jusIT - Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz

Die Weisung im Datenschutzrecht - Konsequenzen aus Datenschutzverstößen durch Mitarbeiter

Datenschutz & E-Government · Mag. Nicole Gosch/MMag. Theresia Leitinger, M.A.I.S. · jusIT 2022/9 · jusIT 2022, 23 · Heft 1 v. 25.2.2022

Dieser Beitrag erscheint als Folgeartikel zum Beitrag jusIT 2021/46, in welchem die Zurechnung unterstellter Personen zum Verantwortlichen mit besonderem Fokus auf das Verhältnis zwischen "Mitarbeiter" und "Arbeitgeber" diskutiert wurde. Nachdem im vorherigen Beitrag die Weisungsunterworfenheit als ein zentrales Kriterium für die Zurechnung identifiziert wurde, setzt sich dieser Artikel näher mit der datenschutzrechtlichen "Weisung", in der DS-GVO auch als "Anweisung" bezeichnet, des Arbeitgebers an den Mitarbeiter auseinander. Es wird untersucht, welche Charakteristika die datenschutzrechtliche Weisung in sich birgt, ob eine Parallele zur arbeitsrechtlichen Weisung vorliegt oder diese als originär datenschutzrechtliches Instrument betrachtet werden muss und welche Konsequenzen Mitarbeiter zu erwarten haben, wenn sie gegen datenschutzrechtliche Vorgaben verstoßen.
» **Deskriptoren:** Weisungscharakteristik, Zurechnung, Verantwortlichkeit, Rechtmäßigkeit, Rechtfertigungskette, Datensicherheit, Haftung

» **Normen:** VO (EU) 2016/679 : Art 5, 6, 9, 24, 28, 29 und 32; DSG: § 6

1. Der Begriff der Weisung in der DS-GVO

1.1. Einordnung der Weisung ins Gefüge der DS-GVO

Der Begriff der "Weisung" findet sich in der DS-GVO[1] nur in vier Artikeln[2] wieder, nämlich in den Bestimmungen über den Auftragsverarbeiter des Art 28, in jener zur Verarbeitung unter Aufsicht des Verantwortlichen oder des Auftragsverarbeiters nach Art 29 und in den Normen zur Unabhängigkeit der Aufsichtsbehörde sowie des

Europäischen Datenschutzausschusses (EDSA) nach Art 52 und 59. Weiters wird in der deutschen Sprachfassung in Art 32 Abs 2, Art 38 Abs 3, Art 72 Abs 2 und Art 82 Abs 2 der Terminus "Anweisung" verwendet, wenngleich ein Grund für diese semantische Differenzierung nicht ersichtlich ist. Die englische Sprachfassung greift nahezu durchgängig auf den Begriff "instruction" zurück, eine Abweichung besteht lediglich in Art 83 der englischen Übersetzung mit dem Wort "order". Für eine durchgängige Verwendung des Begriffes "instruction" in der englischen Sprachfassung spricht weiters, dass auch im englischen Arbeitsrecht der Begriff "instruction" verwendet wird.[3] Es ist sohin wohl davon auszugehen, dass ebenso wie in der englischen Sprachfassung auch für die deutsche Sprachfassung gilt, dass die Begriffe "Weisung" und "Anweisung" synonym verstanden werden können. In weiterer Folge wird daher zur Vermeidung der Verwendung doppelter Begrifflichkeiten durchgängig von der "Weisung" gesprochen, wobei der in der deutschen Sprachfassung der DS-GVO ebenfalls gebräuchliche Terminus "Anweisung" davon mit umfasst ist.

1.2. Terminologische Besonderheiten des Weisungsbegriffs

Eine besondere Bedeutung entfaltet die Weisung im Rahmen des Art 29. Art 29 regelt das Institut der datenschutzrechtlichen Weisung des Verantwortlichen an unterstellte Personen sowie an

Auftragsverarbeiter. In diesem Beitrag wird für "unterstellte Person" der Begriff des "Mitarbeiters", der persönlichen, sachlichen und fachlichen Weisungen des Arbeitgebers unterliegt, herangezogen.[4] Mitarbeiter dürfen dem Wortlaut des Art 29 zufolge personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten. Daneben werden auch Auftragsverarbeiter im Rahmen des Art 29 an die Weisung des Verantwortlichen gebunden. Wie im ersten Beitrag[5] aufgezeigt wurde, nimmt die Weisung eine zentrale Rolle als Zurechnungsinstrument für die Verantwortlichkeit in der DS-GVO ein. Trotz der daraus resultierenden Relevanz wird der Begriff der Weisung in der DS-GVO überraschenderweise nicht legal definiert. Eine bestimmte Form ist nicht normiert.[6] Im allgemeinen Sprachgebrauch ist eine Weisung als *"Anordnung, Hinweis, wie etwas zu tun ist, wie man sich verhalten soll"* [7] zu verstehen. Legt man diese Umschreibung auf die Normadressaten des Art 29 um, dürfen Mitarbeiter (und Auftragsverarbeiter) personenbezogene Daten nur so verarbeiten, wie es den Anordnungen oder Hinweisen des Verantwortlichen entspricht. Die Weisung hätte demnach eine solche Anordnung zu enthalten, wie die Daten zu verarbeiten sind und wie sich Mitarbeiter bei der Verarbeitung der Daten verhalten sollen. Mit der Subsumtion der Normadressaten unter die Definition des Duden kann allerdings nicht das Auslangen gefunden werden. Das Rechtsinstitut der datenschutzrechtlichen Weisung ist unbestimmt und bedarf einer näheren Auslegung.

1.3. Erwägungen zur Auslegung des Weisungsbegriffs

Zunächst ist die Frage zu beantworten, ob die Rechtsqualität der datenschutzrechtlichen Weisung möglicherweise aus einem anderen Rechtsgebiet - der Begriff der Weisung ist vor allem im Arbeitsrecht,[8] aber auch im Strafrecht,[9] Verwaltungsrecht[10] oder im Unternehmensrecht[11] gebräuchlich - herzuleiten ist. Das grundlegende Konzept der Weisung ist bereits hinlänglich aus dem Arbeitsrecht bekannt,[12] wenngleich der Terminus nicht wörtlich im Zusammenhang mit den aus dem Dienstvertrag resultierenden Pflichten des § 1151 ABGB genannt wird. Nach der EuGH-Judikatur ist die Weisungsgebundenheit eines der wesentlichen Bestandsmerkmale des Arbeitsvertrages, ebenso wie die Entgeltlichkeit.[13] Die Weisung ist als wesentliches Charakteristikum dem Dienstvertrag zwischen Mitarbeiter und Arbeitgeber inhärent.[14] Da die Weisung des Verantwortlichen als Zurechnungsinstrument für Mitarbeiter intendiert ist, liegt der Schluss nahe, dass es sich auch bei der datenschutzrechtlichen Weisung um eine arbeitsrechtliche Weisung im engeren Sinn handeln könnte.
Das Arbeitsrecht unterscheidet zwischen persönlichen Weisungen - etwa zur Abgabe der Stundenaufzeichnungen von Mitarbeitern im Homeoffice oder im Außendienst - und Weisungen, welche den Gegenstand der Arbeitspflicht betreffen.[15] Weisungen, die den Gegenstand der Arbeitspflicht betreffen, können in fachliche und sachliche Weisungen unterteilt werden, wobei erstere das Arbeitsverfahren selbst betreffen, sachliche Weisungen hingegen das gewünschte Arbeitsergebnis konkretisieren.[16] Die Weisung, wie personenbezogene Daten zu verarbeiten sind, könnte sohin in beide Kategorien fallen, je nachdem in welchem Umfang und in welcher Form diese zu verarbeiten sind. Hauptsächlich werden Weisungen das Arbeitsverfahren selbst betreffen, nämlich immer dann, wenn Mitarbeiter als ausführende Per-

sonen des Verantwortlichen die Daten von Betroffenen verarbeiten und der Arbeitgeber dafür eine Art 29 entsprechende Weisung erteilt. Eine solche Anordnung würde einer fachlichen Weisung im arbeitsrechtlichen Sinn entsprechen. Auch im Arbeitsrecht sind die Voraussetzungen und die Form der Erteilung der fachlichen Weisung allerdings weder gesetzlich klar determiniert noch bildeten sich bislang eindeutige Kriterien zur Form der arbeitsrechtlichen Weisung in der Rsp heraus. Die Frage, ob die Ausgestaltung der datenschutzrechtlichen Weisung zur Verarbeitung von personenbezogenen Daten an die fachliche Weisung des Arbeitsrechts angelehnt werden kann, kann somit bereits aufgrund der Unbestimmtheit beider Begriffe nicht eindeutig beantwortet

werden. Dass der Weisungsbegriff in der DS-GVO uE ohnehin unabhängig von der arbeitsrechtlichen Definition auszulegen ist,[17] ergibt sich schon daraus, dass Art 29 eine Weisungsbefugnis des Verantwortlichen nicht nur gegenüber unterstellten Personen,[18] sohin Mitarbeitern, sondern auch gegenüber Auftragsverarbeitern, für die die arbeitsrechtlichen Bestimmungen nicht herangezogen werden können, enthält. Die DS-GVO verfolgt dediziert das Ziel, auch Auftragsverarbeiter im Sachzusammenhang der Verarbeitung personenbezogener Daten an den Verantwortlichen zu binden. Eine Auslegung des Weisungsbegriffs im Lichte des Arbeitsrechts[19] wäre daher unter Beachtung der Systematik und Zielsetzung der DS-GVO verfehlt. Darüber hinaus wird die datenschutzrechtliche Weisung im Rahmen eines europarechtlich unmittelbar anwendbaren Rechtsakts, nämlich der DS-GVO, verwendet, deren Begriffe unionsautonome Bedeutung erlangen, weshalb der Begriff der Weisung in der DS-GVO zudem losgelöst von einem etwaigen anders gelagerten nationalen Verständnis auszulegen ist. Demzufolge ist der Weisung im Gefüge des europäischen Datenschutzrechts ein eigenes Begriffsverständnis zugrunde zu legen.

2. Die Rolle der Weisung im Datenschutzrecht

2.1. Charakteristika der Weisung im Datenschutzrecht

Nicht vollständig geklärt ist bisher, welche Charakteristik und in der Folge Bedeutung der Weisung im Datenschutzrecht tatsächlich zukommt. Zunächst kann die Weisung als Bestandteil der Regelungen über die Zuteilung von Verantwortung im Rahmen der DS-GVO[20] und somit als Instrument im Gefüge der Rollenverteilung[21] gesehen werden. Mithilfe der Weisung werden die unterstellten Personen an die Einheit des Verantwortlichen gebunden und bekleiden damit im Rahmen dieser Zuordnung keine eigene Rolle im datenschutzrechtlichen Gefüge. Nach *Hartung* wäre in diesem Zusammenhang auch keine gesonderte Rechtfertigung für Verarbeitungen notwendig, die nicht vom Verantwortlichen selbst, sondern von unterstellten Personen oder auch Auftragsverarbeitern durchgeführt werden.[22] Ob tatsächlich keine gesonderte Rechtsgrundlage benötigt wird, ist insb im Rahmen der Auftragsverarbeitung Thema der laufenden datenschutzrechtlichen Diskussion.[23] UE sprechen jedoch gute Gründe dafür, die datenschutzrechtliche Weisung nicht ausschließlich als Zurechnungsinstrument im Gefüge der Rollenverteilung zu betrachten.

An anderer Stelle nämlich wird die Weisung als zentrales, die Legitimität von Verarbeitungen vermittelnden Steuerungsinstrument im Beziehungsgefüge zwischen dem Verantwortlichen und den ihm unterstellten Personen beschrieben,[24] was auf eine mögliche Verortung der Weisung im Gefüge der Rechtmäßigkeit der Verarbeitung hindeuten könnte. Konkret sieht *Martini* in der Weisung eine "abgeleitete Rechtfertigung", die Akteuren, die eine Datenverarbeitung nicht selbst auf Art 6 stützen können, die Verarbeitung personenbezogener Daten erlaubt.[25] Diese Sichtweise ist uE unter Einbeziehung des Grundsatzes der Rechtmäßigkeit in Art 5 Abs 1 lit a überzeugend. Jede Verarbeitung personenbezogener Daten muss in Einklang mit den in Art 5 konstituierten Grundsätzen stattfinden, um zulässig zu sein. Dabei beziehen sich die Grundsätze des Art 5 darauf, wie personenbezogene Daten verarbeitet werden müssen bzw wie diese im Rahmen von datenschutzrechtlich relevanten Verarbeitungsvorgängen beschaffen sein sollen.[26] Sie nehmen allerdings nicht darauf Bezug, wer konkret die Verarbeitung als solche vornehmen muss, weshalb konsequenterweise nicht anzunehmen ist, dass die Rechtmäßigkeit der Verarbeitung alleine der Sphäre des Verantwortlichen zuzuordnen ist. Verarbeiten Mitarbeiter personenbezogene Daten, handelt es sich dabei um eine Verarbeitung iSv Art 4 Z 2, die grundsätzlich einer Rechtsgrundlage bedarf. Art 29 legt ausdrücklich fest, dass personenbezogene Daten durch die Normadressaten ausschließlich auf Weisung des Verantwortlichen verarbeitet werden dürfen. Somit spricht die Konzeption des Art 29 dafür, die Weisung, neben dem Vorliegen einer unionsrechtlichen oder nationalen Verpflichtung zur Datenverarbeitung, die jedoch ausdrücklich der unterstellten Person oder dem Auftragsverarbeiter obliegen muss, als Teil der Rechtfertigungskette zu betrachten. Verarbeitet der Verantwortliche also nicht selbst personenbezogene Daten, kann die

Rechtmäßigkeit iSv Art 5 Abs 1 lit a nur über die Weisung als legitimierendes Verbindungselement, das die Verarbeitungstätigkeit durch den Auftragsverarbeiter oder den Mitarbeiter der durch Art 6 Abs 1 gerechtfertigten Verarbeitung des Verantwortlichen zurechnet, erreicht werden. Dieser Ansicht folgt offenbar auch das BVwG in einer jüngeren Entscheidung[27] zu Art 29. Laut BVwG *"rechtfertigt die Weisung die durch die unterstellten Personen durchgeführte Datenverarbeitung: sie wird dadurch dem/der Verantwortlichen zugerechnet und nicht der jeweils unterstellten Person".* Somit könnte die Weisung im Arbeitskontext und Auftragsverarbeitungsbereich als eine notwendige Vorstufe oder Vorfrage zur Rechtmäßigkeit zu verstehen sein. Insofern könnte Art 29 eine ähnliche Charakteristik wie Art 9 Abs 2 aufweisen. Für den Fall, dass besondere Kategorien personenbezogener Daten verarbeitet werden, ist neben dem Vorliegen einer konkreten Rechtfertigung durch Art 6 ein Erlaubnistatbestand des Art 9 Abs 2 erforderlich.[28] Für Auftragsverarbeitungsverhältnisse sowie Verarbeitungen durch Mitarbeiter wäre konsequenterweise neben der Rechtfertigung durch Art 6 Abs 1 eine Weisung iSv Art 29 erforderlich, es sei denn, es liegt eine ausdrückliche Verpflichtung zur Datenverarbeitung für die beaufsichtigte Person vor. Sollen personenbezogene Daten von Mitarbeitern verarbeitet werden, reicht es daher nicht aus, wenn der Verantwortliche durch einen Rechtfertigungstatbestand in Art 6 Abs 1 gerechtfertigt ist. Für Mitarbeiter gibt es daher nur zwei Varianten, unter denen sie eine rechtmäßige Datenverarbeitung vornehmen können:

- Es liegt die Weisung des Verantwortlichen für die Datenverarbeitung vor.
- Es gibt eine konkrete Verpflichtung im Unionsrecht oder nationalen Recht, diese Datenverarbeitung vorzunehmen.

Darüber hinaus ist der Weisung aufgrund der expliziten Einbindung in Art 32 Abs 4 wohl auch ein enger Zusammenhang mit der Datensicherheit zu attestieren. Es handelt sich dabei aber wohl in erster Linie nicht selbst um eine organisatorische Maßnahme iSv Art 24 Abs 1, sondern es müssen, wie sich aus dem Wortlaut von Art 32 Abs 4 ergibt, "Schritte" und sohin technische bzw organisatorische Maßnahmen (TOM) getroffen werden, um sicherzustellen, dass eine Verarbeitung auch nur auf Weisung des Verantwortlichen möglich ist. *Bergauer* [29] zufolge sind mit TOM *"sämtliche Handlungen und Vorkehrungen gemeint, die dazu beitragen, die Daten DSGVO-konform zu verarbeiten".* Organisatorische Maßnahmen im Weisungskontext betreffen etwa strukturelle Anordnungen bzw Arbeitsanweisungen oder die Festlegung von Hierarchien und Weisungsstrukturen. Zu Maßnahmen iSv Art 32 Abs 4 kann daher idZ ebenso ein "Berechtigungskonzept" zählen, das ausschließlich angewiesenen Mitarbeitern den Zugang zu personenbezogenen Daten ermöglicht. Aber auch die Dokumentation der erteilten Weisungen durch den Verantwortlichen ist eine organisatorische Maßnahme, die uE aufgrund der legitimierenden Wirkung der Weisung notwendig ist, um iSv Art 24 Abs 1 den Nachweis dafür erbringen zu können, dass die Verarbeitung im Einklang mit der DS-GVO erfolgte. Zusammenfassend kann uE festgehalten werden, dass die Weisung eine zentrale Rolle im Auftragsverarbeitungsbereich sowie bei Verarbeitungen im Beschäftigungskontext spielt. Sie wirkt sich als Zurechnungsinstrument unmittelbar auf die Rollenverteilung, aber auch als legitimierendes Verbindungselement auf die Rechtmäßigkeit der Verarbeitung personenbezogener Daten aus. Für den Mitarbeiter ist das Vorliegen einer Weisung die Rechtfertigung, personenbezogene Daten verarbeiten zu dürfen und dennoch nicht Verantwortlicher dieser Datenverarbeitung zu sein. Darüber hinaus muss die Weisung auch im Kontext der Datensicherheit zusammen mit den dazugehörigen TOM betrachtet werden. Diese Erwägungen sind bei der Frage zu berücksichtigen, wie eine Weisung iSd Art 29 formuliert werden muss bzw zu beschaffen sein hat, um den Anforderungen der DS-GVO zu entsprechen.

2.2. Formanforderungen der datenschutzrechtlichen Weisung

Art 29 statuiert selbst nichts Näheres über den konkreten Inhalt oder die Form, in der die Weisung durch den Verantwortlichen erteilt werden sollte.[30] Obwohl Art 29 neben den Mitarbeitern des Verantwortlichen auch Auftragsverarbeiter adressiert, sieht die DS-GVO

unterschiedliche Regelungen für beide Fallgruppen vor. Art 28 Abs 3 lit a normiert explizit, dass personenbezogene Daten nur auf "dokumentierte" Weisung des Verantwortlichen verarbeitet werden dürfen, eine Voraussetzung, die in Art 29 gänzlich fehlt. Dabei handelt es sich allerdings lediglich um eine dem Auftragsverarbeiter obliegende Dokumentationspflicht und nicht um ein generelles Textformerfordernis für Weisungen.[31] Genaueres zur Form der Weisungserteilung und der Dokumentation ist allerdings auch Art 28 nicht zu entnehmen.[32] Wie bereits im ersten Teil[33] ausgeführt, unterliegt der Arbeitgeber als Verantwortlicher auch im Rahmen des Art 29 einer impliziten Dokumentationspflicht durch die Grundsätze der Verarbeitung in Art 5, speziell Art 5 Abs 1 lit f iVm Art 5 Abs 2. Dies konkretisiert sich in der Dokumentationspflicht aufgrund von Art 32 Abs 4 iVm Art 24 Abs 1 zur Nachweisbarkeit der DS-GVO-Konformität durch schriftliche Dokumentation der erteilten Weisungen. Die-

ses Dokumentationserfordernis bedeutet jedoch nicht, dass Weisungen nur dann gültig sind, wenn sie schriftlich erteilt werden. Vielmehr können Weisungen in jeglicher Form, also auch mündlich erteilt werden[34] und somit die rechtliche Grundlage für die Verarbeitung durch Mitarbeiter darstellen. Aufgrund potenzieller Haftung werden sowohl der Auftragsverarbeiter als auch die unterstellte Person in der Praxis ein nicht unwesentliches Interesse daran haben, eine bereits dokumentierte Weisung vom Verantwortlichen in Textform zu erhalten.[35]
Bei einer Weisung handelt es sich im Gegensatz zu einem Vertrag um eine einseitige Anordnung des Arbeitgebers bzw des Verantwortlichen an einen Mitarbeiter oder Auftragsverarbeiter. Obwohl Art 29 eine Weisungspflicht ex lege vorsieht, muss die Weisung gem Art 28 Abs 3 lit a Eingang in den Auftragsverarbeitungsvertrag finden, der die Grundlage für die Verarbeitung durch einen Auftragsverarbeiter festlegt. Auch hinsichtlich des vertraglichen Rahmens finden sich daher Unterschiede zwischen Mitarbeitern und Auftragsverarbeitern, die sich auch auf die Form der Weisung auswirken könnten. Im Fall des Auftragsverarbeiters konkretisiert Art 28 in insgesamt 10 Absätzen sehr genau, wie die Auftragsverarbeitungsvereinbarung als Vertrag zwischen Verantwortlichem und Auftragsverarbeiter beschaffen zu sein hat. Art 29 selbst ordnet keine Pflicht zum Abschluss eines datenschutzrechtlichen Vertrages zwischen Verantwortlichem und Mitarbeitern an und normiert auch keine näheren Begleitmaßnahmen zur Erteilung einer Weisung. Es ist denkbar, dass der Gesetzgeber die vertragliche Verankerung des Verhältnisses und die konkrete Ausgestaltung der Weisung im Verhältnis von Arbeitgeber zu Mitarbeiter bewusst nicht in der DS-GVO regeln wollte, etwa weil er eine solche Anordnung bereits in Arbeitsverträgen vermutete. Möglicherweise wurde ein gesonderter datenschutzrechtlicher Vertrag zwischen Verantwortlichem und Mitarbeitern auch deshalb nicht in einem eigenständigen Artikel konkretisiert, weil der Unionsgesetzgeber davon ausging, dass ein Mitarbeiter bereits nach zivil- und arbeitsrechtlichen Normen eng an den Verantwortlichen gebunden ist und sich eine Weisungspflicht aus dem Arbeitsrecht ergibt. Es wäre auch denkbar, dass der Gesetzgeber die Erforderlichkeit einer dem Art 28 entsprechenden vertraglichen Auskleidung von Art 29 im Hinblick auf die von Mitarbeitern durchzuführenden Verarbeitungstätigkeiten lediglich aufgrund eines legistischen Fehlers unterließ. Diesfalls könnte Art 28 auch auf das Vertragsverhältnis zwischen Verantwortlichem und Mitarbeiter im Hinblick auf die Ausgestaltung des Arbeitsvertrags per analogiam angewendet werden; Voraussetzung für eine solche Analogie wäre jedoch, dass eine planwidrige Gesetzeslücke gemessen an der gesamten geltenden Rechtsordnung besteht.[36]
In der Praxis wird in Arbeitsverträgen in aller Regel die Leistung, die von Mitarbeitern zu erbringen ist, konkretisiert bzw beschrieben, aber es finden sich keine genaueren Ausführungen dazu, wie personenbezogene Daten in Bezug auf datenschutzrechtliche Vorgaben konkret zu verarbeiten sind. Auftragsverarbeitungsvereinbarungen befassen sich hingegen explizit mit der Verarbeitung personenbezogener Daten. Daher ist es im Rahmen der Auftragsverarbeitung üblich, dass sich Weisungen in Form des Vertrags über die Auftragsverarbeitung wiederfinden.[37]
Es stellt sich allerdings die Frage, ob sich auch Weisungen an Mitarbeiter implizit aus den im

Arbeitsvertrag umschriebenen Tätigkeitsbeschreibungen ableiten lassen. In der deutschen Kommentarliteratur[38] wird derzeit die Meinung vertreten, dass Weisungen sowohl im Einzelfall als auch in Form einer generellen Anordnung erteilt werden können. Laut deutscher *Datenschutzkonferenz* können sich Weisungen insb auch in Prozessbeschreibungen, Ablaufplänen, Betriebsvereinbarungen, allgemeinen Dienstanweisungen, betrieblichen Dokumentationen sowie Handbüchern manifestieren.[39] Daher ist es uE durchaus denkbar, dass sich bereits aus dem Arbeitsvertrag eine Beauftragung zur Datenverarbeitung mit Weisungscharakter ergeben kann, sofern diese ähnlich wie in einem Auftragsverarbeitungsvertrag inhaltlich ausreichend beschrieben ist.

2.3. Inhaltsanforderungen der datenschutzrechtlichen Weisung

Was den konkreten Inhalt betrifft, den eine Weisung aufweisen muss, ist Art 29 allerdings ebenso uneindeutig wie hinsichtlich der Form der Weisungserteilung. Einerseits wird vertreten, dass die Weisung des Verantwortlichen eine Anordnung zu enthalten hat, welche Verarbeitungsschritte wie vorzunehmen sind "oder" welche TOM zu ergreifen sind.[40] Andererseits wird vorausgesetzt, dass sich die Anordnung auf den Gegenstand und die Art des Umgangs mit personenbezogenen Daten "sowie/und" die darauf gerichteten TOM bezieht.[41] Unklar bleibt, ob jede datenschutzrechtliche Weisung auch Handlungsanweisungen im Zusammenhang mit datensicherheitsrelevanten Maßnahmen zu enthalten hat. Einigkeit besteht hingegen darüber, dass ein bloßes Dulden des Verantwortlichen mangels anordnenden Charakters nicht als gültige Weisung verstanden werden soll.[42] Interessanterweise wird im Großteil der deutschen Kommentarliteratur[43] ohne jede weitere Begründung

angeführt, dass Weisungen jedenfalls "hinreichend konkret" sein sollen. Wie bereits ausgeführt, regelt dies die DS-GVO nicht explizit. Betrachtet man die Weisung als Teil der Rechtmäßigkeitskette, ließe sich ein derartiges Konkretisierungserfordernis wohl aus ErwGr 41 ableiten, wonach eine Rechtsgrundlage klar und präzise ausgestaltet und ihre Anwendung für die Rechtsunterworfenen gem der Rsp des EuGH[44] und des EGMR[45] vorhersehbar sein sollte. Als Bestandteil der Rechtmäßigkeitskette wäre die Weisung auch gem Art 13 Abs 1 lit c bzw Art 14 Abs 1 lit c in die der betroffenen Person zur Verfügung zu stellenden Informationen aufzunehmen.

Während die DS-GVO keine weiteren Hinweise bezüglich der Inhaltserfordernisse von Weisungen enthält, darf im nationalen Kontext § 6 DSG[46] nicht außer Acht gelassen werden, der besonders im Beschäftigtenkontext relevant ist und iSd Art 29 sicherstellt, dass Daten nur auf Anweisung des Verantwortlichen verarbeitet werden. *Bergauer* merkte in diesem Zusammenhang bereits an, dass die originär datenschutzrechtlichen auf das Beschäftigungsverhältnis bezogenen Regelungen des § 6 und zT auch der §§ 12 und 13 DSG, welche tatsächlich aufgrund der DS-GVO erlassen wurden, allerdings nicht als Vorschriften im Rahmen der Öffnungsklausel des Art 88 Abs 1 gemeldet wurden.[47] § 6 Abs 2 DSG sieht nicht nur vor, dass Mitarbeiter personenbezogene Daten nur aufgrund einer "ausdrücklichen" Anordnung ihres Arbeitgebers übermitteln dürfen. Darüber hinaus müssen Verantwortliche und Auftragsverarbeiter ihre Mitarbeiter vertraglich verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln. Zusätzlich stellt er sicher, dass personenbezogene Daten auch über das Arbeitsverhältnis hinaus geheim gehalten werden müssen. Art 6 Abs 2 DSG könnte daher so interpretiert werden, dass er eine Pflicht für Verantwortliche bzw Auftragsverarbeiter enthält, in Unternehmen eine konkrete, detaillierte Handlungsanleitung für die Verarbeitung personenbezogener Daten zu erteilen.[48]
Hinsichtlich des Inhalts und der Form von Weisungen kann daher festgehalten werden, dass die diesbezüglichen Voraussetzungen bisher durchwegs unklar sind. Art 29 bietet in seiner derzeitigen Ausgestaltung in diesen Fragestellungen wenig Hilfestellung, sodass es in weiterer

Folge wohl der Rsp überlassen bleibt, die Inhalts- und Formerfordernisse datenschutzrechtlicher Weisungen weiter zu konkretisieren.

3. Datenschutzrechtliche Implikationen fehlender, mangelhafter und korrekter Weisungserteilung

Besonders interessant sowohl für datenschutzverantwortliche Arbeitgeber als auch für Mitarbeiter gestaltet sich die Thematik, wie sich nun die Erteilung fehlender, mangelhafter oder auch korrekter Weisungen datenschutzrechtlich niederschlägt. Wir unterscheiden in der Folge drei Konstellationen der Weisungserteilung, die sich jeweils unterschiedlich auswirken.

3.1. Fehlen einer Weisung

Wird gar keine Weisung erteilt, wie personenbezogene Daten zu verarbeiten sind, und ergibt sich eine solche auch nicht ausreichend deutlich aus dem Arbeitsvertrag, verletzt der Verantwortliche die Pflicht des Art 29. Dadurch, dass ein Mitarbeiter trotz fehlender Weisung personenbezogene Daten verarbeiten kann, wird seitens des Arbeitgebers aufgrund des Fehlens von TOM iSv Art 24 Abs 1 zudem Art 32 Abs 4 verletzt. Liegt keine Weisung vor, besteht allerdings auch für den Mitarbeiter kein legitimierendes Verbindungselement und somit keine Rechtsgrundlage, um personenbezogene Daten verarbeiten zu dürfen. Verarbeitet ein Mitarbeiter ohne Weisung des Arbeitgebers personenbezogene Daten, entscheidet er selbst über die Zwecke und Mittel der Verarbeitung iSd Art 4 Z 7 als Verantwortlicher und kann dem Arbeitgeber nicht zugerechnet werden;[49] dies auch dann nicht, wenn die Verarbeitung nicht in seinem eigenen Interesse, sondern im Interesse des Arbeitsgebers durchgeführt wird. Etwaige Verletzungen der DS-GVO durch den Mitarbeiter sind bei unterlassener Weisung aufgrund des Fehlens einer Anordnung auch diesem selbst zuzurechnen. Dies gilt umso mehr, wenn der Mitarbeiter entgegen der Weisung des Arbeitgebers agiert.

3.2. Erteilung einer unkonkreten/nicht geeigneten Weisung

Erteilt der Arbeitgeber zwar eine Weisung, unterlässt es aber, diese hinreichend zu konkretisieren, sind die Widrigkeiten aus der Verletzung der Datensicherheit iSv Art 32 Abs 4 iVm Art 24 Abs 1 uE dem Arbeitgeber als Verantwortlichem zuzurechnen, weil der Verantwortliche dafür zu sorgen hat, dass die Datenverarbeitung DS-GVO-konform auf seine Anordnung und unter seiner Kontrolle durchgeführt wird.[50] In einem solchen Fall kann der Mitarbeiter nach Art 29 dem Arbeitgeber zugerechnet werden,

weil es grundsätzlich eine Weisung und somit eine Rechtsgrundlage für den Mitarbeiter zur Datenverarbeitung gibt. Die Ungenauigkeit der Weisung und daraus resultierende Datenschutzverstöße können dem Mitarbeiter nicht angelastet werden. Grundsätzlich haben Mitarbeiter sowie Auftragsverarbeiter auch rechtswidrige Weisungen des Verantwortlichen zu befolgen.[51] Dies hat allerdings nur insoweit zu gelten, als durch die Weisung kein offensichtlich rechtswidriges Handeln indiziert wird, da dies dem Grundsatz der Verarbeitung nach Treu und Glauben widersprechen würde.[52] Während Auftragsverarbeiter gem Art 28 Abs 3 UAbs 2 ausdrücklich die Pflicht haben, den Verantwortlichen unverzüglich zu informieren, wenn sie der Auffassung sind, dass eine Weisung gegen Datenschutzbestimmungen verstößt, lässt sich eine derartige Pflicht für Mitarbeiter nicht direkt aus der DS-GVO ableiten. Eine solche Pflicht könnte sich allerdings durchaus aus der generellen Treuepflicht des Mitarbeiters seinem Arbeitgeber gegenüber ergeben.

3.3. Erteilung einer konkreten/geeigneten Weisung

Eine dritte Konstellation wäre, dass der Verantwortliche eine konkrete Weisung für die Verarbeitung von personenbezogenen Daten in Erfüllung seiner Verpflichtung des Art 29 iVm Art 32 Abs 4 bzw Art 24 Abs 1 erteilt. Diesfalls ist der Mitarbeiter jedenfalls dem Verantwortlichen zuzurechnen und die Verarbeitung durch den Mitarbeiter ist im Rahmen des Weisungsumfangs legitimiert. Verstößt der Mitarbeiter gegen die Weisung und resultiert aus diesem Verstoß eine

Datenschutzverletzung, ist der Mitarbeiter selbst verantwortlich. Hält der Mitarbeiter die Weisung ein, kann eine etwaige Datenschutzverletzung durch Verarbeitungstätigkeiten im Rahmen der Weisung nicht dem Mitarbeiter angelastet werden und wird direkt dem Arbeitgeber als Verantwortlichem zugerechnet.

4. Drohende Konsequenzen für Mitarbeiter im Überblick

Eine Datenschutzverletzung, die einem Mitarbeiter zugerechnet wird, kann datenschutzrechtliche, zivilrechtliche, arbeitsrechtliche oder gar strafrechtliche Konsequenzen nach sich ziehen. Im Nachfolgenden kann nur eine überblicksmäßige Übersicht über mögliche Konsequenzen dargestellt werden. Insb wurden besondere Implikationen, die etwa das Dienstnehmerhaftpflichtgesetz (DHG) in diesem Zusammenhang betreffen, außen vor gelassen.

4.1. Datenschutzrechtliche und allgemeine zivilrechtliche Konsequenzen

Mit Geldbußen in Millionenhöhe sieht Art 83 eine empfindliche datenschutzrechtliche Strafdrohung als Sanktion für Datenschutzverstöße vor. Daneben bestehen sowohl im Datenschutzrecht in Art 82 als auch im österreichischen Zivilrecht Schadenersatzansprüche der betroffenen Personen, die Opfer einer Datenschutzverletzung wurden. Dafür, dass ein materieller oder immaterieller Schaden entstanden ist, ist der Betroffene beweispflichtig. In den überwiegenden Fällen wird es sich bei einer Datenschutzverletzung um einen immateriellen Schaden handeln. Da - anders als in anderen Ländern - in Österreich ein immaterieller Schaden nur bei konkreter gesetzlicher Grundlage zugesprochen wird und die gesetzliche Grundlage des Art 82 ("Schaden") auslegungsbedürftig ist, besteht anhaltende Rechtsunsicherheit in dieser für die Praxis sehr bedeutenden Frage, ob ein Schadenersatzanspruch geltend gemacht werden kann oder nicht. Aufgrund dieser Unbestimmtheit und zur Konkretisierung des Begriffes "Schaden" bzw wann dem Betroffenen aus diesem Schaden ein Anspruch iSd Art 82 erwächst, hat der OGH jüngst drei Vorlagefragen an den EuGH gerichtet.[53] Auch was die Höhe eines immateriellen Schadenersatzanspruchs angeht, besteht in Österreich ein eher niedriges Schadenersatzniveau. Zur Frage der Höhe des Schadenersatzes und Beweislast für den Schaden wird auf den aktuellen Diskussionsstand in der Literatur[54] verwiesen. Agiert ein Mitarbeiter außerhalb der vom Verantwortlichen nach Art 29 korrekt erteilten Weisung oder entscheidet er mangels Weisung alleine über die Zwecke und Mittel der Verarbeitung, ist er als Verantwortlicher einzuordnen. In diesem Fall könnte sich ein solcher Schadenersatzanspruch auch direkt gegen ihn richten. Aus diesem Grund ist es ebenso im Interesse des Mitarbeiters, dass die Weisung entsprechend vom Verantwortlichen dokumentiert wird.

4.2. Arbeitsrechtliche Konsequenzen

Weiters drohen einem Mitarbeiter, der außerhalb einer Weisung Daten verarbeitet, auch arbeitsrechtliche Konsequenzen, die von einer Verwarnung bis zur außerordentlichen Kündigung, nämlich vorzeitigem Austritt oder Entlassung als fristlose Auflösung des Dienstverhältnisses, führen können. Dies ist dann der Fall, wenn der Mitarbeiter durch den Datenschutzverstoß eine schuldhafte Pflichtverletzung begeht. Wird aufgrund des Verstoßes gegen den Arbeitgeber eine Geldbuße nach Art 83 verhängt, ist es Voraussetzung, dass von der Aufsichtsbehörde gem § 30 Abs 2 DSG eine natürliche Person ermittelt wird, die den Verstoß beging.[55]

Da somit auch der Arbeitgeber Konsequenzen durch ein Verfahren erfahren könnte, selbst wenn er schlussendlich mangels Verantwortlichkeit nicht selbst Adressat der Geldbuße ist, wird regelmäßig die Treuepflicht des Mitarbeiters gegenüber dem Arbeitgeber verletzt sein. Die Treuepflicht des Arbeitnehmers ergibt sich in Österreich aus § 1153 ABGB, für Angestellte ist sie zudem in § 7 iVm 27 Z 1 AngG normiert. Wird diese etwa durch eine mutwillige Datenschutzverletzung, die als schweres Fehlverhalten einzuordnen ist, so schwer erschüttert, dass ein Entlassungsgrund verwirklicht wurde, kann der Arbeitgeber das Dienstverhältnis rechtmäßig fristlos beenden. Es ist sohin durchaus denkbar, dass ein Mitarbeiter, der

personenbezogene Daten nicht weisungskonform verarbeitet, obwohl eine Art 29 entsprechende Weisung erteilt wurde, auch arbeitsrechtliche Konsequenzen zu befürchten hat.

4.3. Strafrechtliche Konsequenzen

Schlussendlich könnte der Mitarbeiter infolge eines Datenschutzverstoßes auch strafrechtlich zur Verantwortung gezogen werden, nämlich einerseits bei Verwirklichung des § 63 DSG (Datenverarbeitung in Gewinn- oder Schädigungsabsicht) und andererseits im Rahmen des StGB.[56] Zu erwähnen ist außerdem, dass jedes strafrechtliche Vergehen oder Verbrechen, das unter Missbrauch personenbezogener Daten begangen wird, um das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird, dem besonderen Erschwerungsgrund des § 33 Abs 1 Z 8 StGB unterliegt.

5. Fazit

Die datenschutzrechtliche Weisung spielt eine zentrale Rolle im Bereich der Auftragsverarbeitung sowie bei Verarbeitungen im Beschäftigungskontext. Obwohl durch das Anwendungsfeld im Beschäftigtenkontext der Schluss nahe liegt, dass es sich auch bei der datenschutzrechtlichen Weisung um eine arbeitsrechtliche Weisung im engeren Sinn handeln könnte, ist der Begriff der Weisung dennoch originär auszulegen. Die Charakteristik der Weisung im Datenschutzrecht ist nach wie vor weitgehend unklar. Führen Mitarbeiter für ihren Arbeitgeber Verarbeitungstätigkeiten von personenbezogenen Daten durch, trifft zunächst den Arbeitgeber die Pflicht nach Art 29 eine Weisung zu erteilen. Dabei wirkt sich die Weisung als Zurechnungsinstrument unmittelbar auf die Rollenverteilung, aber auch als legitimierendes Verbindungselement auf die Rechtmäßigkeit der Verarbeitung personenbezogener Daten aus. Für Mitarbeiter ist das Vorliegen einer Weisung die Rechtfertigung dafür, personenbezogene Daten verarbeiten zu dürfen und dennoch nicht Verantwortlicher dieser Datenverarbeitung zu sein. Darüber hinaus muss die Weisung auch im Kontext der Datensicherheit zusammen mit den dazugehörigen TOM betrachtet werden. Daher ist es, obwohl Weisungen auch mündlich erteilt werden können, notwendig, diese zu dokumentieren. Auch aus dem Arbeitsvertrag könnte sich schon eine Beauftragung zur Datenverarbeitung mit Weisungscharakter ergeben, sofern diese ähnlich wie in einem Auftragsverarbeitungsvertrag inhaltlich ausreichend umschrieben ist. Hinsichtlich der konkreten Inhalts- und Formerfordernisse von Weisungen ist festzuhalten, dass noch vieles unklar ist. Art 29 bietet in seiner derzeitigen Ausgestaltung in diesen Fragestellungen wenig Hilfestellung. Betrachtet man die Weisung als Teil der Rechtfertigungskette, wird diese jedenfalls einen gewissen Detailgrad in Bezug auf die Umstände der angewiesenen Verarbeitung und möglicherweise sogar zu treffende TOM enthalten müssen. Erteilt der Verantwortliche keine oder eine ungeeignete Weisung und verarbeitet ein Mitarbeiter daher unrechtmäßig personenbezogene Daten, verstößt der Arbeitgeber gegen Art 29 bzw Art 32 Abs 4 iVm Art 24 Abs 1. Aufseiten des Mitarbeiters ist die Verarbeitung als rechtswidrig einzustufen, wenn keine Weisung des Verantwortlichen vorliegt. Unkonkrete oder nicht offensichtlich rechtswidrige Weisungen des Verantwortlichen können dem Mitarbeiter nicht angelastet werden. Im Falle eines Datenschutzverstoßes, der dem Mitarbeiter zuzurechnen ist, drohen neben datenschutzrechtlichen Konsequenzen auch mögliche schadenersatzrechtliche sowie arbeitsrechtliche oder strafrechtliche Folgen. Auch aus diesem Grund ist es ebenso im Interesse des Mitarbeiters, eine konkrete und dokumentierte Weisung zu verlangen und diese im Arbeitsprozess auch einzuhalten.

---

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung), ABl L 2016/119, 1 idF L 2016/314, 72 sowie L 2018/127, 2 und L 2021/074, 35.

[2] Zudem spricht ErwGr 86 von "Weisung" in der deutschen bzw "guidance" in der englischen Sprachfassung und ErwGr 140 von "Anweisung" bzw "under the instructions of".

[3] Vgl bspw den "Health and Safety at Work etc. Act 1974" der UK abrufbar unter <legislation.gov.uk/ukpga/1974/37/pdfs/ukpga_19740037_en.pdf > (15. 1. 2022).

[4] Siehe zum Begriff des "Mitarbeiters" in der DS-GVO ausführlich *Gosch/Leitinger*, Die Zurechnung unterstellter Personen zum Verantwortlichen mit besonderem Fokus auf das Verhältnis zwischen "Mitarbeiter" und "Arbeitgeber", jusIT 2021/46, 115 (116 f).

[5] *Gosch/Leitinger*, jusIT 2021/46, 115 (117 ff).

[6] Martini in Paal/Pauly (Hrsg), DS-GVO und BDSG3 Art 29 Rz 19 (2021).

[7] <duden.de/rechtschreibung/Weisung> (15. 1. 2022).

[8] So ist die Weisungsgebundenheit von Mitarbeitern nach der stRsp des OGH etwa in § 27 AngG, §§ 1151 und 1153 ABGB enthalten (vgl RIS-Justiz RS0021472 und RS0029787).

[9] § 51 StGB.

[10] So etwa die Weisung nach § 9 VStG oder § 44 BDG.

[11] § 115 UGB.

[12] So setzte sich bereits 1970 beim 4. Österreichischen Juristentag die arbeitsrechtliche Abteilung mit der Weisung des Arbeitsgebers auseinander, die Ergebnisse wurden in Form eines Aufsatzes publiziert: *Migsch*, Einige Gedanken zum Weisungsrecht des Arbeitgebers, ZAS 1970, 83.

[13] EuGH 11. 11. 2010, C-232/09 (Danosa) Rz 40.

[14] Weiterführend *Wachter*, Grenzen des Weisungsrechts in Bezug auf Art und Ort der Tätigkeit, DRdA 2001, 495.

[15] Vgl ausführlich Mosler in Mosler/Müller/Pfeil (Hrsg), Der SV-Komm § 4 ASVG Rz 104 ff (Stand 1. 7. 2020).

[16] Rebhahn in Neumayr/Reissner (Hrsg), ZellKomm3 § 1151 ABGB Rz 33 (Stand 1. 1. 2018).

[17] Nach stRsp des EuGH sind bei der Auslegung einer Vorschrift des Unionsrechts nicht nur deren Wortlaut, sondern auch ihr Zusammenhang und die Ziele zu berücksichtigen, die mit der Regelung, zu der sie gehört (wie für die hier relevante Untersuchung die DS-GVO), verfolgt werden; siehe dazu EuGH 19. 7. 2012, C33/11 (A Oy) Rz 27.

[18] Siehe sogar zur Einbeziehung juristischer Personen *Bergauer*, Die Rollenverteilung nach der DS-GVO - zugleich Überlegungen zu einem Übermittlungsprivileg im Konzern innerhalb enger Grenzen, jusIT 2018/24, 60 (64).

[19] Gleiches gilt auch für andere Materien, in denen der Weisungsbegriff verwendet wird, wie etwa im öffentlichen Recht oder Strafrecht.

[20] Hartung in Kühling/Buchner (Hrsg), DS-GVO und BDSG3 Art 29 Rz 8 (2020); *Gosch/Leitinger*, jusIT 2021/46, 115 (117 ff).

[21] Wie sich die Weisung auf die Rollenverteilung auswirkt, wurde im ersten Beitrag dieser Reihe unter "4. Die Rolle und Verantwortlichkeit des "Mitarbeiters" in der DS-GVO" bereits untersucht.

[22] Hartung in Kühling/Buchner3 Art 29 Rz 8.

[23] Zusammenfassung des derzeitigen Diskussionstands bei *Gstöttner*, Der datenschutzrechtliche Auftragsverarbeiter - Eine Analyse des Begriffs, der Pflichten und der Haftung (2021) 30 ff.

[24] Martini in Paal/Pauly3 Art 29 Rz 18.

[25] Martini in Paal/Pauly3 Art 29 Rz 7.

[26] Art 5 Abs 1 "Personenbezogene Daten müssen […]".

[27] BVwG 2. 6. 2021, W211 2223512-2.

[28] Siehe zu dieser Thematik *Gosch*, Die Verarbeitung besonderer Kategorien personenbezogener Daten (2019) 63 f; siehe auch *Bergauer*, Rezension: Christian Marzi und Angelika Pallwein-Prettner, Datenschutzrecht auf Basis der DS-GVO, jusIT 2018/47, 122 (123); *Bergauer*, Zur Rechtmäßigkeit der (Weiter-)Verarbeitung personenbezogener Daten nach der DS-GVO, jusIT 2018/83, 232 (233); *Jahnel/Pallwein-Prettner*, Datenschutzrecht[3] (2021) 85.

[29] *Bergauer* in Jahnel (Hrsg), Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 24 Z 7 und 9 (2021).

[30] Martini in Paal/Pauly3 Art 29 Rz 19; Bertermann in Ehmann/Selmayr (Hrsg), DS-GVO2 Art 29 Rz 4 (2018).

[31] Hartung in Kühling/Buchner3 Art 29 Rz 16; Bertermann in Ehmann/Selmayr2 Art 29 Rz 4; *Spoerr* in Wolff/Brink (Hrsg), Datenschutzrecht Art 29 Rz 15 (Stand 1. 11. 2021).

[32] *Jahnel* (Hrsg), Kommentar zur Datenschutz-Grundverordnung (DSGVO) Art 28 Rz 20 (2021).

[33] *Gosch/Leitinger*, jusIT 2021/46, 115 (119).

[34] Bertermann in Ehmann/Selmayr2 Art 29 Rz 4; *Spoerr* in Wolff/Brink Art 29 Rz 15.

[35] Hartung in Kühling/Buchner3 Art 29 Rz 16; so auch die Empfehlung von Bertermann in Ehmann/Selmayr2 Art 29 Rz 4.

[36] Vgl *Barth/Dokalik/Potyka*, ABGB (MTK) 26 § 7 ABGB Anm 1 (Stand 1. 8. 2018).

[37] Hartung in Kühling/Buchner3 Art 29 Rz 15 verweist hierzu auf *Lutz/Gabel* in Taeger/Gabel (Hrsg), DSGVO - BDSG - TTDSG[4] Art 29 Rz 12 (2022).

[38] Bertermann in Ehmann/Selmayr2 Art 29 Rz 4; Martini in Paal/Pauly3 Art 29 Rz 18.

[39] *Datenschutzkonferenz*, Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO (Kurzpapier 19) vom 29. 5. 2018, 2.

[40] Hartung in Kühling/Buchner3 Art 29 Rz 15.

[41] Martini in Paal/Pauly3 Art 29 Rz 18; *Spoerr* in Wolff/Brink Art 29 Rz 14.

[42] Martini in Paal/Pauly3 Art 29 Rz 18; *Petri* in Simitis/Hornung/Spiecker (Hrsg), Datenschutzrecht Art 29 Rz 14 (2019); *Spoerr* in Wolff/Brink Art 29 Rz 14.

[43] Martini in Paal/Pauly3 Art 29 Rz 18 verweist diesbezüglich auf Hartung in Kühling/Buchner3 Art 29 Rz 15, der auf Bertermann in Ehmann/Selmayr2 Art 29 Rz 4 verweist, welcher wiederum ohne weitere Begründung auf Martini in Paal/Pauly3 Art 29 Rz 18 verweist.

[44] EuGH 9. 7. 1981, C-169/80 (Gondrand und Garancini) Rz 17; EuGH 22. 2. 1984, C-70/83 (Kloppenburg) Rz 11.

[45] EGMR 4. 5. 2000, 28341/95 (Rotaru / Rumänien) Rz 56.

[46] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz - DSG), BGBl I 165/1999 idF I 148/2021.

[47] Österreich hat der Europäischen Kommission die für die Verarbeitung von Beschäftigtendaten relevanten Bestimmungen gemeldet (siehe dazu BMöDS-920.777/0083-III/1/2018 bzw BMASGK-462.501/0012VII/B/8/2018) und durch diese Notifizierung die darin genannten gesetzlichen Bestimmungen als datenschutzspezifische Vorschriften zum Beschäftigtendatenschutz iSv Art 88 gemacht: *Bergauer* in Jahnel, DSGVO Art 88 Rz 16 f.

[48] *Kunnert* in Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl (Hrsg), DSG Datenschutzgesetz Kommentar § 1 Rz 3 (2018).

[49] IdS jüngst OLG Dresden 30. 11. 2021, 4 U 1158/21; ähnl argumentiert etwa *Goricnik* iZm der datenschutzrechtlichen Verantwortlichkeit des Betriebsrats, sofern einzelne BR-Mitglieder neben der/den Datenverarbeitung(en) der BR-Körperschaft oder des BRF Daten für ihre eigenen (zB fraktionellen) Zwecke - datenschutzrechtlich befugt oder unbefugt - verarbeiten, werden sie selbst zu eigenständigen "Verantwortlichen" iSd Art 4 Z 7 und unterliegen persönlich den in der DS-GVO normierten Pflichten; *Goricnik* in Knyrim (Hrsg), DatKomm Art 88 DSGVO Rz 102 (Stand 7. 5. 2020, rdb.at).

[50] IdS auch *Jahnel*, DSGVO Art 29 Z 6.

[51] Martini in Paal/Pauly3 Art 29 Rz 22a.

[52] Martini in Paal/Pauly3 Art 29 Rz 22; Hartung in Kühling/Buchner3 Art 29 Rz 18.

[53] Nämlich *"(1) ob der Zuspruch von Schadenersatz nach Art 82 DS-GVO neben einer Verletzung von Bestimmungen der DSGVO auch erfordert, dass der Kläger einen Schaden erlitten hat oder ob bereits die Verletzung von Bestimmungen der DSGVO als solche für die Zuerkennung von Schadenersatz ausreicht sowie (2) ob für die Bemessung des Schadenersatzes neben den Grundsätzen der Effektivität und Äquivalenz weitere Vorgaben des Unionsrechts bestehen und (3) ob eine Voraussetzung für den Zuspruch immateriellen Schadens jene ist, dass eine Konsequenz oder Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt, die über den durch die Rechtsverletzung hervorgerufenen Ärger hinausgeht".* OGH 15. 4. 2021, 6 Ob 35/21x.

[54] So etwa *Spitzer*, Schadenersatz für Datenschutzverletzungen. Zugleich Bemerkungen zum Diskussionsstand zum Ersatz ideeller Schäden, ÖJZ 2019/76, 629; *Kerschbaumer-Gugu*, Schadenersatz von Datenschutzverletzungen. Die Haftung für Datenschutzverletzungen nach Art 82 DSGVO, § 29 DSG und ABGB (2019).

[55] VwGH 12. 5. 2020, Ro 2019/04/0229.

[56] So stehen unter anderem etwa der widerrechtliche Zugriff auf ein Computersystem gem § 118a StGB, das missbräuchliche Abfangen von Daten nach § 119a StGB, eine Datenschädigung iSd § 126a StGB, Delikte im Zusammenhang mit der Störung oder dem Missbrauch von Computerprogrammen oder -systemen gem §§ 126b und 126c StGB oder betrügerischer Datenverarbeitungsmissbrauch nach § 148a StGB unter Strafe.