Datenverarbeitung gemäß Artikel 6 DSGVO anzugeben.

☐ Wenn Sie sich auf die Zustimmung verlassen, stellen Sie sicher, dass diese ausdrücklich ist.
☐ Bewahren Sie Aufzeichnungen über die Einverständniserklärungen auf
☐ Erstellen Sie einen Dokumentenspeicher, der mindestens die von der DSGVO vorgeschriebenen Dokumente enthält.
☐ Überprüfen Sie, ob die Verarbeitung der Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt.
☐ Erfassen Sie die Ergebnisse dieser vorläufigen Beurteilung.
☐ Führen Sie ein DPIA (Data Protection Impact Assessment (DPIA) / Datenschutz-Folgenabschätzung) durch falls die Datenverarbeitung ein hohes Risiko darstellt.
☐ Wenn die Risiken durch die vorgesehenen Maßnahmen nicht gemindert wurden, sind zusätzliche, geeignete, Maßnahmen zu ergreifen.
☐ Wenn die Risiken nicht gemindert werden können und es nicht möglich ist zusätzliche Maßnahmen zu ergreifen, wenden Sie sich an die Aufsichtsbehörde.
☐ Erfassen Sie das Ergebnis des DPIA.

Checkliste für die Ausführungsphase

Schritt
☐ Verarbeiten Sie die Daten unter Anwendung der in der Vorbereitungsphase festgelegten Sicherheitsvorkehrungen und Vorsichtsmaßnahmen.
☐ Bei der Entwicklung von IKT-Systemen muss sichergestellt werden, dass die betroffene Person (data subject) über eine geeignete Benutzerschnittstelle Zugang zu den erforderlichen Informationen hat.
☐ Bei der Entwicklung von IKT-Systemen sind die Risiken für die betroffenen Personen im Zusammenhang mit jeder Funktion des Systems zu bewerten.
☐ Erfassen Sie die Ergebnisse der Risikobewertung in Bezug auf die Systemfunktionen
☐ Wenn die Risiken nicht gemindert werden können, konsultieren Sie die Aufsichtsbehörde oder verzichten Sie auf die Umsetzung der Aktivität.
☐ Beachten Sie Anwendungsfälle in denen gefährdete Personen involviert sind.
☐ Im Falle des Testens von IKT-Systemen müssen Sie beurteilen, ob das Testen des Systems einen anderen Fall der Datenverarbeitung als die Entwicklung des Systems darstellt.
☐ Erfassen Sie das Ergebnis der Bewertung über das Testen als eine weitere Form der Datenverarbeitung.

☐ Falls das Testen des Systems einen anderen Fall der Datenverarbeitung darstellt, beurteilen Sie ob die Zwecke und Mittel kompatibel sind.
☐ Erfassen Sie das Ergebnis dieses Kompatibilitätstests.
☐ Beurteilen Sie ob die Verbreitung der Ergebnisse auch die Verbreitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten beinhaltet.
☐ Identifizieren Sie Ausnahmen für die Verarbeitung besonderer Kategorien personenbezogener Daten vor der Weitergabe der Daten.
☐ Identifizieren Sie die am besten geeigneten Rechtsgrundlage für die Verarbeitung personenbezogener Daten vor der Weitergabe der Daten.
☐ Benennen Sie die Empfänger der Daten als Datenverarbeiter.
☐ Informieren Sie die betreffenden Personen über den Transfer der Daten.
☐ Überprüfen Sie ob der Transfer der Daten über Landesgrenzen hinweg stattfindet.
☐ Wenn es sich um eine internationale Übermittlung der Daten handelt und keine Ausnahmeregelungen gelten, geben Sie ein Übermittlungsinstrument an.
☐ Überprüfen Sie ob das Speichern der personenbezogenen Daten rechtmäßig ist.
☐ Erfassen Sie die Ergebnisse der Beurteilung zur Rechtmäßigkeit der Datenspeicherung
☐ Falls die Aufbewahrung personenbezogener Daten rechtswidrig ist, löschen oder anonymisieren Sie diese.