— Daten- und Geschäftsgeheimnisschutz als nichtfunktionale Anforderung für Kollaborationsnetzwerke

Datenbasierte Regelung kollaborativer Wertschöpfungsnetzwerke mittels geschützter Transparenz (ReKoNeT)

Dr. Manuela Wagner, Daniel Vonderau

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Veröffentlichung: 01.06.2022

Version 1.0

— Inhaltsverzeichnis

— Einführung

Um ein wettbewerbsfähiges und datenschutzkonformes kollaboratives Wertschöpfungsnetzwerk planen, entwickeln und umsetzen zu können liefert dieser Teil des Handlungsleitfadens den Entscheidungsträger:innen das notwendige Verständnis für die von Anfang an mit zu bedenkenden rechtlichen Anforderungen an ein solches System. Der Fokus liegt hierbei auf den Themen Datenschutz und Geschäftsgeheimnisschutz. Der frühzeitige Einbezug von rechtlichen Anforderungen erspart zeit- und kostenintensive Nachbesserungen im späteren Einsatz.

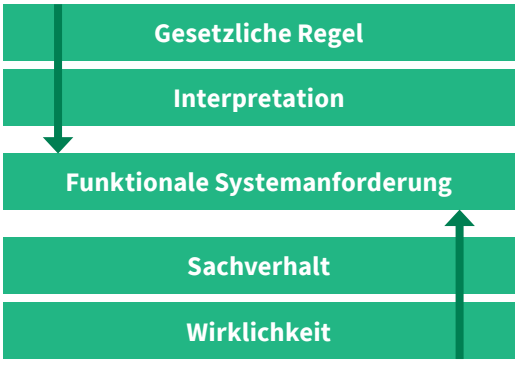
Die Anforderungsanalyse ist der Startpunkt jeder Projektplanung, daher erfolgt zunächst eine Einführung in die methodischen Ansätze der informationsrechtlichen Anforderungsanalyse und Projektbegleitung. Im Anschluss erfolgt die Darstellung der inhaltlichen Anforderungen des Datenschutzrechts mit besonderem Schwerpunkt auf die Verarbeitung von Beschäftigtendaten im Unternehmenskontext und Optionen der Datenminimierung durch Anonymisierung sowie einer kurzen Erläuterung der Regelungen des Geschäftsgeheimnisschutzes.

— Anforderungsanalyse

Die Methode, um die erforderlichen Informationen bzgl. der Datenarten- und Flüsse zu erheben, ist abhängig von der Unternehmensgröße und Organisationsform. Welche Methode für das jeweilige Unternehmen geeignet ist, hängt daher von der individuellen Ausgangssituation ab. Die gewählte Methode kann einen starken Einfluss darauf haben, ob die erforderlichen Informationen überhaupt erlangt werden können.

Die klassische systematische Berücksichtigung rechtlicher Anforderungen in der Softwareentwicklung folgt der KORA-Methode zur Konkretisierung rechtlicher Anforderungen [73], [74]. Die Zielsetzung liegt insbesondere in einer präventiven Vorsorge zur Verhinderung von künftig möglichen Risiken des Technikeinsatzes [74]. Es geht darum die Art und Weise wie gesetzliche Anforderungen formuliert sind, in konkrete, funktionale Anforderungen an die Systementwicklung zu spezifizieren und dabei zu „übersetzen“. Denn Entwickler:innen technischer Systeme verfügen im Normalfall über keine juristische Ausbildung, sodass rechtliche Anforderungen von Rechtsspezialist:innen analysiert und kontextspezifisch aufbereitet werden müssen [75]. Die Spezifizierung abstrakter rechtlicher Vorgaben in konkrete technische Anforderungen erfolgt dabei iterativ [74]. Ähnlich der richterlichen Urteilsfindung müssen relevante Gesetze identifiziert, rechtliche Zielsetzungen extrahiert, Interpretationsspielräume ausgelotet und Designalternativen bewertet werden [76].

Dabei sind zwei Betrachtungsebenen zu unterscheiden: die Verdichtung der regelmäßig technikneutralen und abstrakten gesetzlichen Vorgaben zu konkreten technischen Gestaltungsvorschlägen einerseits und die Erfassung der Realweltphänomene (Wirklichkeit) als zu betrachtender Sachverhalt andererseits (Abbildung 2).



Die grundlegende Fragestellung, die aus datenschutzrechtlicher Perspektive beantwortet werden muss, lautet dabei: Welche Datenverarbeitung dient zu welchem Zeitpunkt welcher Entscheidung als Grundlage?

Interview

Ein Interviewformat bietet sich immer dann an, wenn ein Unternehmen nur über wenig dokumentierte Prozesse verfügt und die Zahl der Verantwortlichen eine gewisse Größe nicht übersteigt. Nachteile von Einzelinterviews liegen allerdings in der bedingten Reproduzierbarkeit des Erkenntnisgewinns, der oftmals nur begrenzten Einblicke in kollaborative Datenverarbeitungsprozesse in Wertschöpfungsnetzwerken aus der Einzelperspektive des/der Interviewten gewährt.

Fragebogen

Sowohl für die Vorbereitung eines Interviews, aber auch als eigenständige Methode, um Informationen zu den geplanten Datenverarbeitungsprozessen in systematisch-strukturierter Art und Weise zu erlangen, kann ein Fragebogen verwandt werden. Als erster Schritt geht es dabei darum den Personenbezug der verarbeiteten Daten festzustellen. Hierfür sollten zumindest Fragen zu den folgenden Kategorien enthalten sein:

1. Informationsebene: Datenarten
2. Personenebene: Datenzugriffe
3. Prozess-/Aktivitätsebene: Datenverarbeitungsschritte
4. Zweck der einzelnen Datenverarbeitungsschritte

Diese Informationen sind zunächst elementar für die Kategorisierung der Datenqualität sowie einer ersten rechtlichen Einordnung. Als weitere Kategorie können Fragen gestellt werden zu:

5. Alternativen zur technischen Gestaltung.

Die komplexe und wechselwirkende Struktur verteilter IKT-Systeme in kollaborativen Wertschöpfungsnetzwerken erfordert es, dass für eine umfassende rechtliche Bewertung, die sich auch an verändernden rechtlichen Rahmen-

bedingungen und technischen Umsetzungsentscheidungen orientieren muss, bereits im Stadium der Anforderungsanalyse aus den technischen Zielen die Einsatzszenarios abgeleitet werden sollten. Das umfassende Verständnis des technischen Entwurfs sowie der darauf basierenden technischen Gestaltungsziele ist Grundlage für die Identifikation anzuwendender Normen und frühzeitige Ermittlung potentieller Implikationen. Die gewählte Methodik zur Informationsbeschaffung und Aufbereitung muss daher die folgenden Parameter erfüllen:

- Dokumentation
- Transferfähigkeit
- Aktualisierbarkeit
- Vergleichbarkeit

Dokumentation: Für ein belastbares Wissensmanagement im Projekt sollten die anvisierten Datenverarbeitungsvorhaben aus den unterschiedlichen Domänen bei den jeweiligen Projektpartnern abgefragt und in Textform vorgehalten werden. Visualisierungskonzepte und Methoden der Modellierung können dabei unterstützen ein gemeinsames Verständnis der datenschutzrechtlichen Vorgänge zu generieren.

Transferfähigkeit: Dabei sollten bewusst keine datenschutzrechtlichen Fachbegriffe verwandt werden, sondern allgemeinsprachliche Formulierungen verwendet werden, um die gewünschten Informationen zu erhalten. Als Interviewe bieten sich Projektverantwortliche als auch im Projekt mit Datenschutz oder IT-sicherheitsrelevanten Themen betraute Personen an. Eine oft anzutreffende Herausforderung liegt in der uneinheitlichen Verwendung von Begrifflichkeiten, die sich in unterschiedlichen Domänen entwickelt und etabliert haben.

Aktualisierbarkeit: Bei der Bearbeitung der Fragebögen hat sich oftmals herausgestellt, dass Informationen ausgelassen werden, weil ein Prozess ggf. noch nicht finalisiert wurde und/oder ein Detail als nicht wichtig erachtet wurde. Dies hatte zur Folge, dass bestimmte Prozesse nicht erfasst werden konnten, bei denen sich zu einem späteren Zeitpunkt herausgestellt hat, dass dieser doch personenbezogenen Daten beinhaltete. Daher ist eine Vorgehensweise zu wählen, durch die Änderungen im Projekt nachvollzogen werden können.

Vergleichbarkeit: Das gewählte Format muss bei kollaborativem Zusammenwirken unterschiedlicher Stakeholder einen Arbeitsmodus bieten, um verschiedene Rückmeldungen zu abzugleichen und so zu einem stimmigen Ergebnis zusammenzuführen.

Durch die Auswertung der Daten können Rückschlüsse auf datenschutzrelevante Vorgänge gezogen werden, die bei der Systementwicklung Berücksichtigung finden konnten. Dabei hat sich herausgestellt, dass bei der Bearbeitung der Fragebögen oftmals Informationen ausgelassen werden, weil ein Prozess ggf. noch nicht finalisiert wurde und/oder ein Detail als nicht wichtig erachtet wurde. Dies hatte zur Folge, dass bestimmte Prozesse nicht erfasst werden konnten, bei denen sich zu einem späteren Zeitpunkt herausgestellt hat, dass dieser doch anders als zuvor angenommen hatte die Verarbeitung personenbezogener Daten beinhaltete.

— Datenschutzrecht als nichtfunktionale Anforderung für Kollaborationsnetzwerke

Datenschutzrechtliche Aspekte als nichtfunktionale Anforderungen zu verstehen, die bei einer Systementwicklung von Anfang an mitgedacht werden müssen, ist ein erster wichtiger Schritt, um die vielschichtigen Vorgaben zur Umsetzung datenschutzrechtlicher Pflichten in einem zukunftsgewandten Themenfeld wie dem transparenten kollaborativen Wertschöpfungsnetzwerk der Zukunft zielgerichtet begegnen zu können. Denn die Technikgestaltung hat einen entscheidenden Einfluss auf die potentielle Eingriffsintensität in betroffene Persönlichkeitsrechte. Zudem werden Verantwortliche unter dem Stichwort „Privacy-by-Design“ zu einer datenschutzfreundlichen Technikgestaltung angehalten.

Führt man sich vor Augen, dass schon die allgemein zu erfüllenden datenschutzrechtlichen Anforderungen in einem Industrieunternehmen viele Betriebe seit Wirksamwerden der Datenschutzgrundverordnung (DSGVO) teilweise vor große Herausforderungen stellen, so kann man sich unschwer vorstellen, dass diese Herausforderungen durch den verstärkten Einsatz von IT im Zuge der Digitalisierungsanstrengungen hin zu der sog. Industrie 4.0 nur noch größer werden. Dabei anzuerkennen, dass Datenschutz weder ein Hemmnis noch ein Hinderungsgrund sein muss, neuartige Wege einzuschlagen und bis dahin in diesen Bereichen nicht gekannte Technologien einzusetzen, kann in diesem Zusammenhang helfen.

Überblick über Art der Daten und Datenflüsse

Bevor man mit der Planung der Umsetzung datenschutzrechtlicher Anforderungen beginnt, gilt es sich zunächst einen Überblick über die Art der Daten, die verarbeitet werden sollen sowie die geplanten Datenflüsse zu verschaffen. Was sich zunächst wie eine triviale Aufgabe anhört, entpuppt sich bei näherer Betrachtung als komplexes Unterfangen, denn diese erste Bestandsaufnahme dient als Startpunkt und Fundament aller weiteren einzuleitenden Maßnahmen. Die Voraussetzungen dafür, dass Datenschutz als nichtfunktionale Anforderung zu beachten ist, werden im Folgenden erläutert.

Anwendbarkeit von Datenschutzvorschriften

Zunächst ist aus datenschutzrechtlicher Perspektive zu beachten, dass die Gesetze zum Schutz personenbezogener Daten nicht bei anonymen Daten oder Sachdaten Anwendung finden. Dies ergibt sich unmittelbar aus Art. 2 Abs. 1 DSGVO und Erwägungsgrund 26 S. 5:

> „Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“

> „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“

Daraus folgt, dass die DSGVO keine Anwendung findet für Daten, die keinen Personenbezug haben, oder nicht automatisiert bzw. in einem Dateisystem verarbeitet werden.[1] Man spricht hierbei vom sog. sachlichen Anwendungsbereich, der eröffnet sein muss.

Nachdem die Voraussetzungen zur Verarbeitung eindeutig bestimmbar sind, ist das Vorliegen eines Personenbezuges

1 Siehe zum Dateisystem: EuGH, Urt. v. 10.07.2018 – C-25/17.

nicht immer einfach zu ermitteln. Die gesetzliche Vorgabe scheint zunächst in Art. 4 Nr. 1 DSGVO noch eindeutig. Demnach sind

> "personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Es kommt also zusammenfassend entscheidend auf die Identifikation oder die Identifizierbarkeit einer natürlichen Person an.

Beispiel: Der Name einer Person, die Steuer- oder Sozialversicherungsnummer sind personenbezogene Daten, da mit ihnen unmittelbar eine bestimmte Person identifiziert wird. Soweit also Namen der Beschäftigten verarbeitet werden, handelt es sich um personenbezogene Daten.

Von einer Identifikation kann zusammenfassend also immer dann ausgegangen werden, wenn keine zusätzlichen Informationen mehr notwendig sind, um eine Person zu identifizieren.

Schwieriger ist die Einordnung, ab wann eine Person durch bestimmte Daten identifizierbar wird. Dies war lange Zeit umstritten. Vertreter:innen des sog. absoluten Ansatz plädierten dafür, dass Identifizierbarkeit immer dann gegeben sei, soweit nur irgendeine Person, die nicht mit dem Verantwortlichen übereinstimmen muss, einen Personenbezug herstellen kann [1], [2]. Da dieser Ansatz faktisch dazu führen könnte, dass kaum eine Datenverarbeitung denkbar wäre, bei der ein Dritter keinen Personenbezug herstellen könnte, geht der sog. relative Ansatz von den individuellen Fähigkeiten des Verantwortlichen zur Identifizierung aus [3]–[5]. Der EuGH entschied sich entsprechend der Regelung in Erwägungsgrund 26 S. 3 für eine vermittelnde Position: danach sind alle Mittel zu berücksichtigen, die nach allgemeinem Ermessen wahrscheinlich genutzt werden können, um eine Person direkt oder indirekt zu identifizieren. Liegen Zusatzinformationen bei Dritten vor und ist ein Zugang weder rechtlich ausgeschlossen noch mit unverhältnismäßigem Aufwand verbunden, ist eine Identifizierung möglich [EuGH, Urt. v. 19.10.2016 – C-582/14]. Nach diesem Ansatz ist somit eine Abwägung erforderlich, bei der die tatsächlichen Möglichkeiten des Verantwortlichen, diese Zusatzinformationen von Dritten zu erhalten mit den Kenntnissen, Mitteln und Möglichkeiten gegenübergestellt werden. Nach dem Urteil weiterhin umstritten war die Frage, ob Zugangsmöglichkeiten individuell oder abstrakt zu bestimmen sind: bei ersterem wäre im Einzelfall zu klären, ob eine den Datenzugang legitimierende Norm tatsächlich erfüllt ist und welche Intentionen bestehen [6], [7]. Die EuGH-Entscheidung deutet dagegen abstrakte Bestimmung [8]–[11]. Dass eine tatsächliche Identifizierung eher unwahrscheinlich ist, soll im Gegenzug im Rahmen der Legitimationstatbestände berücksichtigbar sein [BGH, Urt. v. 16.05.2017 – VI ZR 135/13.].

Beispiel: Das Geburtsdatum oder das Gehalt einer Person allein lässt sich nicht ohne Zusatzinformationen einer bestimmten Person zuordnen. Mit einer Personalnummer ließe sich das Datum einer individuellen Person zuordnen.

Schwierigkeiten bereitet dabei auch die Einordnung von Pseudonymen. Pseudonymisierung wird in Art. 4 Nr. 5 DSGVO definiert als:

> die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden

Gänzlich anonymes Handeln ist oftmals nur in Teilbereichen sozialer Kommunikation und rechtserheblicher Interaktion möglich [5]. In rechtsgeschäftlichen wie auch gesellschaftlichen Beziehungen kann die Pseudonymisierung ermöglichen, dass die Interaktionspartner untereinander (wieder-) erkennbar bleiben ohne vollständige Identifikation [12]. Erwägungsgrund 26 S. 2 DSGVO besagt hierzu:

> Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden.

Vergibt eine verantwortliche Stelle ein Pseudonym sind regelmäßig zwei Möglichkeiten der Re-Identifizierung zu bedenken: einerseits Zugriffsmöglichkeiten auf die Zuordnungsregel und andererseits der Wiedererkennungseffekt eines mehrmalig genutzten Pseudonyms [5], [13]. Daher ist der Einsatz dynamisch wechselnder Pseudonyme zu empfehlen, diese können allenfalls temporär Wiedererkennungseffekte generieren [14].

Von besonderer praktischer Relevanz ist auch die Frage, welche Vorabprüfungspflichten Verantwortliche treffen. Liegen keine personenbezogenen Daten vor, ist die DSGVO nicht anwendbar. Allerding sind die Übergänge von anonymen zu personenbezogenen Daten im Zeitalter von Big Data fließend und zeitvariabel [15]. Die Schwierigkeit bei der Bestimmung der Re-Identifizierungsrisiken liegt darin, dass durch fortschreitende Verknüpfung mit weiteren Datenbeständen, die Gefahr eines dynamischen „Hineinwachsens“ in den Personenbezug droht [16]–[21]. Zum Erhebungszeitpunkt anonyme Daten könnten somit im Laufe ihrer Verarbeitung zu personenbezogenen Daten werden. Einige Experten empfehlen, vorsorglich im Zweifel von einem Personenbezug auszugehen und die datenschutzrechtlichen Vorschriften zu beachten [20] Andere fordern wiederum die Steuerung von (Re)Identifizierungsrisiken durch datenschutzrechtliche Vorsorgeregelungen: [5]. Aufgrund des damit verbundenen Pflichtenkanons erscheint es allerdings praktikabler ein „angemessenes Risikoniveau“ [22] im Hinblick auf Anonymität der Daten sicherzustellen. Insbesondere wenn die Zuordnung der Daten zu individualisierbaren Personen zur Zielerreichung der Produkt- und Prozessoptimierung nicht erforderlich ist, dürfte die Vermeidung des Personenbezugs sowohl dem Schutz der betroffenen Grundrechte als auch den Datenverwertungsinteressen der Beteiligten eher entsprechen [23].

Betriebsdaten als Sachdaten

Im Kontext kollaborativer transparenter Wertschöpfungsnetzwerke stellt sich nunmehr die Frage, inwieweit Besonderheiten in Bezug auf die Verarbeitung personenbezogener Daten bestehen. Dies ergibt sich daraus, dass ein wesentlicher Anteil des Transformationsprozesses auf Industrie-4.0-Anwendungen auf die Nutzbarkeit bislang nicht erhobener oder nicht genutzter Daten im Unternehmensbetrieb entfallen. Ein schon aus bisherigen Industriekontexten bekannter Begriff ist der der Betriebsdatenerfassung. Darunter sind alle Vorgänge der Erhebung verschiedener unternehmerisch relevanter Daten, die zur Steuerung eines Unternehmens beitragen können, zu verstehen [24]. Dabei kann es sich um Daten zu Kundenaufträgen, zur Belegschaft, zur Infrastruktur, zu Vorräten und Qualitätskennzahlen handeln [24]. Von besonderem Interesse sind insbesondere die Daten zur Infrastruktur, da Zustände und Laufzeiten von Maschinen bzw. Standzeiten von Werkzeugen auf den ersten Blick keinerlei datenschutzrechtliche Implikationen bergen.

Sachdaten mit Personenbezug

Mithin könnte man annehmen, dass es sich hierbei lediglich um Sachdaten ohne jedweden Personenbezug handele. Denn Sachdaten beziehen lediglich auf eine Sache und beschreiben diese [Schild in: [25] Art. 4, Rn. 22]. Je nach Detaillierungsgrad können diese Daten jedoch einen Personenbezug enthalten. Dies ist insbesondere der Fall, wenn Sachdaten eine Verknüpfung zu einer Person erlauben [Schild in: [25] Art. 4, Rn. 25].

Beispiel: Die Laufzeit einer Maschine wird zentral erfasst und ausgewertet. Bedient wird die Maschine lediglich von einer Person. Die Daten, die dabei entstehen sind somit einer Person zuordenbar und haben damit einen Personenbezug.

Sachbezogene Daten sind auch als personenbezogen zu charakterisieren, wenn sie eine Sache identifizieren und eine Person-Sach-Beziehung Rückschlüsse auf eine natürliche Person zulassen [26]. Zur Einordnung der Identifizierbarkeit werden folgende Prüfelemente vorgeschlagen [27]:

- **Inhaltselement:** geben die Daten Auskunft über das Verhalten, den Zustand oder über Umstände einer Person?
- **Zweckelement:** Liegt der Zweck der Erhebung in der Zuordnung zu einer Person wird ebenfalls die Annahme des Personenbezugs gefordert.
- **Ergebniselement:** wird mit dem Datum ein realer Effekt in Bezug auf den Betroffenen ausgelöst? Solche Effekte können vorliegen, wenn diese geeignet sind das Verhalten, den Zustand oder die äußeren Umstände einer natürlichen Person zu beeinflussen.

Einige Schutzmaßnahmen können ergriffen werden, um das (Re-)Identifizierungsrisiko zu senken:

- Die Verknüpfung von Datenbeständen mit weiteren Daten sollte **kontrolliert** und bei Bedarf begrenzt werden. Mit jedem zusätzlichen Informationszufluss zu einem bestehenden Datenbestand sollte die Identifizierbarkeit erneut geprüft werden [20], [28]. Mittels Risikoanalyse sollte eine Prognose (auch künftig entstehenden) Personenbezugs erstellt werden [17], [29].
- Neben dem sachgerechten Einsatz von Anonymisierungstechniken [30], [31], können Zugriffsmöglichkeiten für Dritte **technisch** für bestimmte Zwecke und Zeiträume beschränkt werden [22], [32].
- Zugriffmöglichkeiten für Dritte sollten davon abhängig gemacht werden, dass sich Empfänger sanktionsbewehrt **verpflichten** keine (Re-)Identifizierung durchzuführen und Verstöße zu melden [20], [22], [29]. Bloße Absichtserklärungen können zwar die Anwendbarkeit des Datenschutzrechts nicht ausschließen [2], jedoch könnten Vertragsstrafeklauseln bei der Verhältnismäßigkeit des Aufwands berücksichtigt werden [29]. Von **anonymen** Daten kann ausgegangen werden, wenn die Kosten einer De-Anonymisierung unter Berücksichtigung personeller, zeitlicher und technologischer Möglichkeiten so hoch sind, dass vernünftigerweise mit einer Re-Identifizierung nicht gerechnet werden muss [19].

Sofern die erforderlichen datenschutzrechtlich relevanten Datenverarbeitungsprozesse erfasst wurden, müssen diese im Systemkontext dokumentiert werden.

Räumlich anwendbares Recht

Liegen personenbezogene Daten vor, stellt sich die Frage, ob der sog. räumliche Anwendungsbereich eröffnet ist. Dieser ergibt sich aus Art. 3 DSGVO. Dort sind mehrere Varianten aufgeführt, in welchen Fällen es zu einer räumlichen Anwendbarkeit der DSGVO kommen soll, insbesondere das sog. Sitzlandprinzip und das Marktortprinzip.

> (1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
>
> (2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
>
> a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
>
> b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.
>
> (3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Zusammengefasst bedeutet dies, dass soweit eine Verarbeitung von personenbezogenen Daten im Rahmen einer Tätigkeit des Verantwortlichen oder Auftragsverarbeiters

innerhalb der Europäischen Union stattfindet, oder personenbezogenen Daten von Bürgern in der Europäischen Union entsprechend dem Marktortprinzip verarbeitet werden, ist der räumliche Anwendungsbereich erfüllt und die DSGVO für das jeweilige Unternehmen als Verantwortlicher anwendbar.

Die Anwendbarkeit der DSGVO führt zu verschiedenen Pflichten, die der Verantwortliche einzuhalten hat. Hieraus wiederrum lassen sich die entsprechenden nichtfunktionalen Anforderungen und daraus abzuleitende funktionale Anforderungen für ein System entnehmen.

Umsetzung der Datenschutzgrundsätze

Für die Umsetzung der Datenschutzgrundsätze können aus abstrakten Anforderungen konkrete Funktionen folgen, die das System erfüllen muss. Beispielsweise müssen Funktionen vorgesehen werden, mit denen Betroffenenanfragen beantwortet oder Löschfristen umgesetzt werden können. Damit solche Funktionen nicht nachträglich hinzugefügt werden müssen, sollten sich Verantwortliche frühzeitig mit dem Pflichtenkanon vertraut machen.

Rechtmäßigkeit, Treu und Glauben: Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Die im Beschäftigtenkontext besonders relevanten Konstellationen werden im folgenden Abschnitt erläutert.

Transparenz: Art. 12-15 DSGVO konkretisieren Informationsplichten und Auskunftsrechte. Grundsätzlich gelten auch im Arbeitsverhältnis die allgemeinen Informationspflichten der DSGVO nach Art. 12 ff. DSGVO [33]. Pflichtinformationen in Datenschutzerklärungen sollten in deutscher Sprache, verständlich, nachvollziehbar, knapp und präzise sein [34]. Je ausführlicher über die Datenverarbeitung, deren Zwecke usw. informiert werden muss, desto unübersichtlicher wird die Informationsvermittlung für die Betroffenen. Spezifische Vorgaben macht § 26 Abs. 2 S. 4 BDSG im Rahmen der Einwilligung: Danach hat der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht in Textform aufzuklären.

Das Auskunftsrecht besteht auch im Arbeitsverhältnis [33]. Über welche Daten Auskunft zu erteilen ist, hängt von der Bestimmung des Personenbezugs ab [35]. Der BGH lehnte dabei den Vorschlag die erfassten Daten nach Signifikanz einzuschränken ab. Auch ist unerheblich, ob die Information dem Auskunftsersuchenden bereits bekannt ist [BGH, Urt. v. 15.06.2021 –VI ZR 576/19]. Allerdings kann das Auskunftsrecht im Einzelfall durch überwiegende berechtigte Interessen an der Geheimhaltung beschränkt sein [LArbG Baden-Württemberg Urt. v. 20.12.2018, 17 Sa 11/18]. Danach hat der Arbeitgeber eine auf den konkreten Umständen des Einzelfalls beruhende Güterabwägung zwischen dem arbeitgeberseitigen Geheimhaltungsinteresse einerseits und dem arbeitnehmerseitigen Auskunftsinteresse andererseits vorzunehmen.

Ausnahmen gelten bei mangelnder Identifizierbarkeit (Art. 11 DSGVO). Die Befreiung von der Pflicht zur Umsetzung der Betroffenenrechte greift nur, wenn es dem Verantwortlichen nicht mit verfügbaren Mitteln gelingt, eine Zuordnung des Antragstellenden vorzunehmen. Eine eindeutige Identifizierung erfordert nicht Klarnamen, Adresse, Geburtsdatum etc., sondern kann auf verschiedenen Wegen der Authentisierung sichergestellt werden [Weichert: [36] Art. 11 Rn. 13 ff]. Rechte und Freiheiten anderer Personen schränken ebenfalls den Auskunftsanspruch ein. Das Recht auf eine Kopie der personenbezogenen Daten kann begrenzt sein, wenn ein Bezug zu Dritten besteht, überwiegende Urheberrechte oder Geschäftsgeheimnisse berührt sind, oder die Auskunft einen unverhältnismäßigen Aufwand erzeugt (offensichtlich unbegründete oder exzessive Anfragen können abgelehnt werden) [35]. Den Verantwortlichen trifft insoweit die Beweislast einer konkreten Kollisionslage (die bloße Besorgnis der Gefährdung dieser Rechte reicht nicht). Es sollte nicht jegliche Auskunft verweigert, sondern die Mitteilung entsprechend gekürzt werden (z.B. Teilkopie, Schwärzungen, etc.) [Bäcker in: [36] Art. 15 Rn. 42a].

Zweckbindung: Dieses Prinzip besteht aus der **Zweckfestlegung** sowie der **Vereinbarkeit** mit den/dem gewählten Zwecke/n. Entsprechend des risikobasierten Ansatzes der DSGVO sollte sich auch der Konkretisierungsgrad der Zweckfestlegung am Risiko orientieren, d.h. bei geringen Risiken könnten Zwecke weiter gefasst werden als bei

risikobehafteten Verarbeitungsarten oder -kontexten [37]. Es ist durchaus möglich, mehrere Zwecke zu benennen, zu pauschal gehaltene Zweckangaben sollen hingegen nicht genügen [38]. Eine Zweckänderung erfordert nach Art. 6 Abs. 4 DSGVO die Einwilligung, eine legitimierende Rechtsvorschrift oder die Vereinbarkeit der Zwecke, welche durch den sog. **Kompatibilitätstest** nachgewiesen wird.

Datenminimierung: Dieser Grundsatz basiert auf dem Gedanken, dass die DV in Umfang und Eingriffsintensität auf das Maß begrenzt werden soll, welches für die Zweckerreichung wirklich erforderlich ist. Insgesamt sollten so wenig personenbezogene Daten wie möglich verarbeitet werden. Besondere Erwähnung findet der Grundsatz im Rahmen des Konzepts **Privacy by Design und by Default** (Art. 25 DSGVO). Ebenso Relevanz entfalten technische und organisatorische (Schutz-)Maßnahmen (TOM) bei der **Datenschutz-Folgenabschätzung** (DSFA), welche nach Art. 35 DSGVO nur bei besonders risikobehafteter DV durchzuführen ist.

Beim Privacy by Design sind wichtige Gradmesser der Stand der Technik sowie der Schutzbedarf, welcher je nach Eingriffsintensität und (Schadens-)Risiko höher oder niedriger ausfallen kann [39]. Typische TOMs sind u.a.:

- Pseudonymisierung;
- lokale Datenverarbeitung auf Endgeräten, Minimierung der Datenübermittlung an Backend-Systeme;
- Zwei-Faktor-Authentifizierung oder Multi-Faktor-Authentifizierung; gegenseitige Authentisierung der Kommunikationspartner;
- Ende-zu-Ende-, Transport- und Ablageverschlüsselung sowie Sicherung privater Schlüssel vor unberechtigtem Zugriff;
- Ganzheitliche Sicherheitsarchitektur: Bereitstellung sicherer Software-Administration, Patch-Management; Umsetzung des Need-to-Know-Prinzips;
- Aufklärung der Nutzer:innen über unterschiedlich (sichere) Konfigurationsmöglichkeiten.

Richtigkeit: Der Grundsatz umfasst eine aktive Prüfpflicht auf Korrektheit und einen Berichtigungsanspruch. [Schantz in: [25] Art. 5 Rn. 28]. Sachlich richtig ist als objektives Kriterium bei Tatsachenangaben bei Übereinstimmung der Daten mit der Realität erfüllt [Herbst in: [36] Art. 5 Rn. 60]. Die Daten müssen jedoch nicht immer auf dem neuesten Stand sein, wenn es auf den jeweiligen historischen Kontext ankommt, machen nachträgliche Änderungen der Wirklichkeit, z.B. die Namens- oder Geschlechtsanpassung, gespeicherte Daten nicht falsch [OVG Hamburg, Urt. v. 27.5.2019, Az. 5 Bf 225/18.Z]. Insofern besteht ein enger Bezug zum Verarbeitungszweck.

Speicherbegrenzung: Die DSGVO nennt in Art. 17 DSGVO Löschgründe (z.B. Entfallen des Verarbeitungszwecks, Widerruf der Einwilligung oder Widerspruch gegen die Verarbeitung) sowie Ausnahmen. Die Löschung ist **unverzüglich** durchzuführen, was eine anhand der konkreten Verarbeitung einzelfallabhängige Bestimmung erfordert [Paal in: [40] Art. 17 Rn. 31]. Eine DSGVO-Definition von Löschen oder Löschmethoden existiert nicht [Dix in: [41] Art. 17 Rn. 5]. Entscheidend ist, dass eine (Weiter-)Verarbeitung nicht mehr möglich und Daten zu diesem Zweck nicht mehr ohne übermäßigen Aufwand wiederhergestellt werden können [Paal in: [40] Art. 17 Rn. 30]. Die bloße Löschung einer Verknüpfung reicht regelmäßig nicht [Dix in: [41] Art. 17 Rn. 5]. Bei beruflicher Korrespondenz kann sich die Frage des korrekten Löschzeitpunkts herausfordernd gestalten: Individuelles Sichten und Löschen wird bei umfangreicher Korrespondenz unverhältnismäßig ausfallen [42]. Pauschales Löschen nach der längsten für das Unternehmen anwendbaren Aufbewahrungsfrist lässt dagegen eine Ausdifferenzierung der Risiken für die Betroffenen vermissen [42]. Die Einordnung in Löschstufen sollte daher als Mittelweg verfolgt werden. So wird vorgeschlagen als Löschregime zu definieren: (1) kurzfristig zu löschende Nachrichten mit besonders persönlichem Charakter (z.B. Bewerbungsunterlagen), (2) Nachrichten mit längeren Aufbewahrungszeiträumen (6-10 Jahre) und (3) alle übrigen ein- und ausgehenden Nachrichten (kontextabhängig zu löschen, orientiert an Verjährungsfristen, Projektabschlüssen, etc.) [42].

Sofern Aufbewahrungspflichten eingreifen, beschränkt sich der Verarbeitungszweck auf die Archivierung, sodass ggf. Zugriffsbeschränkungen zu erwägen sind [42]. Im Bereich der technischen Normungen kann zudem (je nach Fallgestaltung) auf die DIN 66398 sowie DIN 66399 zurück-

gegriffen werden. Baustein 60 **Löschen und Vernichten** des Standard-Datenschutzmodells bietet Hinweise zur Umsetzung.

Datensicherheit: Auch hier gilt der risikobasierte Ansatz und damit ein relatives, angemessenes Schutzniveau sicherzustellen. Art. 32 Abs. 1 DSGVO nennt nicht abschließend Umsetzungsmöglichkeiten. Die Auswahl geeigneter TOMs, insbesondere unter Berücksichtigung des (jeweils aktuellen) Stands der Technik, darf nicht eine einmalige Maßnahme bleiben, sondern sollte mittels einer transparenten Methode zum Vergleich der am Markt verfügbaren Alternativen regelmäßig wiederholt werden [43].

Pseudonymisierung: statt Klarnamen, Personal-/Telefonnummern oder individualisierte E-Mail-Adressen zu versenden, können variable IDs und Rollenbezeichnungen verwendet werden.

Verschlüsselung: In den meisten Kontexten ist bereits Standard Datenübermittlungen per Transportverschlüsselung abzusichern, hinzu kommen je nach Möglichkeit Ende-zu-Ende-Verschlüsselung sowie die verschlüsselte Ablage von Daten (insbesondere auch im Rahmen von Backups).

Authentifizierung: oftmals ist eine sichere Verifikation von Kontakten bei der Kollaboration erforderlich. Die Anforderungen hängen entscheidend davon ab, welche Risiken mit unautorisierten Zugriffen verbunden wären [44]. Bei höheren Risiken wird eine Zwei-Faktor-Authentifizierung empfohlen [45].

Schutzziele und Assume-Breach-Paradigma: die klassischen Sicherheitseigenschaften der Kryptographie sind Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit und (Nicht-) Abstreitbarkeit. Da immer wieder neue, zuvor noch unbekannte Sicherheitslücken (sog. „Zero-Day-Schwachstellen“) entdeckt werden, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) stets davon auszugehen, dass ein Produkt Schwachstellen enthält[46]. Insofern ist hervorzuheben, dass Sicherheitskonzepte eine ganzheitliche Sicherheitsarchitektur für den gesamten Produktlebenszyklus, angepasst an die jeweiligen Konfigurationsmöglichkeiten bieten sollten [43].

Überprüfung und Dokumentation: insbesondere, wenn externe Dienstleister eingebunden werden, bieten aktuelle Audits durch Dritte, Melde-Möglichkeiten für Sicherheitslücken (bspw. im Rahmen einer **Responsible Disclosure Policy** oder **Bug Bounty Programm**) sowie ein transparenter Umgang mit Meldungen und Patches eine gute Grundlage für den Nachweis eines angemessenen Sicherheitsniveaus.

Im Zusammenhang mit der Datensicherheit sei zudem die Pflicht zur Meldung von Datenschutzverstößen an die Aufsichtsbehörden sowie ggf. betroffenen Personen erwähnt **(Data Breach Notification)**[47].

Rechenschaftspflicht: Der Verantwortliche unterliegt weitreichenden Nachweispflichten. Datenverarbeitungsprozesse sind – sofern keine Ausnahme greift – in einem Verzeichnis der Verarbeitungstätigkeiten zu erfassen (Art. 30 DSGVO). Insbesondere sollten Handlungsanweisungen, Betriebsvereinbarungen mithin alle organisatorischen Maßnahmen im Zusammenhang mit der Einführung und Nutzung von Kommunikations- und Kollaborationstools dokumentiert werden.

Besonderheiten im Zusammenhang mit Arbeitnehmerdaten

In einem Unternehmen gibt es eine Reihe an Vorschriften in Bezug auf Beschäftigte zu beachten. Insofern enthält die DSGVO in Art. 88 DSGVO eine Öffnungsklausel für mitgliedstaatliche Regelungen. Deutschland hat von dieser Möglichkeit in § 26 BDSG Gebrauch gemacht, wo weitere Voraussetzungen niedergelegt sind. Die DSGVO bleibt als Rahmen weiterhin maßgeblich.

Direktionsrecht der Arbeitgeber*innen und Grundrecht auf informationelle Selbstbestimmung

Wie oben bereits festgestellt, können Betriebs- und Sachdaten in entsprechenden Sachverhalten einen Personenbezug enthalten, was dazu führen kann, dass die Tätigkeit der Beschäftigten zunehmend transparenter wird. Daraus kann ein permanenter Überwachungsdruck entstehen, der dazu geeignet sein kann, die Arbeitnehmer*innen bei

der Ausübung ihrer Tätigkeit wesentlich zu hemmen. Auf der anderen Seite besteht durch das Direktionsrecht des Arbeitgebers die Möglichkeit, die Zuweisung von Ort, Zeit und Inhalt der Arbeitsleistung zu bestimmen. Um zum einen diesem Direktionsrecht des Arbeitgebers und zum anderem dem Schutz des allgemeinen Persönlichkeitsrechts der Beschäftigten gerecht zu werden, muss es zu einer Interessenabwägung kommen, welchem Recht zu welcher Zeit der Vorrang eingeräumt wird. Die Verarbeitung von personenbezogenen Daten muss daher stets einen legitimen Zweck verfolgen, geeignet, erforderlich und angemessen sein [Zöll in: [48] § 26, Rn. 25].

Begriff des Beschäftigten

Gemäß § 26 Abs. 8 BDSG ist der Begriff des Beschäftigten weit zu verstehen und umfasst:

1. Arbeitnehmer*innen, einschließlich der Leiharbeitnehmer*innen im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmer*innen an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen EignungoderArbeitserprobung(Rehabilitand*innen),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamt*innen des Bundes, Richter*innen des Bundes, Soldat*innen sowie Zivildienstleistende.

Auch Bewerber*innen für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis bereits beendet ist, gelten als Beschäftigte.

Voraussetzung für die Verarbeitung personenbezogener Daten der Beschäftigten

Die Verarbeitung personenbezogener Daten durch den Arbeitgeber ist zulässig, soweit diese für Zwecke des Beschäftigungsverhältnisses erforderlich ist, oder die Arbeitnehmer:in wirksam eingewilligt hat. Im Folgenden werden die jeweiligen gesetzlichen Anforderungen dargestellt.

Erforderlichkeit

Personenbezogene Beschäftigtendaten dürfen nach § 26 Abs. 1 BDSG verarbeitet werden, soweit dies erforderlich ist:

- für die Entscheidung über die Begründung, die Durchführung des Beschäftigungsverhältnisses, oder die Beendigung des Beschäftigungsverhältnisses oder
- zur Ausübung oder Erfüllung der Rechte und Pflichten der Interessenvertretung der Beschäftigten, die sich ergeben aus:
  - dem Gesetz,
  - einem Tarifvertrag oder
  - einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung)
- Zur Aufdeckung von Straftaten, allerdings nur wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht der Begehung einer Straftat begründen und das schutzwürdige Interesse der/des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Inhaltlich wurde die bisherige Regelung aus der Zeit vor der DSGVO fortgeführt und erweitert, sodass die Erforderlichkeit unter **Abwägung der widerstreitenden Grundrechtspositionen** im Einzelfall zu bestimmen ist [BT-Drs 18/11325, 97]. Bei der Ausgestaltung der Datenverarbeitungsmodalitäten sind die kollidierenden Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weit-

gehend berücksichtigt [BAGE 105, 356-365]. Insbesondere sollte die Datenverarbeitung im Interesse der datengestützten Prozessoptimierung nicht zu einem unzumutbaren Überwachungsdruck der Arbeitnehmer*innen führen, bspw. weil die Datenerfassung permanent oder gar heimlich erfolgt [49]. Je tiefer der Eingriff in die Persönlichkeitssphäre der Beschäftigten ausfällt, desto gewichtiger müssen die Arbeitgeberinteressen ausfallen. Eine „totale, unbegrenzte Überwachung und Erfassung der Daten der Beschäftigten“ gilt als unzulässig [BAGE 111, 173-190].

Beispiel: Die Verarbeitung von personenbezogenen Daten der Beschäftigen, wie Adresse, Kontakt- und Bankinformationen, sind zur Erfüllung oder Durchführung des Arbeitsverhältnisses notwendig und bedarf keiner gesonderten Einwilligung. Die Rechtsgrundlage hierfür ist § 26 Abs. 1 Satz 1 BDSG.

Die Zwecksetzung im Beschäftigtenkontext ist dabei weit zu verstehen [Zöll in: [48] § 26, Rn. 22]. Art. 88 Abs. 1 DSGVO nennt beispielhaft Verarbeitungszwecke wie: Einstellung, Erfüllung des Arbeitsvertrags, Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, Management, Planung und Organisation der Arbeit, Sicherstellung von Gleichheit und Diversität am Arbeitsplatz, Gewährleistung von Gesundheit und Sicherheit am Arbeitsplatz, Schutz des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses.

Zudem enthält § 26 Abs. 3 eine Aussage zur Verarbeitung besonderer Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DSGVO, welche allerdings im vorliegenden Kontext nicht relevant sind.

Auch im Hinblick auf die Grundsätze der Datenminimierung und Speicherbegrenzung sollte stets geprüft werden, welche technischen und organisatorischen Maßnahmen in Frage kommen, um die Eingriffsintensität in die Persönlichkeitssphäre der Beschäftigten zu senken. So kann bspw. eine automatisierte Erfassung der Arbeits- und Pausenzeiten, die sekunden- oder minutengenau erfolgt, gegenüber den Arbeitgebern nur in wesentlich gröberen Zeitintervallen wie Stunden oder Tagen angezeigt werden. Bei dem Monitoring der Maschinenaktivität sollte stets auch bedacht werden, ob darüber eine externe, und damit heimliche Leistungskontrolle der an der Maschine tätigen Arbeitnehmer*innen ermöglicht wird. Hier könnten Anzeigemodalitäten entwickelt werden, über die kleinere Arbeitsunterbrechungen verschleiert werden bspw. indem Maschinenaktivität weiterhin suggeriert wird, um keinen unangemessenen Überwachungsdruck entstehen zu lassen.

Einwilligung

Die Einwilligung im Arbeitnehmerkontext ist höchst umstritten [50], [51]. Denn Art. 4 Nr. 11 DSGVO definiert die Einwilligung wie folgt:

> „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Problematisch im Beschäftigungsverhältnis, das klassischerweise durch eine Über- und Unterordnungsbeziehung bzw. Weisungsgebundenheit der Arbeitnehmer:in charakterisiert ist, wird das Merkmal der Freiwilligkeit gesehen. Folglich gingen EU-Datenschutzbehörden lange Zeit davon aus, dass eine Einwilligung im Arbeitsverhältnis schlichtweg ausgeschlossen ist [51]. Zur Auslegung der Einwilligung unterstreicht Erwägungsgrund 43 S. 1 DSGVO:

> Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, […] und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern.

Dieser schwierigen Ausgangslage versuchte der Gesetzgeber mit § 26 Abs. 2 BDSG zu begegnen. So wird bestimmt,

dass für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere folgendes zu berücksichtigen ist:

- die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie
- die Umstände, unter denen die Einwilligung erteilt worden ist.

Freiwilligkeit kann insbesondere vorliegen, wenn

- für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder
- Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der DSGVO in Textform aufzuklären.

Einbezug des Betriebsrats

Zustimmungsbedürftige Fälle

§ 87 Abs. 1 Betriebsverfassungsgesetz (BetrVG) regelt Mitbestimmungsrechte des Betriebsrats. Besonders relevant sind die Einführung von Verhaltensregeln (Nr. 1), die darauf gerichtet ist das Verhalten der Beschäftigten zu steuern oder die Ordnung des Betriebs zu gewährleisten (z.B. Code of Conducts, Richtlinien, etc.) [BAG, Beschluss vom 22.07.2008 – 1 ABR 40/07], sowie die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer:innen zu überwachen (Nr. 6). Zur Überwachung bestimmt sind technische Einrichtungen, wenn sie objektiv geeignet sind, Verhaltens- oder Leistungsinformationen der Beschäftigten zu erheben und aufzuzeichnen, wobei es auf eine subjektive Überwachungsabsicht des Arbeitgebers nicht ankommt [BAG, Beschluss vom 27.01.2004 – 1 ABR 7/03].

Kommt eine Einigung über eine Angelegenheit nach Absatz 1 nicht zustande, so entscheidet nach § 87 Abs. 2 BetrVG die Einigungsstelle. Der Spruch der Einigungsstelle ersetzt die Einigung zwischen Arbeitgeber und Betriebsrat.

Möglichkeit von Kollektivvereinbarungen

Der Betriebsrat kann als Interessenvertretung der Beschäftigten mit dem Arbeitgeber eine Betriebsvereinbarung abschließen und so eine Rechtsgrundlage schaffen (vgl. Art. 88 DSGVO, § 26 Abs. 4 BDSG).

> Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

Voraussetzung für die Verarbeitung personenbezogener Daten der Beschäftigten von Geschäftspartnern

Im Rahmen der Kollaboration sind Datenverarbeitungsprozesse zu organisieren, in denen Daten der Geschäftskontakte und deren Beschäftigten tangiert sein können. Hierzu gelten folgende Erwägungen:

Beschäftigtendatenschutz: Nach herrschender Meinung greift § 26 BDSG nur im Fall der Verarbeitung von Beschäftigtendaten durch den jeweiligen Arbeitgeber [52]. Dritte können sich dann nicht auf die Regelung berufen.

Vertrag: Explizit greift die Legitimation einer Datenverarbeitung zur Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen nur, wenn die betroffene Person selbst Vertragspartei ist [52] a.A. Taeger in: [48] Art. 6 Rn. 61]. Dies ist nicht der Fall, wenn eine Person im Namen des Unternehmens handelt.

Einwilligung: Bezüglich der Einwilligung sind insbesondere die Aspekte der Freiwilligkeit und Widerrufbarkeit zu bedenken.

Rechtliche Verpflichtung: Handelt es sich um einen Datenaustausch, der als Handels- oder Geschäftsbrief zu qualifizieren ist, müssen sowohl die Mindestangaben als auch die Aufbewahrungsfristen nach § 257 HGB, § 147 AO zu berücksichtigen [53], [54].

Interessenabwägung: Eine mögliche Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse), wobei auch Drittinteressen berücksichtigungsfähig sind [52]. Entscheidend ist:

- Vorliegen eines berechtigten Interesses
- Erforderlichkeit
- Kein Überwiegen entgegenstehender Interessen.

Besonderheiten im Zusammenhang mit der Datenübermittlung innerhalb des Konzerns

Sollen personenbezogene Daten innerhalb eines Konzerns ausgetauscht werden, bedarf es dafür ebenfalls einer Rechtsgrundlage.

Beispiel: Innerhalb eines Konzerns sollen zwischen verschiedenen unabhängigen Produktionsstandorten personenbezogene Daten von Mitarbeiter:innen ausgetauscht werden, die als Betriebsdaten erhoben wurden.

Als Rechtsgrundlage kann die Interessenabwägung in Verbindung mit Erwägungsgrund 48 herangezogen werden. Dort wird erläutert, in welchen Fällen eine Übermittlung von Daten innerhalb einer solchen Unternehmensgruppe zulässig ist:

> „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln […]."

Insoweit hat der Gesetzgeber die Notwendigkeit erkannt, innerhalb von Konzernen die Datenübermittlung auf ein berechtigtes Interesse zu stützen und dies im Erwägungsgrund konkretisiert.

Umsetzung im Unternehmen

Nachdem festgestellt wurde, in welchen Prozessen personenbezogene Daten verarbeitet werden sollen, gilt es nun diese Prozesse in die Datenschutzorganisation des Unternehmens zu integrieren.

Über das Datenschutzmanagementsystem in die Unternehmensstruktur

Jede verantwortliche Stelle hat alle Maßnahmen, die zur Erfüllung datenschutzrechtlicher Anforderungen getroffen werden in einem Datenschutzmanagement zu dokumentieren. Die Pflicht zur Dokumentation ergibt sich aus den Art. 24, 25, 32 DSGVO, sowie – sofern einschlägig – der Datenschutzfolgenabschätzung nach Art. 35 DSGVO. Diese Pflichten des Verantwortlichen können über den Einsatz eines solchen Managementsystems umgesetzt werden.

Zur Ausgestaltung werden keine Vorgaben gemacht. Es bleibt somit jedem Verantwortlichen überlassen, in welcher Form er ein solches Managementsystem betreibt.

Abhängig von der Größe, Organisationsform sowie der Datenschutzorganisation des Unternehmens, gilt es verschiedene Punkte zu beachten:

Zentrale Struktur

Bei der zentralen Datenschutzstruktur existiert eine Datenschutzorganisationseinheit, die für das Gesamtunternehmen verantwortlich ist. D.h., dass bspw. in der Unternehmenszentrale eine für den Datenschutz verantwortliche Abteilung oder Person sitzt.

Dezentrale Struktur

Bei der dezentralen Datenschutzstruktur existieren in verschiedenen Unternehmensbestandteilen selbständige für die Datenschutz verantwortliche Datenschutzorganisationseinheiten, die jeweils für den jeweiligen Unternehmensbestandteil verantwortlich sind.

Datenschutzrichtlinien- und Policys

Die Pflicht zur technischen- und organisatorischen Gewährleistung der Umsetzung der Datenschutzvorschriften, kann

auf organisatorischer Ebene durch Datenschutzrichtlinien und Policys gewährleistet werden.

In Datenschutzrichtlinien- und Policys können verbindliche Handlungsanweisungen erteilt werden, Datenverarbeitungsprozesse beschrieben werden und die Mitarbeiter über ihre Rechte aber v.a. ihre Pflichten aufzuklären.

Individual- oder Betriebsvereinbarung

Wie bereits oben festgestellt benötigt jede Verarbeitung von personenbezogenen Daten eine Rechtsgrundlage. Sofern diese nicht bereits zur Durchführung des Arbeitsverhältnisses erforderlich ist gibt es im Wesentlichen zwei Möglichkeiten: Die Individual- oder Betriebsvereinbarung.

Bei der Individualvereinbarung wird mit jedem Mitarbeiter eine Vereinbarung bzgl. Der Verarbeitung bestimmter personenbezogener Daten getroffen. Dies wird in der Regel eine datenschutzrechtliche Einwilligungserklärung sein, mit der in die jeweilige Datenverarbeitung eingewilligt wird.

Sofern es sich um die unternehmensweite oder zumindest über eine über den Einzelfall hinaus gehende Verarbeitung handelt, kann eine Betriebsvereinbarung die notwendige Rechtsgrundlage bereit stellen.

Praxistipp: Eine Betriebsvereinbarung ist je nach Regelungsgegenstand mit einer längeren Vorlaufzeit verbunden. Es bietet sich daher an, sofern diese Option in Betracht gezogen wird, diese frühzeitig in enger Abstimmung mit der Unternehmensleitung und den entsprechenden Fachverantwortlichen vorzubereiten und abzustimmen.

Einsatzoptionen

Bezüglich der Einsatzmöglichkeiten im Unternehmen, sollen vorliegend zwei Varianten behandelt werden. Die Variante eines Einsatzes eines kollaborativen transparenten Wertschöpfungsnetzwerkes nur zu Forschungszwecken oder für einen Einsatz im Realbetrieb. Ggf. soll ein Verfahren auch zunächst nur im Rahmen eines Forschungsprojektes getestet werden, um es zu einem späteren Zeitpunkt in den Realbetrieb zu überführen. Auch auf diese Besonderheiten, die im Zusammenhang mit einer Überführung aus einem (Forschungs-) Testbetrieb in einen Realbetrieb einhergehen, soll in diesem Abschnitt nachgegangen werden.

Einsatz im Realbetrieb

Der Einsatz im Realbetrieb richtet sich nach den obigen Ausführungen.

Einsatz zu Forschungszwecken

Die Verfolgung von Forschungszwecken wird in der DSGVO privilegiert.

Erfasste Forschungstätigkeiten: Die DSG-VO differenziert nicht nach Forschung durch Forschungseinrichtungen und angewandter Forschung im Unternehmenskontext (vgl. Erwägungsgrund 159 DSGVO) [55]. Im Hinblick auf die einschlägigen Rechtsgrundlagen bestehen allerdings graduelle Unterschiede, da Forschungsklauseln für öffentliche Stellen des Landes wie Hochschulen in den Landesdatenschutzgesetzen geregelt sind, welche aufgrund der Öffnungsklauseln der DSGVO und dem Subsidiaritätsgrundsatz des BDSG vorrangig anzuwenden sind. Daneben finden sich Regelungen in § 27 BDSG.

Privilegien: Im Rahmen der Einwilligung wird unter dem Begriff **Broad Consent** eine gewisse Flexibilisierung im Hinblick auf die Bestimmtheit der Einwilligung gewährt [56]. Neben der Angabe konkreter Forschungsprojekte als Verarbeitungszweck kann die Einwilligung auch auf Forschungsbereiche ausgedehnt werden [57]. Pauschaleinwilligungen bleiben dennoch unwirksam [51]. Noch unklar ist das Verhältnis zu § 26 Abs. 2 BDSG, wenn die Beschäftigten gleichzeitig Forscher:innen sind. Insofern könnten – je nach Sachverhalt im Einzelfall – gleichlaufende Interessen vorliegen.

Umstritten ist die Privilegierung im Hinblick auf die Zweckbindung, d.h. die Möglichkeiten bereits vorhandene Daten zu Forschungszwecken weiterzuverarbeiten: einige gehen bei einer Nachnutzung von Daten zu Sekundärzwecken von einer Fiktion der Zweckidentität aus [55], [58], andere fordern auch im Forschungskontext weiterhin die Durch-

führung eines Kompatibilitätstests zwischen Primär- und Sekundärzweck (vgl. Art. 6 Abs. 4 DSGVO) [59].

Auch im Hinblick auf die Speicherbegrenzung ist noch nicht abschließend geklärt, inwieweit Archivierungen zu Forschungszwecken auch übe die Erforderlichkeit im konkreten Forschungsprojekt hinausgehen darf. Die Leitlinien guter wissenschaftlicher Praxis fordern Archivierungen bis zu 10 Jahre [59].

Im Hinblick auf die Transparenzpflichten bestehen Forschungsausnahmen in den Fällen, in denen die Daten nicht bei der betroffenen Person selbst erhoben wurden und die Information unmöglich ist oder einen unverhältnismäßigen Aufwand verursachen würde (Art. 14 Abs. 4 DSGVO). Allerdings müssen dann alternative Wege zur Herstellung von Transparenz gefunden werden, bspw. die Bereitstellung der Informationen für die Öffentlichkeit [60].

Zudem können je nach Sachlage die Rechte der Betroffenen auf Auskunft, Berichtigung, Datenübertragbarkeit, Widerspruchsrecht, etc. eingeschränkt werden.

Die gewährten Privilegien werden durch die Forderung von Schutzmaßnahmen nach Art. 89 Abs. 1 DSGVO kompensiert. Zentral steht die Pflicht zur Anonymisierung im Vordergrund. Sofern dies nicht möglich ist, muss geprüft werden, ob eine Pseudonymisierung eingesetzt werden kann. Als dritten Schritt sind sonstige Schutzmaßnahmen zu prüfen.

Überführung vom Forschungs- in den Realbetrieb

Sofern in einem Forschungsprojekt die Datenverarbeitung stattgefunden hat und nunmehr in einen Realbetrieb oder in eine Betriebsphase überführt werden soll, ist regelmäßig zu prüfen, auf welche Rechtsgrundlage die Datenverarbeitung gestützt wurde. Hier kann es notwendig werden, die Rechtmäßigkeit unter neuer Zweckrichtung neu zu bewerten und Erklärungen ggf. erneut einzuholen. Sollte eine Individual oder Kollektivvereinbarung als Rechtsgrundlage genutzt worden sein, ist zu klären, inwiefern eine etwaige Zweckbindung besteht, bevor diese als Grundlage für die weitere Datenverarbeitung herangezogen werden.

Anonymisierung als Mittel der Datenminimierung

Bei jedem kollaborativen Austausch von personenbezogenen Daten ist die Frage nach der Erforderlichkeit zu stellen. Dies ergibt sich schon aus dem Datenminimierungsgrundsatz. Demnach muss jede Datenverarbeitung dem Zweck angemessen und erheblich sein und auf für die Zwecke der Verarbeitung notwendigen Maß beschränkt sein. Bereits bei der Gestaltung von technischen Systemen wie einem Kollaborationsnetzwerk, sollte die Verarbeitung personenbezogener Daten begrenzt oder ganz vermieden werden. Technische Möglichkeiten wie Anonymisierung könnten dabei helfen mit Betriebsdaten Prozesse zu optimieren ohne in Gefahr zu laufen, durch die Verarbeitung personenbezogener Daten die Rechte und Freiheiten von Mitarbeitern zu gefährden. Zudem findet bei einem Einsatz anonymer Daten das Datenschutzrecht keine Anwendbarkeit.

Da die Anonymisierung von personenbezogenen Daten selbst ein Verarbeitungsvorgang gemäß Art. 4 Nr. 2 DSGVO ist, der einer Legitimationsgrundlage bedarf, könnte im Wege einer erlaubten Zweckänderung gemäß Art. 6 Abs. 4 DSGVO eine Anonymisierung erfolgen [30].[2] Dazu muss im Einzelfall begutachtet werden, inwiefern die Weiterverarbeitung mit dem Ausgangszweck vereinbar ist. Leitlinien dazu sind auf nationaler Ebene durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aufgestellt worden [61].

Anonymitätslevel

Die DSGVO enthält keine explizite Definition der Anonymisierung. Erwägungsgrund 26 S. 5 und 6 DSGVO stellen klar, dass die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in

2 Weitere mögliche Rechtsgrundlagen sind die Einwilligung; Art. 6 Abs. 1 lit. c) i.V.m. Art. 17 Abs. 1 lit. a) DSGVO als Alternative zur Löschung oder Spezialgesetzliche Erlaubnistatbestände.

einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

Aus der empirischen Forschung sind unterschiedliche Level der Anonymität bekannt:

Formale Anonymität

Dies bezeichnet das bloße Entfernen direkt identifizierender Merkmale wie Name, Anschrift, Personalnummer etc. (Merkmale oder Merkmalskombinationen, die im Datenbestand i.d.R. einmalige Werte enthalten). Eine formale Anonymisierung ist zur Annahme von Anonymität im Rechtssinne regelmäßig nicht ausreichend, solange hierdurch die Re-Identifizierung nicht mit unverhältnismäßigem Aufwand verbunden wird. Für Bestimmbarkeit ist nicht nur die Identifizierung mit bürgerlichen Namen erforderlich, es reicht vielmehr die Individualisierung der Person [3], [5], [12], [30], [62].

Faktische Anonymität

Daten werden als faktisch anonym bezeichnet, wenn eine De-Anonymisierung zwar nicht gänzlich ausgeschlossen ist, aber nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer betroffenen Person zugeordnet werden können [62]. Dieser Abgrenzung folgt auch der gesetzliche Ansatz [61].

Absolute Anonymität

Unter absoluter Anonymisierung versteht sich die Datenveränderung derart, dass die Re-Identifizierung auch mit Zusatzwissen für Jedermann ausgeschlossen ist. Dies wird in der Realität oftmals als kaum umsetzbar bemängelt [63]. In nahezu jedem Szenario ist ein zumindest theoretisches Mittel denkbar, um eine vormalige Zuordnung zu betroffenen Personen zu rekonstruieren [2]. Daher ist die absolute Anonymität nur eine Variante neben der faktischen Anonymität, die somit den eigentlichen rechtlichen Maßstab bildet.

Anonymisierungsmethoden

Es existieren unterschiedliche Wege um die Wahrscheinlichkeit einer Deanonymisierung zu senken:

Informationsreduktion

Übliche Verfahren der Informationsreduktion liegen in der Löschung identifizierender Merkmale, Vergröberung, Aggregation oder Klassenbildung. Bei der Generalisierung werden konkrete Werte durch allgemeinere ersetzt, sodass Detailgrad und Genauigkeit verringert werden, dabei aber auch der Aussagehalt leidet [64]. Als Datensuppression werden Verfahren bezeichnet, bei denen Daten teilweise oder komplett gelöscht werden.

Ein neuer Ansatz ist die **Bucketization**: Hier werden die Daten selbst nicht verändert, aber die Beziehungen zwischen Personen, die durch Quasi-Identifikatoren identifizierbar bleiben, und den sensiblen Attributen verschleiert [65]. Die Daten werden getrennt gespeichert: einerseits die identifizierenden bzw. quasi-identifizierenden Merkmale und andererseits die sensitiven Merkmale [66].

Informationsveränderung

Die Identifizierbarkeit kann erschwert werden, indem Datenbestände randomisiert bzw. verrauscht werden, indem kontrolliert Zufallsfehler integriert werden oder mittels Data Swapping einzelne Daten vertauscht werden.

Eine Methode der Randomisierung ist die **stochastischen Überlagerung**: einzelne Attribute eines Datensatzes werden durch zufällige numerische Werte modifiziert [67]. Statistische Informationen können trotz der Hinzufügung von Rauschen (engl. **Additive Noise**) noch abgeleitet werden, wobei auch die sensitiven Daten wiederherstellbar sind, wenn die Korrelationen zwischen Attributen hoch und das Rauschen gering sind [66]. Ein anderer Ansatz ist die Vertauschung der sensiblen Attributwerte zwischen Datensätzen (engl. **Data Swapping**). Die Anonymisierung wird durch die willkürliche Verknüpfung der einzelnen Merkmalsausprägungen erreicht [66].

Je nach Anonymisierungswirkung der einzelnen Verfahren kann es erforderlich und sinnvoll sein, mehrerer Ansätze miteinander zu kombinieren [30].

(Re-)Identifizierungsrisiken

Die unterschiedlichen Anonymisierungstechniken sind unterschiedlich effektiv: typische Risiken einer Deanonymisierung liegen in [30]:

- **Herausgreifen bzw. Aussondern (singling out):** Erwägungsgrund 26 S. 3 DSGVO nennt mit dem Aussondern beispielhaft eine der Identifizierungsgefahren. Dies bezeichnet die Möglichkeit, in einem Datenbestand einige oder alle Datensätze derart zu isolieren, dass dies die Identifizierung einer Person ermöglicht.
- **Verkettbarkeit:** Verkettbarkeit oder auch Verknüpfbarkeit bezieht sich auf die Möglichkeit min. zwei Datensätze einer Person bzw. Personengruppe zu verknüpfen um bspw. Inhaltsdaten mit direkten Identifiern zu verbinden oder ein Profil zu erstellen und so die Person zu identifizieren.
- **Inferenz:** Als Inferenz wird die Möglichkeit bezeichnet, den Wert eines Merkmals mit einer signifikanten Wahrscheinlichkeit von den Werten einer Reihe anderer Merkmale abzuleiten.

Anonymitätsgarantien

Um die Belastbarkeit der Anonymisierungstechniken zu belegen, haben sich bestimmte Anonymitätsbegriffe und -Kriterien herausgebildet:

k-Anonymität

Der Begriff charakterisiert ein Prinzip, dass die Individualisierung einer Person aus einem Datenbestand erschwert. Über Generalisierung wird jedes potentiell identifizierende Merkmal mindestens k-mal im Datenbestand vorkommen, sodass über die Korrelation punktueller Merkmalswerte die Bildung von Quasi-Identifikatoren verhindert wird [68]. Zunächst müssen im betreffenden Datenbestand alle direkt identifizierbaren Merkmale natürlicher Personen entfernt werden. Darüber hinaus müssen auch quasi-identifizierbare Angaben soweit generalisiert oder maskiert werden, damit keine Unterscheidung von Betroffenen in einer Gruppe von k Personen möglich ist. k-Anonymität bietet allerdings keinen Schutz vor Inferenztechniken [30]. Ist bereits bekannt zu welcher Gruppe eine Person gehört, ist es oftmals möglich den Wert einer Eigenschaft zu ermitteln.

L-Diversität und t-Closeness

Um die Schwachstellen der k-Anonymität zu schließen, stellt das Konzept L-Diversität sicher, dass die einzelnen Merkmale jeder Äquivalenzklasse mindestens l verschiedene Werte aufweist [69]. Selbst für Angreifer mit entsprechendem Zusatzwissen soll so eine signifikante Unsicherheit bestehen bleiben [30]. Weiter verfeinert wird dieses Konzept durch den Ansatz t-Closeness: um auch probabilistische Inferenzangriffe zu erschweren werden Äquivalenzklassen gebildet, die die der ursprünglichen Verteilung der Merkmalswerte in der Tabelle ähneln [70].

Differential Privacy

Differential Privacy, entwickelt von Cynthia Dwork [71], ist der aktuelle Gold-Standard [72]. Hierbei werden Datensätze derart generalisiert oder verändert, dass die An- oder Abwesenheit einer Person im Datensatz nicht mehr vorhersagbar ist. Das Ziel dieses Ansatzes liegt darin auf der einen Seite die Genauigkeit für Datenbankabfragen zu maximieren und gleichzeitig auf der anderen Seite die Wahrscheinlichkeit einer Identifizierung von Einzelpersonen zu minimieren.

Zwischenergebnis

Anonymisierung ist ein Weg der „Flucht aus dem Datenschutz“, muss in diesem Fall allerdings ausreichend sicher Re-Identifizierungsrisiken ausschließen. Diese Risiken sollten regelmäßig re-evaluiert werden. Welche Anonymisierungsmethoden in Frage kommen, hängt entscheidend von der Form des Datenbestands ab.

Liegt hingegen eine nicht ausreichende Anonymisierung vor, kann diese nichtsdestotrotz als Schutzmaßnahme ähnlich der Pseudonymisierung Risiken für die Rechte und Freiheiten der betroffenen Personen senken und somit einen positiven Effekt auf die Durchführbarkeit eines Kollaborationsprojekts haben.

— Der Schutz von Geschäftsgeheimnissen als nichtfunktionale Anforderung für Kollaborationsnetzwerke

Neben dem Datenschutz kann auch der Schutz von Geschäftsgeheimnissen durch die Kollaboration in Wertschöpfungsnetzwerken tangiert sein.

Definition des Geschäftsgeheimnisses

Die Definition in § 2 Nr. 1 GeschGehG basiert auf den Vorgaben der Trade-Secrets-Richtlinie (EU) 2016/943, wonach es darauf ankommt, dass die Information geheim, d.h. nicht allgemein bekannt oder nicht ohne weiteres zugänglich ist, daher von kommerziellem Wert ist, sowie Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen. Abweichend von der bisherigen Rechtslage wird ein Geheimhaltungsinteresse nicht bereits vermutet, sondern es müssen **aktiv** Maßnahmen zur Geheimhaltung ergriffen werden [BT-Drs. 19/4724, 24]. Als weitere Voraussetzung nennt das GeschGehG ein berechtigtes Interesse an der Geheimhaltung. Auf inhaltlicher Ebene bestehen weder qualitative noch quantitative Anforderungen an die Information: obwohl der Schutzzweck in der Förderung der Innovation im Wettbewerb verortet wird, muss die Information keine innovative Note (wie Individualität, Neuheit, Kreativität, Originalität oder ähnliches) aufweisen [Alexander in: [77] § 2 Rn. 27].

Bezüglich der Angemessenheit von Maßnahmen gilt ein relativer Maßstab: nach dem konkreten Kontext des Einzelfalls, welcher ggf. Veränderungen unterliegt, ist nach einem objektiven Maßstab zu eruieren, was nach Informationswert, Entwicklungskosten, Natur der Information, Bedeutung für das Unternehmen, Unternehmensgröße, üblichen Geheimhaltungsmaßnahmen, Art der Informationskennzeichnung sowie vereinbarten vertraglichen Regelungen mit Beschäftigten und Geschäftspartnern sinnvoll erscheint [BT-Drs. 19/4724, 24]. Ohne Darlegung entsprechender Anstrengung, genießen die Informationen keinen rechtlichen Schutz [78].

Zur Strukturierung wird empfohlen, die Informationen nach Schutzstufen zu kategorisieren, ob es sich um (1) sog. **Kronjuwelen** handelt, deren Offenlegung existenzgefährdend wäre, (2) strategisch wichtige Informationen, bei deren Verlust ein dauerhafter wirtschaftlicher Nachteil droht und (3) sonstige schützenswerte sensible Informationen [79]–[81].

Als mögliche Maßnahmen kommen tatsächliche (räumliche) Zugangsbeschränkungen, technische und organisatorische Schutzvorkehrungen (IT-Sicherheitsmaßnahmen, interne Richtlinien / Anweisungen, Benennung von Sicherheitsverantwortlichen, Audits, Verbote bestimmter Medien) sowie rechtliche Geheimhaltungsverpflichtungen in Betracht [80], [81]. Letztere dürfen allerdings nicht pauschal auf sämtliche Informationen bezogen werden [82]. Umstritten ist, ob Informationen über rechtswidriges Verhalten oder über private Umstände mit Unternehmensbezug schutzfähig sind [80], [83], [84]. Auch wenn die eindeutige Abgrenzung oft schwierig ausfällt, wird sowohl die systematische Identifizierung als auch die Kategorisierung aufgrund der Notwendigkeit differenzierter Geheimhaltungsmaßnahmen sowie der Gefahr einer „Verwässerung“ des Geheimnisschutzes bei nachlassender Sorgfalt oder mangelnder Akzeptanz auf Seiten der Beschäftigten empfohlen [81].

Konsequenzen

Geschäftsgeheimnisse werden vor unerlaubter Erlangung, Nutzung und Offenlegung geschützt. §§ 4-5 GeschGehG definieren Handlungsverbote als auch erlaubte Handlungen (u.a. Reverse Engineering) und Ausnahmen (z.B. Whistleblower). Inhaber von Geschäftsgeheimnissen können gegenüber Rechtsverletzenden Unterlassung und Schadensersatz verlangen. Verliert das Unternehmens-Know-How hingegen bspw. wegen mangelnder Geheimhaltungsmaßnahmen seine Klassifikation als Geschäftsgeheimnis, können daraus Haftungsrisiken für die Geschäftsführung

folgen [80]. Zudem ist der Wert eines Unternehmens oftmals stark mit seinem Know-How verbunden: wurde dieses ohne notwendige Schutzmaßnahmen als Geschäftsgeheimnis deklariert, könnte dies den Unternehmenswert schmälern und bei Unternehmenstransaktionen Kaufpreisminderung, Garantiefall oder Rückabwicklung und Schadensersatzansprüche auslösen [85]. Hat sich ein Unternehmen gegenüber Geschäftskontakten zur Geheimhaltung von Drittgeheimnissen verpflichtet, haftet es für die Nichteinhaltung der Anforderungen sowie auferlegter Schutzmaßnahmen.

Parallelen zum Datenschutzrecht

Zu Überlappungen kommt es, wenn Geschäftsgeheimnisse ebenfalls über Personenbezug verfügen. Organisatorische und technische Schutzmaßnahmen erfüllen dann eine Doppelfunktion [86]. Tabelle 1 skizziert Parallelen und Unterschiede.

Fazit

Der Schutz von Daten mit Personenbezug unterliegt dem Datenschutzrecht und stellt verbindliche Vorgaben an Datenverarbeitung im Rahmen von Kollaborationsformaten. Der Schutz von Daten mit Unternehmensbezug kann im Eigeninteresse liegen, um wertvolles Know-How des Unternehmens nicht nach außen zu offenbaren. Beide Aspekte sollten bei der Konzeption einer Kollaboration in Produktionsnetzwerken von Beginn an mitbedacht werden, damit diese in der Praxis erfolgreich umsetzbar sind.

	Datenschutz	Geschäftsgeheimnisse
Sensitivitätslevel	– besondere Kategorien nach Art. 9 DSGVO – personenbezogene Daten – pseudonymisierte Daten – anonymisierte Daten	– „Kronjuwelen“ – strategisch wichtige Informationen – sonstige schützenswerte Informationen
Risiken	– Datenverarbeitung – unautorisierte Datenzugriffe	– unautorisierte Datenzugriffe
Organisation	– Leitungsebene & Durchführungsverantwortliche – Datenschutzbeauftragte:r – Betriebsrat	– Leitungsebene & Durchführungsverantwortliche – empfohlen: Ernennung Geheimnisschutzbeauftragte:r
Beispiele	– Organistaorisch: Zugangsbeschränkungen, Need-to-Know-Prinzip, Dokumentation, Training, Schulungen, Audits – Technisch: Verschlüsselung, Anonymisierung, Datentrennung, CIA-Prinzipien – Rechtlich: Geheimhaltungsvereinbarung, Meldeobliegenheiten	

Table 1 Vergleich Daten- und Geschäftsgeheimnisschutz

— Fazit und Ausblick

Die Verarbeitung von personenbezogenen Daten im Unternehmenskontext bei der Planung, Entwicklung und Umsetzung eines kollaborativen Wertschöpfungsnetzwerk der Zukunft ist möglich und bedarf der umsichtigen und vorausschauenden Planung. Wie jede andere Einführung von Verarbeitungsprozessen mit personenbezogenen Daten wird eine gewisse Vorlaufzeit und die Beteiligung zentraler Bereiche als auch der jeweiligen Fachverantwortlichen benötigt.

Daneben gilt zu bedenken, dass das Datenschutzrecht nicht der einzige Fall ist, in dem bestimmte Daten als besonders schützenswert eingestuft werden. Auch ohne Personenbezug kann die Geheimhaltung bestimmter Informationen für ein Unternehmen essentiell sein, um Geschäftsgeheimnisse zu schützen. Im Rahmen von Kollaborationen müssen Unternehmen besonders bedenken, dass rechtlicher Schutz nur bei Umsetzung angemessener Geheimhaltungsmaßnahmen gewährt wird. Kollaborationspartner:innen sollten daher ggf. auf Einhaltung bestimmter Schutzmaßnahmen verpflichtet werden, wobei sich diese anhand der Schutzbedürftigkeit orientieren sollten. Ist das Datenschutzrecht gleichzeitig einschlägig, können Schutzmaßnahmen eine Doppelfunktion erfüllen.

— Quellen

[1] I. Pahlen-Brandt, „Datenschutz braucht scharfe Instrumente Beitrag zur Diskussion um ‚personenbezogene Daten'", *DuD*, Bd. 32, Nr. 1, S. 34–40, Jan. 2008, doi: 10.1007/s11623-008-0009-8.

[2] M. Bergt, „Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag", *ZD*, S. 365, 2015.

[3] M. Karg, „Anonymität, Pseudonyme und Personenbezug revisited?", *DuD*, Bd. 39, Nr. 8, S. 520–526, Aug. 2015, doi: 10.1007/s11623-015-0463-z.

[4] S. Brink und J. Eckhardt, „Wann ist ein Datum ein personenbezogenes Datum? – Anwendungsbereich des Datenschutzrechts", *ZD*, S. 205, 2015.

[5] A. Roßnagel und P. Scholz, „Datenschutz durch Anonymität und Pseudonymität Rechtsfolgen der Verwendung anonymer und pseudonymer Daten", *MMR*, S. 721, 2000.

[6] J. Eckhardt, „Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?", *CR*, Bd. 32, Nr. 12, S. 786–790, Jan. 2016, doi: 10.9785/cr-2016-1206.

[7] I. Kartheuser und F. Gilsdorf, „EuGH: Dynamische IP-Adressen können personenbezogene Daten sein", *MMR-Aktuell*, S. 382533, 2016.

[8] M. Kring und J. Marosi, „Ein Elefant im Porzellanladen – Der EuGH zu Personenbezug und berechtigtem Interesse", *K&R*, S. 773–776, 2016.

[9] S. Jensen und F. Knoke, „EuGH-Urteil zur Personenbezogenheit dynamischer IP-Adressen: Quo vadis, deutsches Datenschutzrecht?", *ZD-Aktuell*, S. 05416, 2016.

[10] R. Weinhold, „EuGH: Dynamische IP-Adresse ist personenbezogenes Datum – Folgen der Entscheidung für die Rechtsanwendung", *ZD-Aktuell*, S. 05366, 2016.

[11] J. Kühling und M. Klar, „Anmerkung zu EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite", *ZD*, S. 27, 2017.

[12] T. Probst, „Anonymität und Pseudonymität bei biometrischen Identifikationsverfahren", in *Anonymität im Internet*, 1. Aufl., H. Bäumler und A. von Mutius, Hrsg. Braunschweig ; Wiesbaden: Vieweg, 2003, S. 179.

[13] A. Roßnagel, „Pseudonymisierung personenbezogener Daten – Ein zentrales Instrument im Datenschutz nach der DS-GVO", ZD, S. 243, 2018.

[14] M. Hansen, „Auf dem Weg zum Identitätsmanagement – von der rechtlichen Basis bis zur Realisierung", in *Anonymität im Internet*, 1. Aufl., H. Bäumler und A. von Mutius, Hrsg. Braunschweig ; Wiesbaden: Vieweg, 2003, S. 198.

[15] M. Wagner, *Datenökonomie und Selbstdatenschutz – Grenzen der Kommerzialisierung personenbezogener Daten*, Bd. 39. Carl Heymanns Verlag, 2020.

[16] N. Marnau, „Anonymisierung, Pseudonymisierung und Transparenz für Big Data: Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung", *DuD*, Bd. 40, Nr. 7, S. 428–433, Juli 2016, doi: 10.1007/s11623-016-0631-9.

[17] A. Roßnagel, „Big Data – Small Privacy?", *ZD*, Bd. 11, S. 562–567, 2013.

[18] M. Sarunski, „Big Data – Ende der Anonymität?: Fragen aus Sicht der Datenschutzaufsichtsbehörde Mecklenburg-Vorpommern", *DuD*, Bd. 40, Nr. 7, S. 424–427, Juli 2016, doi: 10.1007/s11623-016-0630-x.

[19] V. Boehme-Neßler, „Das Ende der Anonymität: Wie Big Data das Datenschutzrecht verändert", *DuD*, Bd. 40, Nr. 7, S. 419–423, Juli 2016, doi: 10.1007/s11623-016-0629-3.

[20] G. Hornung und C. Herfurth, „Datenschutz bei Big Data Rechtliche und politische Implikationen“, in *Big Data*, C. König, J. Schröder, und E. Wiegand, Hrsg. Wiesbaden: Springer Fachmedien Wiesbaden, 2018, S. 149–183. doi: 10.1007/978-3-658-20083-1_11.

[21] O. Raabe und M. Wagner, „Verantwortlicher Einsatz von Big Data: Ein Zwischenfazit zur Entwicklung von Leitplanken für die digitale Gesellschaft“, *DuD*, Bd. 40, Nr. 7, S. 434–439, Juli 2016, doi: 10.1007/s11623-016-0632-8.

[22] Internationale Arbeitsgruppe für Datenschutz in der Telekommunikation, „Arbeitspapier zu Big Data und Datenschutz“. 2014. Zugegriffen: 25. Januar 2018. [Online]. Verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Sachthemen/BerlinGroup/55_DigData.html

[23] Smart Data – Innovationen aus Daten, Fachgruppe Rechtsrahmen, „Smart Data – Smart Solutions“. Smart-Data-Begleitforschung, 2018. Zugegriffen: 1. Februar 2022. [Online]. Verfügbar unter: https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2018_06_smartdata_smart_solutions.pdf?__blob=publicationFile&v=4

[24] M. Schmidl, *IT-Recht von A – Z: Accessprovider bis Zwischenspeicherung*, 2., Vollst. überarb. Aufl. München: Beck, 2014.

[25] H. A. Wolff und S. Brink, Hrsg., *BeckOK Datenschutzrecht*, 38. Edition. München: C.H.Beck, 2021.

[26] T. Weichert, „Der Personenbezug von Kfz-Daten“, NZV, S. 507–513, 2017.

[27] Artikel-29-Datenschutzgruppe, „Stellungnahme 4/2007 zum Begriff ‚personenbezogene Daten‘ - WP 136“, Artikel-29-Datenschutzgruppe, Brüssel, Juni 2007. Zugegriffen: 31. August 2018. [Online]. Verfügbar unter: https://www.lda.bayern.de/media/wp136_de.pdf

[28] S. Balaban und M. Wagner, „Minimizing the Risks of Data Protection Infringement – Data Lifecycle Risk Assessment“:, in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, Porto, Portugal, 2017, S. 356–362. doi: 10.5220/0006358103560362.

[29] K. Brisch und F. Pieper, „Das Kriterium der ‚Bestimmbarkeit‘ bei Big Data-Analyseverfahren: Anonymisierung, Vernunft und rechtliche Absicherung bei Datenübermittlungen“, CR, Bd. 31, Nr. 11, S. 724–729, 2015, doi: 10.9785/cr-2015-1109.

[30] Artikel-29-Datenschutzgruppe, „Stellungnahme 5/2014 zu Anonymisierungstechniken – WP 216“, Brüssel, Apr. 2014. Zugegriffen: 10. November 2018. [Online]. Verfügbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

[31] E. Buchmann, „Wie kann man Privatheit messen?: Privatheitsmaße aus der Wissenschaft“, *DuD*, Bd. 39, Nr. 8, S. 510–514, Aug. 2015, doi: 10.1007/s11623-015-0461-1.

[32] N. Forgó und T. Krügel, „Der Personenbezug von Geodaten“, *MMR*, S. 17–23, 2010.

[33] F. J. Düwell und S. Brink, „Die EU-Datenschutz-Grundverordnung und der Beschäftigtendatenschutz“, *NZA*, S. 665–668, 2016.

[34] Artikel-29-Datenschutzgruppe, „Guidelines on transparency under Regulation 2016/679 - WP 260 rev.01“, Brüssel, Apr. 2018. Zugegriffen: 19. Oktober 2018. [Online]. Verfügbar unter: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[35] M. Engeler und P. Quiel, „Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht“, *NJW*, S. 2201–2206, 2019.

[36] J. Kühling und B. Buchner, *Datenschutz-Grundverordnung, BDSG Kommentar*, 3. München: C.H.BECK, 2020.

[37] M. von Grafenstein, „Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit: Zur mangelnden Differenzierung der Rechtsgüterbetroffenheit in der Datenschutzgrund-VO“, *DuD*, Bd. 39, Nr. 12, S. 789–795, Nov. 2015, doi: 10.1007/s11623-015-0520-7.

[38] N. Culik und C. Döpke, „Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen“, *ZD*, S. 226–230, 2017.

[39] European Data Protection Board, „Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0“, Brüssel, Okt. 2020.

[40] B. P. Paal und D. A. Pauly, *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*, 3. München: C.H.BECK, 2021.

[41] S. Simitis, G. Hornung, und I. Spiecker gen. Döhmann, Hrsg., *NomosKommentar Datenschutzrecht*, 1. Auflage. Nomos, 2019.

[42] E. Durmus, A. Selzer, und U. Pordesch, „Das Löschen nach der DSG-VO: Eine Diskussion der datenschutzkonformen Umsetzung bei E-Mails“, *DuD*, Bd. 43, Nr. 12, S. 786–791, Dez. 2019, doi: 10.1007/s11623-019-1206-3.

[43] Bundesverband IT-Sicherheit e.V. (TeleTrusT), *IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ technischer und organisatorischer Maßnahmen.* Berlin: TeleTrusT, 2020.

[44] O. M. Bühr, „Videokonferenzen und Datenschutz“, *K&R*, S. 221–225, 2021.

[45] DSK - Datenschutzkonferenz, „Orientierungshilfe Videokonferenzsysteme“, Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Okt. 2020.

[46] BSI, „Die Lage der IT-Sicherheit in Deutschland 2020“, Bonn, BSI-LB20/509, Sep. 2020. Zugegriffen: 30. Juli 2021. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1

[47] European Data Protection Board, „Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01“, Brüssel, WP250rev.01, Okt. 2017. Zugegriffen: 30. Juli 2021. [Online]. Verfügbar unter: https://ec.europa.eu/newsroom/article29/items/612052

[48] J. Taeger und D. Gabel, Hrsg., *DSG-VO – BDSG: Kommentar*, 3. Frankfurt am Main: Fachmedien Recht und Wirtschaft, dfv Mediengruppe, 2019.

[49] C. Brecht, A. Steinbrück, und M. Wagner, „Der Arbeitnehmer 4.0? – Automatisierte Arbeitgeberentscheidungen durch Sensorik am smarten Arbeitsplatz“, *PinG*, S. 10–15, 2018.

[50] Artikel-29-Datenschutzgruppe, „Opinion 2/2017 on data processing at work - WP 249“, Brüssel, Juni 2017. Zugegriffen: 23. März 2021. [Online]. Verfügbar unter: https://ec.europa.eu/newsroom/article29/news-overview.cfm

[51] Artikel-29-Datenschutzgruppe, „Guidelines on consent under Regulation 2016/679 - WP 259“, Brüssel, Nov. 2017. Zugegriffen: 22. August 2018. [Online]. Verfügbar unter: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[52] H. A. Wolff und T. Kosmider, „Verarbeitung der E-Mail-Adressen von Mitarbeitern von Vertragspartnern“, *ZD*, S. 13–18, 2021.

[53] J. Schrey, J. Kielkowski, und P. Gola, „Chatten für den Arbeitgeber“, *MMR*, S. 656, 2017.

[54] A. de Wolf, „Kollidierende Pflichten: zwischen Schutz von E-Mails und „Compliance” im Unternehmen“, *NZA*, S. 1206–1211, 2010.

[55] T. Weichert, „Die Forschungsprivilegierung in der DS-GVO“, ZD, S. 18–24, 2020.

[56] European Data Protection Supervisor (EDPS), „A Preliminary Opinion on data protection and scientific research“, Jan. 2020.

[57] DSK – Datenschutzkonferenz, „Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs ‚bestimmte Bereiche wissenschaftlicher Forschung‘ im Erwägungsgrund 33 der DS-GVO“, Apr. 2019.

[58] P. C. Johannes und P. Richter, „Privilegierte Verarbeitung im BDSG-E: Regeln für Archivierung, Forschung und Statistik“, *DuD*, Bd. 41, Nr. 5, S. 300–305, Mai 2017, doi: 10.1007/s11623-017-0779-y.

[59] A. Roßnagel, „Datenschutz in der Forschung“, *ZD*, S. 157–164, 2019.

[60] K. Schaar, „Anpassung von Einwilligungserklärungen für wissenschaftliche Forschungsprojekte“, *ZD*, S. 213–220, 2017.

[61] BfDI, „Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche“. 29. Juni 2020. [Online]. Verfügbar unter: https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung-DS-GVO-TKG.html;jsessionid=1F8AAD411491776E589343B60C6004B4.1_cid507

[62] O. Watteler und K. E. Kinder-Kurlanda, „Anonymisierung und sicherer Umgang mit Forschungsdaten in der empirischen Sozialforschung“, *DuD,* Bd. 39, Nr. 8, S. 515–519, Aug. 2015, doi: 10.1007/s11623-015-0462-0.

[63] N. Härting und J. Schneider, „Das Ende des Datenschutzes – es lebe die Privatsphäre“, *CR*, Bd. 31, Nr. 12, S. 819–827, 2015, doi: 10.9785/cr-2015-1213.

[64] P. Samarati und L. Sweeney, „Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression“, Technical Report, SRI International, 1998.

[65] X. Xiao und Y. Tao, „Anatomy: Simple and effective privacy preservation“, New York, 2006, S. 139–150.

[66] B. C. Fung, K. Wang, A. W.-C. Fu, und S. Y. Philip, *Introduction to privacy-preserving data publishing: Concepts and techniques*, Bd. Data Mining and Knowledge Discovery Series. Boca Raton: Chapman and Hall/CRC, 2010.

[67] M. Rosemann, „Auswirkungen von stochastischer Uberlagerung und Mikroaggregation auf die Schätzung linearer und nichtlinearer Modelle“, *Wirtschaft und Statistik*, Bd. 4, Nr. 2007, S. 417–437, 2007.

[68] L. Sweeney, „k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY“, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Bd. 10, Nr. 05, S. 557–570, Okt. 2002, doi: 10.1142/S0218488502001648.

[69] A. Machanavajjhala, D. Kifer, J. Gehrke, und M. Venkitasubramaniam, „l-diversity: Privacy beyond k-anonymity“, *ACM Transactions on Knowledge Discovery from Data (TKDD)*, Bd. 1, Nr. 1, S. 3-es, 2007.

[70] N. Li, T. Li, und S. Venkatasubramanian, „t-Closeness: Privacy Beyond k-Anonymity and l-Diversity“, in *2007 IEEE 23rd International Conference on Data Engineering*, Istanbul, Apr. 2007, S. 106–115. doi: 10.1109/ICDE.2007.367856.

[71] C. Dwork, „Differential Privacy: A Survey of Results“, in *Theory and Applications of Models of Computation*, Bd. 4978, M. Agrawal, D. Du, Z. Duan, und A. Li, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, S. 1–19. doi: 10.1007/978-3-540-79228-4_1.

[72] G. Eibl, K. Bao, P.-W. Grassal, D. Bernau, und H. Schmeck, „The influence of differential privacy on short term electric load forecasting“, *Energy Informatics*, Bd. 1, Nr. S1, S. 93, Okt. 2018, doi: 10.1186/s42162-018-0025-3.

[73] A. Kahlert, „Rechtsgestaltung mit der Methode KORA: Entwicklung von Vorschlägen für die Gesetzgebung am Beispiel der Internetwahl bei Sozialwahlen“, *DuD*, Bd. 38, Nr. 2, S. 86–92, Feb. 2014, doi: 10.1007/s11623-014-0038-4.

[74] A. Hoffmann, S. Jandt, H. Hoffmann, und J. M. Leimeister, „Integration rechtlicher Anforderungen an soziotechnische Systeme in frühe Phasen der Systementwicklung“, *GI-Edition*, Bd. 185, S. 72–76, 2011.

[75] A. Siena, J. Mylopoulos, A. Perini, und A. Susi, „From laws to requirements“, 2008, S. 6–10.

[76] P. N. Otto und A. I. Anton, „Addressing Legal Requirements in Requirements Engineering“, in *15th IEEE International Requirements Engineering Conference (RE 2007)*, Okt. 2007, S. 5–14. doi: 10.1109/RE.2007.65.

[77] H. Köhler, J. Bornkamm, und J. Feddersen, Hrsg., *Gesetz gegen den unlauteren Wettbewerb*, 39. Auflage. München: C.H. Beck, 2021.

[78] P. Gola, „Das Geschäftsgeheimnisgesetz und die Datenschutz-Grundverordnung: Parallele Regelungen mit neuen Verpflichtungen und Aufgaben für Datenschutzbeauftragte?“, *DuD*, Bd. 43, Nr. 9, S. 569–574, Sep. 2019, doi: 10.1007/s11623-019-1165-8.

[79] B. Kalbfus, „Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie“, *GRUR-Prax*, S. 391–393, 2017.

[80] M. Dann und J. W. Markgraf, „Das neue Gesetz zum Schutz von Geschäftsgeheimnissen“, *NJW*, S. 1774–1779, 2019.

[81] S. Maaßen, „‚Angemessene Geheimhaltungsmaßnahmen‘ für Geschäftsgeheimnisse“, *GRUR*, S. 352–360, 2019.

[82] LAG Düsseldorf, Bd. E-CLI:DE:LAGD:2020:0603.12SAGA4.20.00. 2020.

[83] C. Alexander, „Geheimnisschutz nach dem GeschGehGE und investigativer Journalismus“, *AfP*, S. 1–11, 2019.

[84] R. Hauck, „Grenzen des Geheimnisschutzes“, *WRP*, S. 1032–1037, 2018.

[85] A. Leister, „Haftungsgefahren beim neuen Geheimnisschutz“, *GRUR-Prax*, S. 579–581, 2020.

[86] M. Wagner, H. Tran, M. Pieper, D. Vonderau, und S. Balaban, *Daten- und Geheimnisschutz bei der Kommunikation im Unternehmenskontext*, 1.0. Karlsruhe: FZI Forschungszentrum Informatik, 2021. Zugegriffen: 4. Januar 2022. [Online]. Verfügbar unter: https://www.fzi.de/fileadmin/user_upload/2021_11_19_ThreemaFINAL.pdf