DATENSCHUTZAKTUELL

NOV 2026

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

Themenheft:
Anonym oder nicht? Prüfen Sie Daten richtig



AI GENERATED

ANONYMISIERT, PSEUDONYMISIERT, PERSONENBEZOGEN? RICHTIG EINORDNEN!

SELBSTTEST
Anonym oder pseudonymisiert? Testen Sie Ihr Wissen 3

PRÜFSCHEMA
Erfolgreich anonymisiert? So prüfen Sie Schritt für Schritt 4–5



„Anonym“ ist nicht gleich anonym

Liebe Leserin, lieber Leser,

Namen gelöscht, Personen anonym – und die Daten können frei genutzt werden? So einfach ist es leider nicht. Denn ein Datensatz kann auf den ersten Blick anonym wirken und rechtlich trotzdem personenbezogen sein. Dann gilt die Datenschutz-Grundverordnung (DSGVO) weiter – mit allen dazugehörigen Pflichten.

Die neuen Leitlinien des Europäischen Datenschutzausschusses (EDSA) schaffen mehr Klarheit. Erfahren Sie, woran Sie echte Anonymisierung erkennen und Datensätze in der Praxis richtig prüfen.

Viele Grüße



Dr. Anna-Kathrin Mauch
Rechtsanwältin und Redakteurin

Ihre Expertin für Datenschutz
Dr. Anna-Kathrin Mauch ist Rechtsanwältin und Europajuristin mit Erfahrung im Vertrags- und Datenschutzrecht. Sie bringt Datenschutz verständlich und praxisnah auf den Punkt.

Inhalt

Datenschutz kompakt
Anonymisiert – oder doch personenbezogen?
Seiten 1–2

Selbsttest
Anonym oder pseudonymisiert? Testen Sie Ihr Wissen
Seite 3

Prüfschema
Erfolgreich anonymisiert? So prüfen Sie Schritt für Schritt
Seiten 4–5

Know-how
In 7 Schritten gelingt die Anonymisierung in der Praxis
Seiten 6-7

Lösung Selbsttest
Wirklich anonym? Die Auflösung
Seite 8

Zu Ihrem Onlinebereich:
https://www.privacyxperts.de

Live-Talk:
https://t1p.de/live-talk

E-Mail-Beratung:
https://t1p.de/anna-mauch

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Michael Schrader, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Autorin:
Dr. Anna-Kathrin Mauch, Rottweil

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: KI generiert; Seite 1: Adobe Stock | contrast-werkstatt

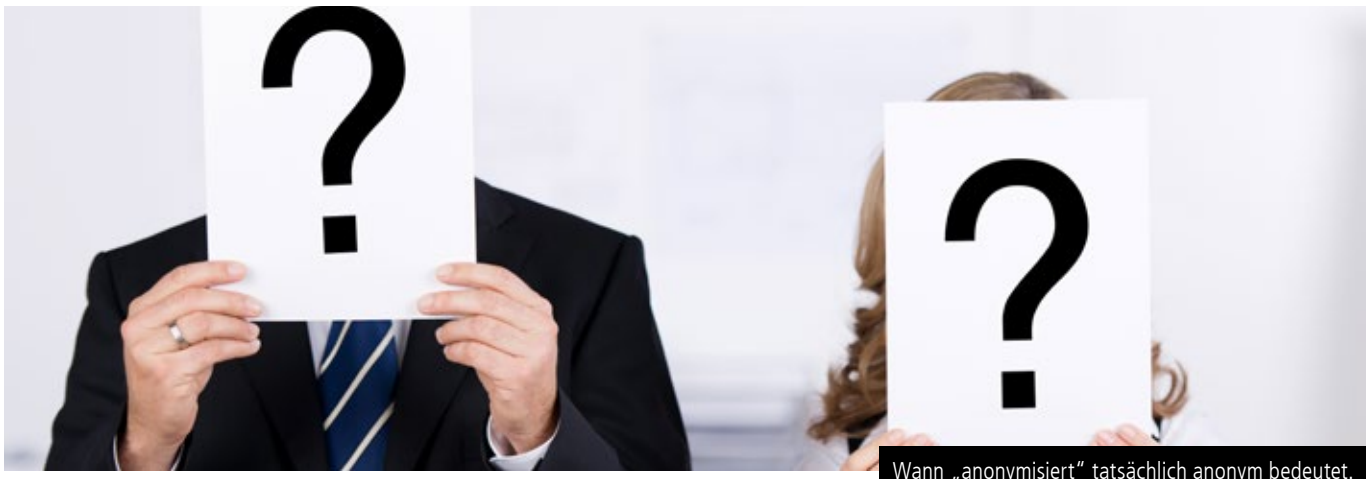
Erscheinungsweise: 36-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau



Wann „anonymisiert“ tatsächlich anonym bedeutet.

Anonymisiert – oder doch personenbezogen?

Wann sind Daten anonym und wann bleiben sie personenbezogen? Diese Frage ist wichtiger, als sie auf den ersten Blick erscheint. Denn stuft Ihr Unternehmen Daten fälschlicherweise als anonym ein, kann das Folgen haben: Wichtige Datenschutzregeln werden möglicherweise nicht mehr beachtet. Dazu gehören etwa Rechtsgrundlagen, Informationspflichten, Löschfristen und Betroffenenrechte. Die neuen Leitlinien des EDSA zeigen, worauf Sie bei der Prüfung achten müssen und wann „anonymisiert“ tatsächlich anonym bedeutet.

3 Begriffe, die Sie auseinanderhalten sollten

Wann sind Daten personenbezogen, wann pseudonymisiert – und wann wirklich anonym? Auch wenn Sie offensichtliche Identifikationsmerkmale wie Namen, E-Mail-Adressen oder Personalnummern entfernen, sind die Daten noch nicht automatisch anonym. Denn auch andere Informationen oder deren Kombination können eine Person identifizierbar machen.

1. Personenbezogene Daten

Personenbezogen sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Auch die Kombination verschiedener Informationen kann eine Identifizierung ermöglichen.

Beispiel: Eine Kundenliste enthält Namen, E-Mail-Adressen und Informationen zu den getätigten Käufen. Die Daten lassen sich den einzelnen Kunden direkt zuordnen.

2. Pseudonymisierte Daten

Bei der Pseudonymisierung werden identifizierende Merkmale beispielsweise durch Kennzeichen oder Nummern ersetzt. Lässt sich die Person mithilfe zusätzlicher Informationen wieder zuordnen, bleiben die Daten personenbezogen.

Beispiel: Das Unternehmen ersetzt die Namen seiner Kunden durch zufällige Kennnummern. Eine separat gespeicherte Liste zeigt, welche Kennnummer zu welchem Kunden gehört. Die Daten sind pseudonymisiert – die DSGVO gilt weiterhin.

3. Anonyme Daten

Bei anonymen Daten ist eine Identifizierung auch mit den vernünftigerweise zu erwartenden Mitteln nicht möglich. Die DSGVO findet auf ihre weitere Verarbeitung grundsätzlich keine Anwendung.

Beispiel: Statt einzelner Kundendaten enthält eine Auswertung nur noch die Information, dass 32 % der Kunden zwischen 40 und 49 Jahre alt sind. Lassen sich aus der Gruppe keine einzelnen Personen mehr identifizieren, handelt es sich tatsächlich um anonyme Daten.

Auf einen Blick

	Personenbezogen	Pseudonymisiert	Anonym
Identifizierung	Person ist direkt oder indirekt identifizierbar.	Zuordnung ist insbesondere mithilfe zusätzlicher Informationen möglich.	Person ist mit den vernünftigerweise zu erwartenden Mitteln nicht identifizierbar.
DSGVO	gilt	gilt	gilt für die anonymen Daten grundsätzlich nicht
Typischer Irrtum	–	„Ohne Namen sind die Daten anonym.“	„Eine Person lässt sich nur schwer identifizieren, also sind die Daten anonym.“

Das sollten Sie beachten

Pseudonymisierung und Anonymisierung sind nicht dasselbe. Lassen sich Daten mithilfe zusätzlicher Informationen oder anderer vernünftigerweise zu erwartender Mittel wieder einer Person zuordnen, sind sie nicht allein deshalb anonym, weil direkte Identifikatoren fehlen.

Neue EDSA-Leitlinien: Wann sind Daten tatsächlich anonym?

Die entscheidende Frage lautet also: Wann sind Daten so anonym, dass die DSGVO nicht mehr gilt? Genau damit beschäftigt sich der EDSA in seinen neuen Leitlinien zur Anonymisierung. Sie befinden sich derzeit noch in der öffentlichen Konsultation. Die Leitlinien sollen Unternehmen einen konkreteren Rahmen für die Frage geben, wann sie Daten tatsächlich als anonym ansehen können.

Eine wichtige Erkenntnis daraus: Schauen Sie nicht nur auf den Datensatz selbst. Entscheidend ist auch, wer die Daten verarbeitet und welche Möglichkeiten diese Stelle vernünftigerweise hat, eine Person zu identifizieren.

Damit kann die Bewertung je nach Empfänger oder beteiligter Stelle unterschiedlich ausfallen. In diese Richtung deutet auch der Entwurf des „Digital Omnibus": Die dort vorgeschlagene Änderung des Art. 4 Nr. 1 DSGVO stellt stärker darauf ab, ob die jeweilige Stelle über Mittel verfügt, mit denen sie die betroffene Person identifizieren kann.

Beispiel: Derselbe Datensatz – unterschiedliche Möglichkeiten

Ein Unternehmen erstellt einen Datensatz und ersetzt darin die Kundennamen durch zufällige Kennnummern. Die Zuordnungsliste speichert es getrennt.

Unternehmen A besitzt weiterhin die Zuordnungsliste und kann feststellen, welcher Kunde hinter welcher Kennnummer steht.

Für Unternehmen A sind die Daten nicht anonym.

Unternehmen B erhält dagegen nur den Datensatz ohne Zuordnungsliste. Hat Unternehmen B auch sonst keine vernünftigerweise zu erwartende Möglichkeit, die betroffenen Personen zu identifizieren, kann die Bewertung für Unternehmen B anders ausfallen.

Achtung: Ein Datensatz wird nicht automatisch anonym, nur weil Sie die Zuordnungsliste nicht mitübermitteln. Prüfen Sie auch, welche anderen Möglichkeiten der jeweilige Empfänger hat, die betroffenen Personen zu identifizieren.

3 Fragen entscheiden über eine erfolgreiche Anonymisierung

Für die praktische Prüfung stellt der EDSA drei Kriterien in den Mittelpunkt. Sie bieten Ihnen einen guten Ausgangspunkt, um zu beurteilen, ob Daten tatsächlich anonym sind.

1. Können einzelne Personen herausgegriffen werden?

„No Record Isolation"

Prüfen Sie zunächst, ob sich eine einzelne Person innerhalb eines Datensatzes von anderen Personen unterscheiden oder wiederholt herausgreifen lässt.

Dafür müssen Sie weder den Namen noch die konkrete Identität der Person kennen. Es kann bereits ausreichen, dass bestimmte Merkmale oder eine Kombination von Merkmalen einen Datensatz eindeutig einer Person zuordnen und diese dadurch von anderen Personen unterscheiden.

Beispiel: Eine Mitarbeiterbefragung enthält keine Namen oder Personalnummern, dafür aber Angaben zu Alter, Abteilung und Betriebszugehörigkeit. Gibt es in einer kleinen Abteilung nur eine 61-jährige Mitarbeiterin mit mehr als 30 Jahren Betriebszugehörigkeit, kann sie aufgrund dieser besonderen Merkmalskombination aus der Gruppe herausgegriffen werden.

2. Können Informationen miteinander verknüpft werden?

„No Linkage"

Prüfen Sie im nächsten Schritt, ob sich Informationen aus unterschiedlichen Datensätzen miteinander verknüpfen lassen. Entscheidend ist, ob Daten aus verschiedenen Quellen mit Sicherheit oder hoher Wahrscheinlichkeit derselben Person zugeordnet werden können.

Beispiel: Ein Unternehmen veröffentlicht die Ergebnisse einer Mitarbeiterbefragung ohne Namen oder Personalnummern. Die Daten enthalten jedoch Angaben zu Abteilung und Betriebszugehörigkeit. Ein anderer Datensatz enthält Eintrittsdatum und Abteilung der Beschäftigten. Lassen sich die Angaben aus beiden Datensätzen verknüpfen und dadurch einzelnen Beschäftigten zuordnen, ist das Kriterium „No Linkage" nicht erfüllt.

3. Lassen sich Informationen über eine Person ableiten?

„No Inference"

Auch wenn sich eine Person nicht unmittelbar identifizieren lässt, können Daten Rückschlüsse auf sie ermöglichen. Prüfen Sie deshalb, ob sich aus den vorhandenen Informationen – ggf. zusammen mit weiteren verfügbaren Informationen – spezifische und aussagekräftige Erkenntnisse über eine einzelne Person ableiten lassen.

Beispiel: Ein Datensatz enthält detaillierte Standortdaten, jedoch weder Namen noch andere unmittelbare Identifikationsmerkmale. Aus regelmäßig aufgesuchten Orten und Zeiten lässt sich dennoch beispielsweise ableiten, wo eine Person arbeitet oder welchen Gewohnheiten sie nachgeht.

Sind alle drei Kriterien erfüllt, können Sie die Daten nach dem Prüfansatz des EDSA als anonym ansehen. Ist eines der Kriterien nicht erfüllt, sind die Daten jedoch nicht automatisch personenbezogen. Prüfen Sie dann genauer, ob mit den konkret verfügbaren Mitteln eine Identifizierung der betreffenden Person vernünftigerweise zu erwarten ist.

Nicht jedes Risiko zählt

Eine Anonymisierung setzt nicht voraus, dass eine Identifizierung unter allen Umständen ausgeschlossen ist. Prüfen Sie vielmehr, ob eine Identifizierung mit vernünftigerweise zu erwartenden Mitteln möglich ist. Berücksichtigen Sie dabei insbesondere verfügbare Daten, technische Möglichkeiten, Kosten und Zeitaufwand sowie Zugriffsrechte. Dokumentieren Sie Ihre Bewertung anhand der konkreten Umstände nachvollziehbar.

Anonym oder pseudonymisiert? Testen Sie Ihr Wissen

Namen gelöscht – also anonym? Ganz so einfach ist es häufig nicht. Ob ein Datensatz noch personenbezogen ist, hängt davon ab, welche Informationen er enthält und welche Möglichkeiten bestehen, einzelne Personen zu identifizieren.

Machen Sie den Praxistest: Wie würden Sie die folgenden Fälle einordnen?

Ordnen Sie jedem Fall die aus Ihrer Sicht richtige Antwort zu:

A = anonyme Daten

B = pseudonymisierte Daten

C = personenbezogene Daten

Selbsttest

Nr.	Fallkonstellation	A	B	C
1	**Kundenliste ohne Namen:** Ein Unternehmen ersetzt in seiner Kundendatenbank Namen und Kontaktdaten durch zufällige Kundennummern. Eine separate Liste enthält die Zuordnung zwischen Kundennummer und Kunde. Nur zwei Beschäftigte haben Zugriff auf diese Liste.	○	○	○
2	**Mitarbeiterbefragung:** Bei einer Beschäftigtenbefragung werden weder Namen noch Personalnummern erhoben. Die Teilnehmer geben jedoch Alter, Geschlecht, Abteilung und Dauer der Betriebszugehörigkeit an. In einigen kleinen Abteilungen gibt es nur wenige Beschäftigte mit der jeweiligen Merkmalskombination. Die Personalabteilung kennt die Zusammensetzung der einzelnen Abteilungen und kann auf die üblichen Personaldaten der Beschäftigten zugreifen.	○	○	○
3	**Gehashte E-Mail-Adressen:** Für eine Auswertung ersetzt ein Unternehmen die E-Mail-Adressen seiner Kunden durch Hashwerte. Dabei wird für jede E-Mail-Adresse nach demselben Verfahren stets derselbe Hashwert erzeugt. Dadurch können Datensätze desselben Kunden über mehrere Auswertungen hinweg wiedererkannt und miteinander verknüpft werden. Die ursprünglichen E-Mail-Adressen werden unabhängig davon weiterhin im CRM-System des Unternehmens gespeichert.	○	○	○
4	**Umsatzstatistik nach Regionen:** Die Geschäftsleitung erhält eine Auswertung über den durchschnittlichen Jahresumsatz ihrer Kunden. Die Ergebnisse werden grundsätzlich nur für Regionen mit mindestens 5.000 Kunden zusammengefasst; einzelne Namen, Kundennummern oder Transaktionen enthält die Auswertung nicht. Auch besonders hohe oder niedrige Einzelumsätze werden nicht gesondert ausgewiesen. Aus der Statistik lässt sich daher weder erkennen, ob ein bestimmter Kunde enthalten ist, noch welchen Umsatz einzelne Kunden erzielt haben.	○	○	○
5	**Standortdaten ohne Namen.** Ein Unternehmen wertet Bewegungsdaten seiner Dienstfahrzeuge aus. Namen und Personalnummern fehlen im Datensatz. Jedes Fahrzeug besitzt jedoch eine feste Kennung. Aus dem Dienstplan lässt sich feststellen, welcher Beschäftigte das jeweilige Fahrzeug genutzt hat.	○	○	○
6	**Bewerberdaten für statistische Zwecke.** Nach Abschluss eines Bewerbungsverfahrens möchte die Personalabteilung auswerten, welche Bewerbergruppen sich im vergangenen Jahr auf offene Stellen beworben haben. Namen, Kontaktdaten, Bewerbungsunterlagen und sonstige individuelle Angaben werden gelöscht. Für die Statistik bleiben ausschließlich zusammengefasste Angaben, etwa die Gesamtzahl der Bewerbungen sowie die Verteilung auf breite Altersgruppen und Qualifikationsstufen. Gruppen mit sehr wenigen Bewerbern werden mit anderen Gruppen zusammengefasst. Eine Rückführung der statistischen Angaben auf einzelne Bewerber ist nicht mehr möglich.	○	○	○
7	**Webanalyse mit zufälliger Nutzer-ID:** Ein Analysetool speichert keine Namen oder E-Mail-Adressen. Jeder Websitebesucher erhält jedoch eine eindeutige Nutzer-ID, die bei späteren Besuchen wiedererkannt wird. So lässt sich nachvollziehen, welche Seiten derselbe Nutzer besucht und welche Aktionen er ausführt. Über längere Zeit entsteht dadurch ein individuelles Nutzungsprofil, auch wenn dem Unternehmen der Name des Besuchers nicht bekannt ist.	○	○	○
8	**Krankheitsstatistik:** Die Personalabteilung erstellt für die Geschäftsführung eine Statistik über krankheitsbedingte Fehlzeiten. Für eine Abteilung mit drei Beschäftigten weist die Statistik aus, dass ein Beschäftigter im vergangenen Jahr mehr als 50 Krankheitstage hatte. Namen enthält die Auswertung nicht.	○	○	○
9	**Datensatz für KI-Training:** Ein Unternehmen möchte frühere Kundenanfragen für das Training eines KI-Systems verwenden. Vorher entfernt es Namen, E-Mail-Adressen, Kundennummern und andere strukturierte Identifikationsmerkmale. Die eigentlichen Freitexte der Anfragen bleiben jedoch unverändert. Darin berichten Kunden teilweise über ihren Arbeitgeber, ihren Wohnort, konkrete Bestellungen oder persönliche Umstände. Einzelne Anfragen enthalten so spezifische Kombinationen von Informationen, dass sich zumindest manche Verfasser mit zusätzlichen Informationen wiedererkennen oder ermitteln lassen.	○	○	○
10	**Weitergabe an ein Forschungsinstitut:** Ein Unternehmen ersetzt Kundennamen durch zufällige Kennnummern und übermittelt den Datensatz an ein Forschungsinstitut. Die Zuordnungsliste verbleibt beim Unternehmen. Das Forschungsinstitut hat weder Zugriff darauf, noch verfügt es über andere vernünftigerweise zu erwartende Möglichkeiten, die Kunden zu identifizieren.	○	○	○

Die Auflösung mit ausführlichen Erläuterungen und Praxishinweisen finden Sie auf Seite 8.

Erfolgreich anonymisiert? So prüfen Sie Schritt für Schritt

Ein Fachbereich möchte Daten für Statistiken, zur Weitergabe oder für das Training einer KI nutzen. Die Aussage lautet: „Die Daten sind anonymisiert." Doch stimmt das? Mit dem folgenden Prüfschema lässt sich feststellen, ob das tatsächlich der Fall ist oder weiterhin ein Personenbezug besteht.

Das Ergebnis zählt – nicht nur die Methode

„Wir haben die Namen gelöscht", „Die Daten wurden gehasht" oder „Wir verwenden nur noch IDs": Solche Aussagen beschreiben zunächst nur, was mit den Daten gemacht wurde. Entscheidend ist, ob sich eine Person anhand der verbleibenden Daten und zusätzlicher Informationen noch identifizieren lässt. Berücksichtigen Sie dabei auch, wer die Daten nutzt und welche Informationen dieser Stelle zur Verfügung stehen.

Schritt 1: Welche Angaben bleiben?

Verschaffen Sie sich einen Überblick: Welche Angaben wurden entfernt oder verändert – und welche sind noch vorhanden?

Achten Sie dabei nicht nur auf Namen und Kontaktdaten. Auch scheinbar harmlose Angaben können eine Person erkennbar machen, vor allem wenn mehrere Merkmale zusammenkommen.

Prüfen Sie:	Erledigt?
Sind Namen vollständig entfernt?	○
Sind Anschriften und Kontaktdaten entfernt?	○
Sind Personal-, Kunden-, Vertrags- oder andere eindeutige Nummern entfernt oder verändert?	○
Sind Geräte-, Cookie-, Nutzer- oder andere dauerhafte IDs berücksichtigt?	○
Sind IP-Adressen und andere Onlinekennungen berücksichtigt?	○
Sind Standort-, Datums- und Zeitangaben entfernt, vergröbert oder geprüft?	○
Haben Sie Freitextfelder auf identifizierende Angaben geprüft?	○
Haben Sie seltene Merkmale, kleine Gruppen und besondere Merkmalskombinationen berücksichtigt?	○

Beispiel: Die Angabe „61 Jahre" reicht meist nicht aus, um eine Person zu erkennen. Zusammen mit „weiblich", „Rechtsabteilung" und „seit 32 Jahren beschäftigt" kann das ganz anders aussehen.

Entscheidungsregel: Namen und Kontaktdaten sind weg? Das ist nur der erste Schritt. Prüfen Sie, ob die übrigen Angaben eine Person trotzdem erkennbar machen können.

Schritt 2: Ist eine Zuordnung noch möglich?

Prüfen Sie als Nächstes, ob sich die Daten mithilfe anderer Informationen wieder einer bestimmten Person zuordnen lassen.

Gibt es z. B. eine separate Tabelle, die eine Kundennummer mit einem Namen verbindet? Dann sind die Daten regelmäßig nicht anonym, sondern pseudonymisiert. Das gilt auch, wenn nur wenige Beschäftigte auf diese Tabelle zugreifen können oder sie besonders geschützt ist.

Prüfen Sie:	Erledigt?
Gibt es keine Zuordnungsliste oder einen anderen Schlüssel?	○
Lassen sich verwendete Kennnummern keiner Person mehr zuordnen?	○
Ermöglichen andere interne Systeme keine einfache Zuordnung?	○
Besteht auch über Back-ups, Archive oder andere Datenbestände keine naheliegende Zuordnungsmöglichkeit?	○

Entscheidungsregel: Gibt es eine Zuordnungsliste oder einen vergleichbaren Schlüssel? Dann liegt regelmäßig eine Pseudonymisierung vor. Die DSGVO gilt weiterhin. Auch eine verschlüsselte oder besonders geschützte Zuordnungsliste ändert daran grundsätzlich nichts.

Schritt 3: Können Sie einzelne Personen herausgreifen?

Prüfen Sie, ob sich einzelne Personen im Datensatz unterscheiden oder über mehrere Vorgänge hinweg wiedererkennen lassen. Dabei muss der Name nicht bekannt sein.

Auch ein Merkmal oder eine Kombination von Merkmalen kann ausreichen, um einzelne Datensätze immer wieder derselben Person zuzuordnen.

Beispiel: Sämtliche Käufe von „Kunde 4711" sind über mehrere Jahre unter derselben Nummer gespeichert. Die Person bleibt damit wiedererkennbar.

Entscheidungsregel: Lässt sich eine Person herausgreifen oder wiedererkennen? Dann ist „No Record Isolation" nicht erfüllt. Das allein bedeutet aber noch nicht, dass die Daten personenbezogen sind. Prüfen Sie weiter, ob die Person tatsächlich identifiziert werden könnte.

Schritt 4: Lassen sich die Daten verknüpfen?

Schauen Sie jetzt über den einzelnen Datensatz hinaus. Gibt es weitere Informationen, die eine Zuordnung ermöglichen könnten? Denken Sie dabei an eigene Datenbestände, öffentlich verfügbare Informationen und – bei einer Weitergabe – an Daten, über die der Empfänger verfügt.

Prüfen Sie:	Erledigt?
Enthält der Datensatz keine Merkmale, die sich leicht in anderen Datenbeständen wiederfinden lassen?	○
Ermöglichen interne Kunden-, Personal- oder Vertragsdaten keine Zuordnung?	○
Ermöglichen öffentlich verfügbare Informationen keine naheliegende Zuordnung?	○
Kann der Empfänger die Angaben nicht mit eigenen Datenbeständen abgleichen?	○
Ermöglichen auch seltene Merkmalskombinationen sowie Zeit-, Orts- oder Verhaltensdaten keine Zuordnung?	○

Beispiel: Lassen sich Angaben aus einer Mitarbeiterbefragung mit anderen internen Daten verknüpfen und dadurch Beschäftigte erkennen, besteht weiterhin ein Identifizierungsrisiko.

Entscheidungsregel: Lassen sich die Angaben mit anderen Daten verknüpfen? Dann ist „No Linkage" nicht erfüllt. Prüfen Sie nun, ob die verfügbaren Zusatzinformationen tatsächlich zur Identifizierung einer Person führen könnten.

Schritt 5: Welche Rückschlüsse sind möglich?

Eine Person muss nicht unbedingt namentlich bekannt sein. Auch Daten, aus denen sich gezielt Informationen über eine einzelne Person ableiten lassen, können problematisch sein.

Fragen Sie deshalb: Welche Aussagen lassen sich über eine bestimmte Person treffen, wenn Sie die vorhandenen Angaben miteinander kombinieren?

Prüfen Sie:	Erledigt?
Lassen sich keine individuellen Verhaltensprofile bilden?	○
Lassen Bewegungs- oder Standortdaten keine Rückschlüsse auf einzelne Personen zu?	○
Verraten Kauf-, Nutzungs- oder Kommunikationsmuster keine individuellen Eigenschaften, Interessen oder Gewohnheiten?	○
Lassen sich auch aus mehreren Merkmalen zusammen keine zuverlässigen Rückschlüsse auf eine einzelne Person ziehen?	○

Entscheidungsregel: Lassen sich gezielt Informationen über eine einzelne Person ableiten? Dann ist „No Inference" nicht erfüllt. Prüfen Sie anschließend, ob dadurch unter den konkreten Umständen weiterhin ein Personenbezug besteht. Praxistipp: Fragen Sie nicht nur: „Können wir herausfinden, wer diese Person ist?" Fragen Sie auch: „Was können wir über diese Person herausfinden, obwohl wir ihren Namen nicht kennen?"

Schritt 6: Wer nutzt die Daten?

Jetzt kommt es auf die Perspektive an. Prüfen Sie, wer den Datensatz tatsächlich nutzt oder erhält und welche zusätzlichen Daten, Zugriffsrechte, technischen Möglichkeiten und Kenntnisse dieser Stelle zur Verfügung stehen. Berücksichtigen Sie auch, ob ein realistisches Interesse an einer Identifizierung besteht.

Das ist vor allem bei einer Weitergabe wichtig: Ihr Unternehmen verfügt möglicherweise über Informationen zur Zuordnung, auf die ein externer Empfänger keinen Zugriff hat.

Entscheidungsregel: Die Daten gehen an einen Dritten? Dann wechseln Sie die Perspektive. Derselbe Datensatz kann für Ihr Unternehmen anders zu beurteilen sein als für den Empfänger.

Schritt 7: Wäre eine Identifizierung realistisch?

Nicht jede theoretisch denkbare Möglichkeit verhindert eine Anonymisierung. Entscheidend ist, ob jemand die vorhandenen Möglichkeiten vernünftigerweise tatsächlich nutzen könnte. Fragen Sie deshalb: Wie aufwendig wäre es, die Person zu identifizieren – und gibt es einen realistischen Grund, diesen Aufwand zu betreiben?

Betrachten Sie den Aufwand nicht isoliert. Bei besonders wertvollen Daten kann auch ein hoher technischer Aufwand weniger ins Gewicht fallen.

Prüfen Sie:	Erledigt?
Würde eine Identifizierung sehr viel Zeit erfordern?	○
Fehlen die dafür notwendigen technischen Mittel?	○
Wären die Kosten im Verhältnis zum möglichen Nutzen sehr hoch?	○
Sind notwendige zusätzliche Informationen nicht zugänglich?	○
Fehlt ein realistischer Anlass oder Anreiz für eine Identifizierung?	○
Haben Sie absehbare technische Entwicklungen berücksichtigt?	○

Entscheidungsregel: Die Identifizierung ist nur theoretisch denkbar? Das allein schließt eine Anonymisierung nicht aus. Wäre sie dagegen mit realistisch verfügbarem Aufwand und vorhandenen Mitteln möglich? Dann spricht das gegen eine wirksame Anonymisierung.

Schritt 8: Zu welchem Ergebnis kommen Sie?

Am Ende müssen Sie die Ergebnisse zusammenführen. Ordnen Sie den Datensatz ein und halten Sie kurz fest, warum Sie zu dieser Einschätzung gekommen sind.

A: Die Daten sind anonym

Eine Person lässt sich mit den vernünftigerweise zu erwartenden Mitteln nicht identifizieren. Auch das Herausgreifen, Verknüpfen oder Ableiten von Informationen führt unter den konkreten Umständen nicht zu einer Identifizierung.

Die DSGVO gilt für den anonymen Datensatz grundsätzlich nicht.

B: Die Daten sind pseudonymisiert

Die Person ist im Datensatz nicht unmittelbar erkennbar. Mithilfe zusätzlicher Informationen – etwa einer Zuordnungsliste – lässt sich der Personenbezug aber wiederherstellen.

Die DSGVO gilt weiterhin.

C: Die Daten sind weiterhin personenbezogen

Eine Person lässt sich anhand der enthaltenen Angaben, durch die Kombination mehrerer Merkmale oder mithilfe anderer verfügbarer Informationen identifizieren.

Behandeln Sie den Datensatz weiterhin als personenbezogen.

In 7 Schritten gelingt die Anonymisierung in der Praxis

Namen löschen, Werte zusammenfassen oder Identifikatoren durch andere Zeichenfolgen ersetzen: Es gibt viele Möglichkeiten, den Personenbezug eines Datensatzes zu reduzieren. Doch nicht jede Maßnahme führt automatisch zu anonymen Daten.

Vom personenbezogenen zum anonymen Datensatz

Können Sie einzelne Personen noch identifizieren, herausgreifen oder Informationen über sie ableiten, stellt sich die Frage: Was müssen Sie verändern, um den Datensatz wirksam zu anonymisieren?

Die eine richtige Methode gibt es nicht. Häufig müssen Sie mehrere Maßnahmen kombinieren und anschließend erneut prüfen, ob eine Identifizierung mit vernünftigerweise zu erwartenden Mitteln noch möglich ist.

Schritt 1: Direkte Identifikatoren entfernen

Entfernen Sie zunächst Informationen, anhand derer eine Person unmittelbar erkennbar ist, etwa:

- Name,
- Anschrift,
- E-Mail-Adresse,
- Telefonnummer,
- Personal- oder Kundennummer sowie
- andere unmittelbar zuordenbare Kennzeichen.

Das ist häufig der erste Schritt zur Anonymisierung – allein reicht er aber meist nicht aus.

Beispiel: Mitarbeiterbefragung

Ein Unternehmen entfernt aus einer Mitarbeiterbefragung Namen und Personalnummern. Im Datensatz bleibt:

„weiblich – 61 Jahre – Rechtsabteilung – 32 Jahre Betriebszugehörigkeit"

Trifft diese Kombination nur auf eine Person zu, kann sie weiterhin erkennbar sein.

Merke: Fragen Sie nicht nur: „Sind die Namen weg?", sondern: „Was verraten die verbleibenden Informationen über einzelne Personen?"

Schritt 2: Zu genaue Angaben vergröbern

Problematische Informationen müssen Sie nicht immer vollständig löschen. Häufig können Sie ihren Wert für die Auswertung erhalten und zugleich das Identifizierungsrisiko reduzieren, indem Sie Angaben generalisieren.

Aus genauen Werten werden beispielsweise größere Kategorien:

61 Jahre – 60 bis 69 Jahre

53113 Bonn – Bonn

14.03.2026, 10:43 Uhr – März 2026

Rechtsabteilung – Verwaltung

32 Jahre Betriebszugehörigkeit – mehr als 20 Jahre

Aus „weiblich – 61 Jahre – Rechtsabteilung – 32 Jahre Betriebszugehörigkeit" könnte so „weiblich – 60 bis 69 Jahre – Verwaltung – mehr als 20 Jahre Betriebszugehörigkeit" werden.

Ob das ausreicht, hängt vom Unternehmen und den übrigen verfügbaren Informationen ab. Gibt es auch in der größeren Gruppe nur eine Person mit dieser Merkmalskombination, müssen Sie Angaben weiter vergröbern oder Merkmale entfernen.

Praxistipp: Gehen Sie schrittweise vor. Vergröbern Sie Informationen nur so weit wie nötig und prüfen Sie nach jeder Veränderung, ob der Datensatz für den vorgesehenen Zweck noch aussagekräftig genug ist.

Schritt 3: Kleine Gruppen vermeiden

Auch zusammengefasste Auswertungen ohne Einzeldaten können bei kleinen Gruppen Rückschlüsse auf einzelne Personen ermöglichen.

Problematisch wäre etwa:

„In der dreiköpfigen Geschäftsleitung war eine Person im vergangenen Jahr an 73 Tagen arbeitsunfähig."

Wissen andere, dass zwei Mitglieder kaum gefehlt haben, kann die dritte Person erkennbar werden. Bilden Sie deshalb ausreichend große Gruppen. Statt Ergebnisse für kleine Abteilungen auszugeben, können Sie etwa mehrere Abteilungen zu einem Unternehmensbereich zusammenfassen.

Legen Sie für regelmäßige Auswertungen möglichst feste Mindestgruppengrößen fest. Als Ausgangspunkt können Sie Ergebnisse beispielsweise erst ab fünf Personen ausweisen. Bei besonders sensiblen Daten oder leicht unterscheidbaren Personen kann eine größere Gruppe erforderlich sein.

Wichtig: Eine bestimmte Gruppengröße garantiert keine Anonymität. Prüfen Sie zusätzlich, ob seltene Merkmale, Extremwerte oder besondere Merkmalskombinationen einzelne Personen erkennbar machen.

Schritt 4: Dauerhafte Kennungen kritisch prüfen

Eine Kennnummer statt eines Namens kann das Datenschutzrisiko reduzieren, führt aber nicht automatisch zur Anonymisierung.

Aus „Sabine Müller" wird beispielsweise „Person 84721".

Existiert eine getrennte Tabelle, aus der hervorgeht, wer hinter „Person 84721" steht, handelt es sich regelmäßig um eine Pseudonymisierung. Die Zuordnung bleibt möglich und die Daten personenbezogen.

Das gilt auch, wenn die Zuordnungstabelle verschlüsselt oder besonders geschützt ist oder nur wenige Beschäftigte darauf zugreifen können.

Auch ohne Zuordnungstabelle können dauerhafte Kennungen problematisch sein. Wird dieselbe Person über längere Zeit immer als „Person 84721" bezeichnet, lassen sich ihre Aktivitäten verbinden und ihr Verhalten verfolgen.

Fragen Sie deshalb:

- Kann die Kennung einer konkreten Person zugeordnet werden?
- Können mehrere Datensätze mit derselben Kennung verbunden werden?
- Kann eine Person dauerhaft wiedererkannt und herausgegriffen werden?

Ist dies der Fall, sind weitere Maßnahmen erforderlich.

Schritt 5: Hashing nicht mit Anonymisierung verwechseln

Ähnliches gilt für Hashwerte. Beim Hashing wird ein Ausgangswert wie eine E-Mail-Adresse in eine andere Zeichenfolge umgewandelt:

anna.beispiel@unternehmen.de – 7e4a9...

Die ursprüngliche E-Mail-Adresse ist nicht mehr unmittelbar erkennbar. Das bedeutet aber nicht, dass der Hashwert anonym ist.

Erzeugt dieselbe E-Mail-Adresse immer denselben Hashwert, können Vorgänge derselben Person miteinander verknüpft werden. Bekannte oder vorhersehbare Ausgangswerte können außerdem selbst gehasht und mit vorhandenen Hashwerten verglichen werden.

Besitzt das Unternehmen die ursprünglichen E-Mail-Adressen weiterhin, können zusätzliche Zuordnungsmöglichkeiten bestehen.

Prüfen Sie deshalb insbesondere:

- Welche Daten werden gehasht?
- Welches Verfahren wird eingesetzt?
- Können gleiche Ausgangswerte wiedererkannt werden?
- Sind die ursprünglichen Daten noch vorhanden?

Die Aussage „Die Daten sind gehasht" beantwortet die Frage nach der Anonymität noch nicht.

Schritt 6: Freitexte gesondert behandeln

Eine häufig unterschätzte Schwachstelle sind Freitextfelder. Strukturierte Angaben wie Name, Anschrift oder Kundennummer lassen sich gezielt entfernen oder vergröbern.

In Freitexten können identifizierende Informationen dagegen an vielen Stellen auftauchen.

Das betrifft etwa Kundenanfragen, Beschwerden, Support-Tickets, Bewerbungsunterlagen, Gesprächsnotizen, Kommentarfelder sowie interne E-Mails und Dokumente.

Ein Unternehmen entfernt beispielsweise Name und E-Mail-Adresse aus einer Kundenbeschwerde. Im Text steht weiterhin:

„Ich wohne seit 25 Jahren direkt über Ihrer Filiale in der Musterstraße und habe dort am vergangenen Dienstag mit Ihrem Filialleiter Herrn X gesprochen."

Trotz fehlenden Namens können diese Angaben eine Identifizierung ermöglichen.

Besonders wichtig bei KI-Projekten: Möchte Ihr Unternehmen Kundenanfragen, E-Mails oder Support-Tickets für das Training oder Testen eines KI-Systems nutzen, prüfen Sie nicht nur standardisierte Datenfelder. Nehmen Sie auch Freitexte und andere unstrukturierte Inhalte in den Blick. Auch dort können Informationen stehen, die Personen identifizierbar machen.

Schritt 7: Maßnahmen kombinieren

In der Praxis führt häufig erst die Kombination mehrerer Maßnahmen zu einem ausreichend anonymisierten Datensatz. Nehmen wir noch einmal die Mitarbeiterbefragung:

Ausgangsdatensatz: *„Anna Beispiel – 61 Jahre – weiblich – Rechtsabteilung – 32 Jahre Betriebszugehörigkeit"*

1. Direkte Identifikatoren entfernen

„61 Jahre – weiblich – Rechtsabteilung – 32 Jahre Betriebszugehörigkeit"

Der Name ist entfernt. Die besondere Merkmalskombination kann die Person weiterhin erkennbar machen.

2. Angaben generalisieren

„60 bis 69 Jahre – weiblich – Verwaltung – mehr als 20 Jahre Betriebszugehörigkeit"

Die Identifizierung wird schwieriger. In einer kleinen Belegschaft kann die Kombination dennoch eindeutig sein.

3. Merkmale weiter reduzieren

„60 bis 69 Jahre – Verwaltung"

Der Datensatz enthält deutlich weniger Informationen über die Person.

4. Nur noch aggregiert auswerten

„18 % der Beschäftigten im Bereich Verwaltung sind zwischen 60 und 69 Jahre alt."

Lassen sich unter Berücksichtigung der Gruppengröße und anderer verfügbarer Informationen keine einzelnen Beschäftigten mehr herausgreifen oder identifizieren, kann die Auswertung sein.

Das Beispiel zeigt: Anonymisierung ist häufig kein einzelner technischer Vorgang, sondern ein schrittweiser Prozess.

Nach der Veränderung: Prüfen Sie erneut

Prüfen Sie nach den vorgenommenen Änderungen erneut, ob einzelne Personen noch identifizierbar sind. Berücksichtigen Sie dabei auch mögliche Zusatzinformationen und Verknüpfungsmöglichkeiten. Erst das Ergebnis dieser erneuten Prüfung entscheidet darüber, ob die vorgenommenen Maßnahmen tatsächlich zu anonymen Daten geführt haben.

Wirklich anonym? Die Auflösung

Wie viele Fälle haben Sie richtig eingeordnet? Gerade das Entfernen von Namen oder anderen eindeutigen Merkmalen führt nicht automatisch zu anonymen Daten. Die folgenden Lösungen zeigen, worauf es bei der Einordnung ankommt.

1. Kundenliste ohne Namen

Lösung: B – pseudonymisierte Daten

Über die separate Zuordnungsliste kann das Unternehmen weiterhin feststellen, welche Person hinter welcher Kundennummer steht. Die eingeschränkten Zugriffsrechte schützen die Daten zusätzlich, machen sie aber nicht anonym. Praxistipp: Solange eine Zuordnung möglich bleibt, gilt die DSGVO weiterhin.

2. Mitarbeiterbefragung

Lösung: C – personenbezogene Daten

Auch ohne Namen können Alter, Geschlecht, Abteilung und Betriebszugehörigkeit einzelne Beschäftigte erkennbar machen. Das gilt besonders für kleine Abteilungen und seltene Merkmalskombinationen. Praxistipp: Fassen Sie Angaben beispielsweise in Altersgruppen oder größeren Unternehmensbereichen zusammen.

3. Gehashte E-Mail-Adressen

Lösung: B – pseudonymisierte Daten

Das Hashing macht die Daten nicht automatisch anonym. Das Unternehmen besitzt die ursprünglichen E-Mail-Adressen weiterhin und kann gleiche Hashwerte zudem wiedererkennen und miteinander verknüpfen. Achten Sie darauf: Prüfen Sie bei Hashing immer das konkrete Verfahren und die vorhandenen Zuordnungsmöglichkeiten.

4. Umsatzstatistik nach Regionen

Lösung: A – anonyme Daten

Die Statistik fasst die Ergebnisse für mindestens 5.000 Kunden zusammen. Einzelne Kunden oder Transaktionen lassen sich daraus nach dem beschriebenen Sachverhalt nicht erkennen. Praxistipp: Prüfen Sie bei Statistiken neben der Gruppengröße auch seltene Merkmale und Extremwerte.

5. Standortdaten ohne Namen

Lösung: C – personenbezogene Daten

Über die feste Fahrzeugkennung und den Dienstplan kann das Unternehmen die Bewegungsdaten einem Beschäftigten zuordnen. Dass der Name im eigentlichen Datensatz fehlt, ändert daran nichts. Merke: Beziehen Sie bei der Prüfung auch andere interne Datenbestände ein.

6. Bewerberdaten für statistische Zwecke

Lösung: A – anonyme Daten

Nach dem Entfernen der identifizierenden Informationen bleiben nur zusammengefasste Angaben zu Bewerberzahlen, Altersgruppen und Qualifikationen. Eine Zuordnung zu einzelnen Bewerbern ist laut Sachverhalt nicht mehr möglich. Achten Sie darauf: Bei kleinen Bewerberzahlen können ungewöhnliche Merkmale trotzdem einzelne Personen erkennbar machen.

7. Webanalyse mit zufälliger Nutzer-ID

Lösung: C – personenbezogene Daten

Die dauerhafte Nutzer-ID ermöglicht es, denselben Besucher wiederzuerkennen und sein Verhalten über mehrere Besuche hinweg zu verfolgen. Dafür muss sein Name nicht bekannt sein. Praxistipp: Prüfen Sie bei Trackingdaten insbesondere dauerhafte Nutzer-, Cookie- und Gerätekennungen.

8. Krankheitsstatistik

Lösung: C – personenbezogene Daten

Bei nur drei Beschäftigten kann die Angabe von mehr als 50 Krankheitstagen Rückschlüsse auf eine bestimmte Person zulassen. Das gilt besonders, wenn die anderen Beschäftigten die Fehlzeiten ihrer Kollegen ungefähr kennen. Achten Sie darauf: Als Datenschutzbeauftragter sollten Sie gerade bei sensiblen Informationen auf ausreichend große Gruppen achten.

9. Datensatz für KI-Training

Lösung: C – personenbezogene Daten

Namen und Kontaktdaten wurden zwar entfernt. In den unveränderten Kundenanfragen können aber weiterhin Arbeitgeber, Wohnorte, Bestellungen oder persönliche Umstände stehen, die eine Person erkennbar machen. Praxistipp: Prüfen Sie bei KI-Trainingsdaten auch Freitexte, Anhänge und andere unstrukturierte Inhalte.

10. Weitergabe an ein Forschungsinstitut

Lösung: A – anonyme Daten für das Forschungsinstitut

Das Unternehmen besitzt die Zuordnungsliste weiterhin. Für das Unternehmen selbst bleiben die Daten daher personenbezogen. Das Forschungsinstitut hat dagegen weder Zugriff auf die Liste noch andere vernünftigerweise zu erwartende Möglichkeiten, die Kunden zu identifizieren. Für das Institut sind die Daten nach dem beschriebenen Sachverhalt daher anonym. Achten Sie darauf: Derselbe Datensatz kann je nach beteiligter Stelle unterschiedlich einzuordnen sein.

Wichtig: „Anonymisiert" sollte immer das Ergebnis Ihrer Prüfung sein – und nicht nur die Bezeichnung eines Datensatzes.

Datenschutz aktuell Live Talk: Gratis-Webinar



Austausch, Aktualität, fachliche Tiefe für alle mit Aufgaben im Datenschutz

am letzten Freitag jeden Monats

um 16:30 Uhr 60 Minuten

Moderator & Fachexperte
Andreas Würtz

Warum am Live Talk teilnehmen?

Neue Leitlinien, geplante Gesetzesänderungen, behördliche Anforderungen und praxisnahe Umsetzungsfragen stellen Datenschutzverantwortliche regelmäßig vor neue Herausforderungen. Oft bleiben dabei konkrete Fragen offen – oder es fehlt die Gelegenheit, Themen direkt mit einem Experten zu besprechen.

Der **Datenschutz aktuell Live Talk** ist aufgrund seines digitalen Formats bequem von überall erreichbar. Im Mittelpunkt steht ein **vertraulicher, fachlicher Austausch** zu aktuellen Schwerpunktthemen aus Datenschutzrecht und Datenschutzpraxis.

Die Veranstaltung wird **nicht aufgezeichnet.** So entsteht ein geschützter Rahmen, in dem auch sensible Fragestellungen offen angesprochen werden können. Sie entscheiden selbst, wie aktiv Sie teilnehmen möchten: **Bringen Sie Ihre Fragen ein oder hören Sie einfach zu** – ganz nach Ihrem Bedarf und ganz wie Sie mögen.

Der Live Talk ist bewusst kein klassisches Webinar mit Frontalvortrag, sondern ein dialogorientiertes Format, das auf Austausch, Aktualität und fachliche Tiefe setzt.

Ich freue mich auf Ihre Teilnahme!

Ihr Moderator & Fachexperte Andreas Würtz
Rechtsanwalt | Datenschutzexperte
Chefredakteur des Fachratgebers „Datenschutz aktuell“

Jetzt zum nächsten Live-Talk anmelden:

t1p.de/live-talk



Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn