von Rechtsanwalt **Phil Salewski**

Alte Grundsätze und neue Rechtmäßigkeitsvoraussetzungen – Teil 3 der Serie zur neuen DSGVO

Der dritte Teil der neuen Serie der IT-Recht Kanzlei zur EU-Datenschutzgrundverordnung (DSGVO) skizziert zunächst rechtsvergleichend die datenschutzrechtlichen Grundprinzipien, an denen sich jeglicher Umgang mit personenbezogenen Daten zu orientieren hat, und geht in einem zweiten Schritt auf die neu gefassten Anforderungen für rechtmäßige Datenverarbeitungsprozesse ein. Welche Prämissen liegen dem neuen EU-Datenschutzrecht zugrunde? Existieren neue Anforderungen für die datenschutzrechtliche Einwilligung und für deren Ausgestaltung? Inwiefern wird der Katalog bislang geltender gesetzlicher Erlaubnistatbestände modifiziert? Mehr zu diesen und weiteren Fragen lesen Sie im folgenden Beitrag.

I. Unveränderte Datenschutzgrundsätze

Die DSGVO stellt in Artikel 5 allgemeine Grundsätze für den Umgang mit erhobenen personenbezogenen Daten auf, die weitestgehend an die in Deutschland bereits vorherrschenden Leitlinien für die Datenverarbeitung angelehnt sind und somit keine bedeutenden Änderungen mit sich bringen, im Online-Handel aber dennoch uneingeschränkte Beachtung finden müssen.

1.) Verarbeitungsverbot mit Erlaubnisvorbehalt

Dem geltenden deutschen Datenschutzrecht liegt ebenso wie der DSGVO die Maxime des Erlaubnisvorbehalts zugrunde, nach welchem sämtliche Datenerhebungs- und Verarbeitungsvorgänge verboten und nur ausnahmsweise dann zulässig sind, wenn der Betroffene dies ausdrücklich gestattet oder eine gesetzliche Legitimation zugunsten des Verantwortlichen eingreift.

Erfolgt eine Prozessierung personenbezogener Daten ohne privatautonome oder gesetzliche Berechtigung, gestaltet sich der Vorgang nach deutschem und europäischen Leitbild gleichermaßen als rechtswidrig (vgl. §4 Abs. 1 BDSG, 6 DSGVO).

2.) Datensparsamkeit und enge Zweckbindung

Die nach §§ 3 und 4 BDSG maßgeblichen Prinzipien der Datensparsamkeit und zweckgebundenen Verarbeitung spiegeln sich in Art. 5 Abs. 1 lit. b und c wieder. Danach muss die Datenerhebung zum einen auf das für die Erfüllung ihres Zwecks erforderliche Maß derart begrenzt sein, dass nicht mehr Daten erhoben werden dürfen als zwingend benötigt.

Dies ist, soweit mit dem Erhebungszweck vereinbar und zumutbar, gemäß Erwägungsgrund 78 durch eine bestmögliche Pseudonymisierung zu erreichen.

Dem Grundsatz der Datensparsamkeit dient auch das in Art. 5 Abs. 1 lit. e formulierte Prinzip der Speicherbegrenzung, welches dem Verantwortlichen die Einhaltung einer am Verarbeitungszweck bemessenen Speicherdauer abverlangt und ihn zur Löschung verpflichtet, sofern der Zweck erreicht ist (so momentan auch §20 Abs. 2 Nr. 2 BDSG).

Das Prinzip der Speicherbegrenzung ist im Online-Handel vor allem bei der Datennutzung zur Abwicklung von Verträgen zu berücksichtigen und verpflichtet zur Löschung nach gegenseitiger Erfüllung und Ablauf der Widerrufsfrist.

Gleichzeitig ergeht aus der genannten Bestimmung der Grundsatz, dass Daten nur für festgelegte und mithin genau eingegrenzte, legitime und eindeutige Zwecke erhoben werden dürfen. Eine Weiteverarbeitung über den vereinbarten Zweck hinaus sowie eine einseitige Umwidmung des Erhebungs- und Nutzungszwecks mit dem Ziel, die Daten auch anderweitig zu verwenden, sind grundsätzlich untersagt.

3.) Datensicherheit

Anders als im BDSG ist in der DSGVO das Prinzip der Datensicherheit als allgemeiner Grundsatz normiert. Geht er in den einschlägigen nationalen Regelungen implizit aus spezifischen Anforderungen hervor, fordert Art. 5 Abs. 1 lit. f (i.V.m. Art 32) ausdrücklich zur Gewährleistung dessen auf, dass unter Berücksichtigung der technischen und organisatorischen Möglichkeiten, der Kosten und der zweckbedingten Umstände der Verarbeitung erhobene Daten angemessen geschützt und dem Zugriff unbefugter Dritter entzogen werden. Gleichzeitig soll die Verhinderung unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sichergestellt werden.

Das Sicherheitsniveau muss dabei dem jeweiligen Gefahrenpotenzial angemessen angepasst sein.

Auch die Datensicherheit kann zur bestmöglichen zweckwahrenden Anonymisierung und Pseudonymisierung verpflichten, hält aber auch zur Wartung und Überprüfung der Integrität der verwendeten Systeme an.

4.) Datenrichtigkeit

Ebenfalls als datenschutzrechtlicher Grundsatz ist in Art. 5 Abs. 1 lit. d DSGVO auch das in §20 Abs. 1 BDSG zum Ausdruck kommende Richtigkeitsgebot formuliert, das den Verantwortlichen verpflichtet, für die sachliche und inhaltliche Tatsächlichkeit der erhobenen Daten und für ihre Aktualität Sorge zu tragen.

Gleichsam fordert das allgemeine Prinzip dazu auf, alle technischen und organisatorischen Maßnahmen dafür zu treffen, dass im Falle der Unrichtigkeit oder Rückständigkeit der verwendeten Daten eine unverzügliche Berichtigung oder Löschung erfolgen kann.

Damit geht die genannte Vorschrift weiter als §20 Abs. 1 BDSG, der nur eine Berichtigung, aber keine Löschung als ultima ratio vorsieht.

5.) Neuartig: Rechenschaftspflicht

Als gegenüber den bewährten Datenschutzgrundsätzen relevante Änderung erweist sich die in Art. 5 Abs. 2 DSGVO erstmalig eingeführte Pflicht, auf Anforderung die Einhaltung aller Datenschutzprinzipien nachweisen zu können.

Mit der so begründeten Rechenschaftspflicht wollte der europäische Gesetzgeber der Umsetzung der datenschutzrechtlichen Grundpflichten Nachdruck verleihen und zur unbedingten Befolgen anhalten.

Inwiefern sich aus der neuartigen Verbindlichkeit Eingriffsbefugnisse der Aufsichtsbehörden herleiten lassen, vermag noch nicht abschließend beurteilt zu werden. Allerdings können bei einem belegbaren Verstoß gegen die Basisprinzipien nach Art. 83 Abs. 5 DSGVO äußerst empfindliche Geldbußen bis zu einer Höhe von 20 000 000€ oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.

Empfehlenswert ist es für Online-Händler deshalb, durch eine geeignete Protokollierung ihrer Verarbeitungssysteme und Nutzungsumfänge im Zweifel beweisen zu können, dass eine kontinuierliche und gewissenhafte autonome Ausrichtung nach den geltenden Leitlinien erfolgt ist und weiterhin erfolgt.

II. Änderungen der Voraussetzungen für rechtmäßige Datenverarbeitungen

Ebenso wie das bisherige deutsche Datenschutzrecht geht auch die europäische DSGVO von einem grundsätzlichen Datenverarbeitungsverbot mit Erlaubnisvorbehalt aus. Während jedoch die Tatbestände einer rechtmäßigen Erhebung und Nutzung von personenbezogenen Daten im BDSG über das Gesetz hinweg verstreut aufzufinden sind, kodifiziert der europäische Gesetzgeber diese gesammelt in Art. 6 DSGVO. Zwar wird auch hier eine Differenzierung zwischen der durch eine Einwilligung des Betroffenen gerechtfertigten Datennutzung und gesetzlichen Gestattungstatbeständen vorgenommen. Dabei entfallen allerdings bisher nach dem BDSG ausdrücklich vorgesehene

Rechtmäßigkeitsgrundlagen.

1.) Die datenschutzrechtliche Einwilligung

Wie auch das deutsche Recht macht der europäische Gesetzgeber die Rechtmäßigkeit einer Datenverarbeitung maßgeblich von der Einwilligung des Betroffenen abhängig, Art. 6 Abs. 1 lit. a DSGVO.

a) Ausdrücklichkeits- und Bestimmtheitserfordernis

Dabei ist, ähnlich der derzeitigen Kodifizierung in §4a BDSG, zwingend darauf zu achten, dass die Einwilligung des Nutzers auf dessen autonomer und ausdrücklich selbstbestimmter Entscheidung zur Preisgabe der relevanten Daten beruht. Sie ist insofern streng zweckgebunden einzuholen und muss, wie sich aus dem Umkehrschluss der Formulierung „Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben“ ergibt, stets die mit der Einwilligung zu rechtfertigenden Verarbeitungszwecke anführen.

Ebenso wie im geltenden deutschen Recht entfällt damit die Möglichkeit einer Generaleinwilligung in eine unbeschränkte Verarbeitung und Nutzung der personenbezogenen Daten.

Auch der europäische Gesetzgeber sieht die Möglichkeit einer elektronischen Einwilligung (derzeit geregelt in §13 Abs. 2 TMG) vor, regelt deren Anforderungen aber nicht spezifisch, sondern ordnet sie ausweislich des Erwägungsgrundes 32 als einen Unterfall der „schriftlichen Erklärung“ ein.

Wird die Einwilligungserklärung – wie im Online-Handel üblich – elektronisch eingeholt, so soll dies nach Erwägungsgrund 32 beispielsweise durch das aktive Anklicken eines Kontrollkästchens möglich sein.

Erstmalig normiert wird im unmittelbaren Zusammenhang auch die – in Deutschland vor allem durch die Rechtsprechung geprägte – Kasuistik der vorangekreuzten Einwilligungsfelder.

Nach Erwägungsgrund 32 sollen Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person keine wirksame Einwilligung darstellen.

b) Beweisbarkeits- und Transparenzgebot

Aus Art. 7 DSGVO, welcher die Anforderungen an die rechtfertigende datenschutzrechtliche Einwilligung konkretisiert, geht hervor, dass eine eingeholte Einwilligung zwingend zu dokumentieren und zu speichern ist. Online-Händler haben insofern durch informationstechnologische Systeme sicherzustellen, dass sie eine erteilte Nutzereinwilligung im Zweifel beweisen können.

Weil die elektronische Einwilligungserklärung als Form der schriftlichen gewertet wird, ist für ihr Wirksamwerden das neue spezialgesetzlich normierte Transparenzgebot des Art. 7 Abs. 2 DSGVO zu beachten. Danach muss die Einwilligung in klarer und verständlicher Sprache erfolgen und insbesondere dann, wenn der Einwilligungstext noch andere Sachverhalte betrifft, die datenschutzrechtliche Relevanz gesondert hervorheben.

c) Freiwilligkeit

Ist die Einwilligung nur rechtfertigend, wenn sie Ausdruck einer selbstbestimmten und ungezwungenen Entscheidung ist, so muss sie zwingend freiwillig erteilt werden (Erwägungsgrund 32). Jegliche forcierenden Handlungen des Verarbeitenden sowie die Ausübung von Druck lassen ihre Wirksamkeit entfallen.

In diesem Zusammenhang neu ist die Regelung des Art. 7 Abs. 4 DSGVO, welche die Freiwilligkeit auch davon abhängig macht, ob die Einwilligung in Datenverarbeitungsprozesse als zwingende Bedingung für die Durchführung eines Vertrages formuliert ist, obwohl der Verarbeiter die Daten dafür eigentlich nicht benötigt.

Anzunehmen ist insofern, dass die Freiwilligkeit und mithin die Wirksamkeit der Einwilligung fortan entfallen soll, wenn an ihre Erteilung das „Ob" der Durchführung eines Kausalgeschäfts gekoppelt wird, das mit der konkreten Datennutzung oder dem Umfang der erhobenen Daten in keinem sachlichen Zusammenhang steht.

Auswirkungen ergeben sich hier vor allem für Online-Gewinnspiele, bei denen eine Teilnahme nicht selten von der Einwilligung des Nutzers in die Verarbeitung von Daten zu Werbezwecken abhängig gemacht wird, die für die konkrete Gewinnaktion nicht zwangsweise erforderlich sind. Ebenso wird die Zulässigkeit des Erfordernisses einer Newsletter-Anmeldung zur möglichen Inanspruchnahme eines Gewinns in Zukunft vor neue Hürden gestellt werden.

d) Widerruflichkeit

Wie im deutschen Datenschutzrecht muss auch nach der DSGVO der Betroffene eine einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können, Art. 7 Abs. 3.

Neu ist hierbei allerdings die Pflicht des Verarbeiters zur Einhaltung eines Simplizitätsgebots: der Widerruf der Einwilligung muss in Zukunft genau so einfach sein wie ihre Erteilung.

Dies erscheint insbesondere im Falle elektronisch eingeholter Einwilligungen durch die schlichte Betätigung einer Checkbox problematisch, weil es – ohne registriertes Kundenkonto – meist an der Möglichkeit fehlen wird, das Checkbox-Häkchen nachträglich wieder zu entfernen. Zwar wird ausdrücklich nicht gefordert, dass das Widerrufsverfahren demjenigen der Erteilung 1:1 entspricht. Fraglich bleibt aber dennoch, ob ein Widerruf per Mail oder Telefonanruf in seiner Unkompliziertheit dem bloßen Setzen eines Häkchens nebst einer Einwilligungserklärung wird entsprechend können.

Immerhin für die wegen ihrer Marketingwirksamkeit besonders bedeutsamen Fälle der Newsletter-Werbung wird auch dem neuen Simplizitätsgebot wohl hinreichend dadurch Rechnung getragen, dass jeder Mail am Ende ein eigener „Unsubscribe-Link" beigestellt wird, dessen bloße Betätigung der Datenverarbeitung Einhalt gebietet.

e) Wichtig: Fortgeltung für vor 2018 eingeholte Einwilligungen

Weil mit Auslaufen der Übergangsfristen zum 25.05.2018 die besonderen Einwilligungsbestimmungen der DSGVO an die Stelle der bis dato geltenden nationalen Vorschriften treten werden, war fraglich, wie die bis zu diesem Zeitpunkt unter Geltung der alten Rechtslage in den Mitgliedsstaaten wirksam eingeholten Einwilligungen umgegangen werden sollte.

Zugunsten der Verarbeiter hat sich der europäische Gesetzgeber hier für eine Fortgeltung der bereits eingeholten datenschutzrechtlichen Einwilligungen entschieden.

Nach Erwägungsgrund 171 bleiben insofern auf Grundlage des geltenden BDSG und TMG wirksam eingeholte Einwilligungen in Verarbeitungsprozesse auch unter Geltung der neuen DSGVO bestehen, sofern die Art der erteilten Einwilligung auch den Bedingungen der DSGVO entspricht. Da die maßgeblichen Einwilligungserfordernisse nach geltendem und neuem Recht in Deutschland sich weitgehend überschneiden, entfällt im Online-Handel in der Regel die Notwendigkeit, zum 25.05.2018 von jedem Nutzer, dessen Daten bereits mit Einwilligung verarbeitet werden, eine solche erneut einzuholen.

f) Neu: besondere Erfordernisse für die Einwilligung Minderjähriger

Eine neuartige Ausprägung hat die datenschutzrechtliche Einwilligungsdogmatik in der Normierung spezieller Wirksamkeitsanforderungen für die datenschutzrechtliche Verarbeitungserlaubnis Minderjähriger erhalten, welche die Tragweite und Reichweite von erteilten Rechtfertigungen weniger sicher und umfassend abzuschätzen wissen als Erwachsene.

Während nach geltendem deutschen Recht die Wirksamkeit von Einwilligungen Minderjähriger individuell nach deren geistiger Reife und konkreter Einsichtsfähigkeit bemessen wird, wird es nach Art. 8 DSGVO zukünftig starre Altersgrenzen geben.

Gemäß Art. 8 Abs. 1 DSGVO wird die Einwilligung eines Minderjährigen in die Verarbeitung von diesen betreffenden personenbezogenen Daten in Kommunikationsmedien grundsätzlich nur wirksam, wenn dieser das 16. Lebensjahr vollendet hat.
Kinder und Jugendliche unter 16 Jahren sollen demgegenüber autonom keine wirksamen Erlaubnisse erteilen können. Vielmehr bedarf es für die rechtmäßige Nutzung der Daten von unter 16-Jährigen in Zukunft der ausdrücklichen Genehmigung des gesetzlichen Vertreters.

Die maßgebliche Altersgrenze bei 16 Jahren ist allerdings nur ein Richtwert, von welchem die Mitgliedsstaaten gemäß Art. 8 Abs. 1 Unterabsatz 2 DSGVO abweichen dürfen. Dabei darf in Anbetracht der Wirksamkeit von Minderjährigeneinwilligungen allerdings nicht die absolute Untergrenze von 13 Lebensjahren unterschritten werden.

Inwiefern der deutsche Gesetzgeber bei der nationalen Ausgestaltung der speziellen Anforderungen an der vorgegebenen Altersgrenze von 16 Jahren festhalten oder diese über- oder unterbieten wird, kann bisher noch nicht gesagt werden.

Fest steht aber jetzt schon, dass Online-Händler künftig geeignete Altersverifikationssysteme in ihre

elektronischen Einwilligungsprozesse werden integrieren müssen, um sich nicht der Gefahr unrechtmäßiger Datenverarbeitungen auszusetzen und mithin die Wirksamkeit aller eingeholten Einwilligungen garantieren zu können. Gleichsam wird die Einrichtung neuer informationstechnologische Mechanismen erforderlich werden, mit denen ein gesetzlicher Vertreter als solcher identifiziert und zur Abgabe einer eigenständigen Einwilligung für den Schutzbefohlenen veranlasst werden kann.

Dies gilt insbesondere deshalb, weil Art. 8 Abs. 2 DSGVO den Verantwortlichen abverlangt, „angemessene Anstrengungen zu unternehmen“, um die Einhaltung der altersgerechten Differenzierung zu gewährleisten und im Zweifel die Einschaltung der elterlichen Vertreter sicherzustellen.

2.) Gesetzliche Erlaubnistatbestände

Neben der ausdrücklichen und autonomen Einwilligung des Betroffenen, die als primäres datenschutzrechtliches Institut für die Rechtmäßigkeit jeglicher Verarbeitung von Nöten ist, kodifiziert die DSGVO zusätzliche Konstellationen zulässiger Datennutzungsprozesse, bei denen eine vorherige Einwilligung entbehrlich sein soll.

Gleichzeitig entfallen aber auch gesetzliche Erlaubnisse für bisher nach dem BDSG und TMG zulässige Verarbeitungsprozesse.

a) Rechtmäßige Verarbeitungen ohne Einwilligungserfordernis

Erlaubt ist nach Art. 6 Abs. 1 lit. b-f die einwilligungslose Datenverarbeitung, die

- für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist (vgl. die gleichlautende Regelung des §28 Abs. 1 Nr. 1 BDSG), oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen
- zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt
- erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist
- die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen (vgl. §28 Abs. 1 Nr. 2 BDSG)

Insbesondere die Datenverarbeitung zur Wahrung berechtigter Interessen wird im Online-Handel große Bedeutung erlangen, da sie im Einzelfall nicht nur Fälle des Direktmarketings, sondern auch nutzungsbasierte Online-Werbung zu rechtfertigen vermag, ohne dass es einer Einwilligung bedürfte. So ergibt sich aus Erwägungsgrund 47, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann. Voraussetzung bleibt aber in jedem Einzelfall, dass vor allem die persönlichkeitsrechtlichen Belange des Geworbenen die Werbeinteressen nicht überwiegen.

b) Wegfall anerkannter Erlaubnisgründe

Ein Rückgriff auch die berechtigten Interessen wird in Zukunft vor allem deswegen maßgebliche Bedeutung erlangen, weil für die Praxis des Online-Handels hoch relevante Nutzungsvorgänge, die bisher ohne Einwilligung möglich waren, ab 2018 den generellen Einwilligungserfordernissen unterliegen werden.

So werden die besonderen datenschutzrechtlichen Erlaubnistatbestände der §§28a und 28b BDSG durch die DSGVO vollständig aufgehoben. Eine Datenübermittlung an Auskunfteien sowie die Evaluation von Nutzerverhaltensmuster im Wege des „Scoring" werden künftig nur noch dann zulässig sein, wenn Ihnen eine ausdrückliche Einwilligung des Betroffenen im Sinne des Art. 6 Abs. 1 lit. a DSGVO vorangegangen ist.

Gleiches gilt für die Sondererlaubnis der Datennutzung im Beschäftigungsverhältnis nach dem – zum 25.05.2018 entfallenden - §32 BDSG.

Besonders zu beachten ist gleichsam, dass die gesetzliche Erlaubnis zur pseudonymisierten Erstellung von Nutzungsprofilen zu Marktforschungszwecken ohne vorangegangene Einwilligung entfällt nach §15 Abs. 3 TMG ersatzlos wegfällt. Die Rechtmäßigkeit eines solchen „Profilings" – ob mit oder ohne Pseudonymisierung – wird sich in Zukunft ausschließlich am Vorliegen einer wirksamen zweckgerichteten Betroffeneneinwilligung orientieren.

Zwar ermöglichen die neuen, meist generell gehaltenen Erlaubnistatbestände der DSGVO eine flexiblere Rechtsanwendung. In Ermangelung klarer Abgrenzungskriterien und der Normierung eindeutig zulässiger Datenverarbeitungsprozesse geht dies aber für die Verantwortlichen gleichsam zu Lasten der Rechtssicherheit.

3.) Geänderte Zulässigkeitsbedingungen für die Zweckänderung von Verarbeitungen

Die DSGVO statuiert im Verhältnis zur derzeitigen Rechtslage deutlich strengere Anforderungen an die Zulässigkeit von Datenverarbeitungen, die zu einem anderen Zweck erfolgen sollen als zu demjenigen, für den die Betroffeneneinwilligung ursprünglich eingeholt wurde.

Konnte die einwilligungslose Zweckänderung, beispielsweise die Verwendung einer für den Empfang von Newslettern erhobenen E-Mail-Adresse zu Zwecken der Marktforschung oder der Liquiditätsprüfung oder der Erstellung eines Nutzerprofils, bisher nach §28 Abs.2 Nr. 1 BDSG durch berechtigte Interessen gerechtfertigt werden, ist nunmehr ausweislich des Art. 6 Abs. 4 BDSG eine umfangreiche Interessenabwägung der Vereinbarkeit erforderlich, die bei negativem Ausfall die Einholung einer separaten Einwilligung erforderlich machen soll.

Für die Bewertung, ob der intendierte Nutzungszweck mit dem ursprünglichen vereinbar ist, sind zukünftig insbesondere folgende Gesichtspunkte zu berücksichtigen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten (sensible Daten nach Art. 9 DSGVO) verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann

Ergibt die stets im Einzelfall durchzuführende Prüfung eine Unvereinbarkeit, ist die Zweckänderung nur bei expliziter Einwilligung zulässig.

Weil der Verantwortliche das positive Abwägungsergebnis und seine Grundlagen im Zweifelsfall aber beweisen muss und die genannten Kriterien in Ermangelung konkreter Bewertungsmaßstäbe kaum geeignet sind, dem Laien eine interessengerechte Entscheidung zu ermöglichen, wird sich die Änderung der Zulässigkeitsanforderungen faktisch wie eine Sperre der einwilligungslos erlaubten Zweckänderungen auswirken.

Zu hoch sind nämlich die Gefahren einer fehlerhaften Beurteilung und zu gering ist die Rechtssicherheit, sodass zu empfehlen ist, im Interesse einer Risikominimierung künftig jeder Zweckänderung eine erneute Einwilligungserteilung vorangehen zu lassen.

Autor:
RA Phil Salewski
Rechtsanwalt