ZAP

Zeitschrift für die Anwaltspraxis

10 | 2018

11. Mai
30. Jahrgang
ISSN 0936-7292

Inklusive ZAP App!

Details unter: www.zap-zeitschrift.de/App

AUS DEM INHALT

ZAP

In Zusammenarbeit mit der Bundesrechtsanwaltskammer

Individualarbeitsrecht

Datenschutzgrundverordnung: Beschäftigtendatenschutz in einer Arbeitswelt 4.0

Von Rechtsanwalt und Fachanwalt für Arbeitsrecht Dr. Joachim Holthausen, Köln

Inhalt

I. Einleitung

„*Wer nicht für seine Privatsphäre kämpft, wird sie verlieren*" und „*Technologie bedarf der leitenden Hand des Menschen, um Positives zu bewirken*" sind zwei Kernaussagen von Ex-Google-Chairman Eric Schmidt und des Politikberaters und Managers Jared Cohen in ihrem Buch „Die Vernetzung der Welt". Weite Teile der digitalen Arbeitswelt (Arbeit 4.0) sind bislang kaum reguliert und bieten wenig Schutz vor Überwachung und Datenmissbrauch. Die bereits im Mai 2016 in Kraft getretene **Datenschutz-Grundverordnung** (kurz: DSGVO) findet **ab** dem **25.5.2018 Anwendung**. Sie stellt eine bedeutende Zäsur im Datenschutzrecht dar. Mit ihr legt der europäische Gesetzgeber einen neuen Rechtsrahmen fest, der das Datenschutzrecht der EU-Mitgliedstaaten vereinheitlichen soll. Gleichfalls soll das modernisierte Datenschutzrecht der DSGVO im Zusammenspiel mit dem **reformierten deutschen Bundesdatenschutzgesetz** (kurz: BDSG n.F.) zeitgemäße Antworten – u.a. auf die Herausforderungen der Digitalisierung in einer Arbeitswelt 4.0 – geben.

II. Rechtscharakter DSGVO/Inkrafttreten

Die DSGVO, eine Verordnung der Europäischen Union, Verordnung (EU) 2016/679 (kurz: Verordnung EU), ist ein Rechtsakt der Europäischen Union mit allgemeiner Gültigkeit und **unmittelbarer Wirksamkeit in den Mitgliedstaaten** (Art. 288 AEUV, Art. 249 EGV a.F.). Die Verordnung 2016/679 ist

Teil des Sekundärrechts der Union und genießt als Unionsrecht Anwendungsvorrang vor dem nationalen Recht und somit auch vor dem BDSG n.F. Die DSGVO ist bereits am 24.5.2016 in Kraft getreten, **gilt** allerdings erst **ab** dem **25.5.2018** und löst zu diesem Zeitpunkt die EU-Datenschutzrichtlinie (95/46/EG) ab, auf der das bisherige Bundesdatenschutzgesetz (BDSG a.F.) beruht.

III. Datenschutzrechtliche Grundbegriffe

1. Personenbezogene Daten, besondere Kategorien

Nach Art. 4 Abs. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder **identifizierbare natürliche Person beziehen**. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Besondere Kategorien personenbezogener Daten (u.a. die Gewerkschaftszugehörigkeit, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, wie z.B. Arbeitsunfähigkeitsbescheinigungen, ärztliche Atteste und Gutachten, Bescheide über einen Grad der Behinderung [GdB] etc.), die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, **sind bei der Verarbeitung besonders geschützt**. Ihre Verarbeitung ist nach Art. 9 Abs. 1 DSGVO untersagt, wobei Art. 9 Abs. 2 DSGVO die Ausnahmen zu diesem Verbot regelt. Der Grund für den besonderen Schutz ist, dass im Zusammenhang mit der Verarbeitung besonderer Kategorien personenbezogener (sensibler) Daten erhebliche **Risiken für die Grundrechte und Grundfreiheiten** auftreten können (vgl. die Erwägungsgründe 46, 51–56 zur DSGVO und §§ 22, 24, 26–28 BDSG n.F.).

Auch die Verarbeitung besonderer Kategorien personenbezogener Daten kann grundsätzlich für einen oder mehrere festgelegte Zwecke (**Datenzweckbindung**) durch eine **ausdrückliche Einwilligung** der betroffenen Person gedeckt sein (Verbot mit Erlaubnisvorbehalt), es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Art. 9 Abs. 1 DSGVO durch die Einwilligung der betroffenen Person nicht aufgehoben werden (Art. 9 Abs. 2 lit. a DSGVO).

Nach § 26 Abs. 3 BDSG n.F. ist abweichend von Art. 9 Abs. 1 DSGVO die **Verarbeitung** besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO **für Zwecke des Beschäftigungsverhältnisses zulässig**, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Praxishinweis:
§ 26 Abs. 2 BDSG n.F. (Freiwilligkeit der Einwilligung) gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Abs. 2 BDSG n.F. (zulässige Verarbeitung durch öffentliche Stellen aus Gründen eines erheblichen öffentlichen Interesses, zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit etc.) gilt entsprechend.

2. Verarbeitung von Daten

Der **Begriff** der Verarbeitung von Daten ist nach der DSGVO denkbar **weit gefasst**. Nach Art. 4 Nr. 2 DSGVO bezeichnet „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung,

Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

IV. Zusammenspiel von DSGVO und Erwägungsgründen

Die Artikel der DSGVO wurden in Erwägung von Gründen erlassen. Diese Erwägungsgründe sind ein elementares Instrument zum richtigen Verständnis und für die **Anwendung der DSGVO** (die finalen Erwägungsgründe vom 27.4.2016 können unter *https://dsgvo-gesetz.de/erwaegungsgruende* im Internet abgerufen werden). Beispielhaft sind die Erwägungsgründe 1, 2 und 6 zu nennen, welche den Ansatz und die Zielrichtung der DSGVO anschaulich verdeutlichen:

> **Erwägungsgrund 1: Datenschutz als Grundrecht**
> Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union sowie Art. 16 Abs. 1 AEUV hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> **Erwägungsgrund 2: Wahrung der Grundrechte**
> Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Die DSGVO soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.
>
> **Erwägungsgrund 6: Hohes Datenschutzniveau trotz Zunahme des Datenaustauschs**
> Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein hohes Datenschutzniveau zu gewährleisten ist.

V. Datenschutzrechtliche Grundsätze für die Verarbeitung personenbezogener Daten

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a DSGVO)

Der Grundsatz der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz fordert, dass personenbezogene Daten auf **rechtmäßige** Weise, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise verarbeitet** werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten **leicht zugänglich und verständlich** und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die **Identität des Verantwortlichen** und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und **Auskunft** darüber zu erhalten, welche sie betreffenden personenbezogenen Daten verarbeitet werden. Natürliche Personen sollten **über** die **Risiken**, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können (vgl. Erwägungsgrund 39).

2. Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO)

Der Grundsatz der Zweckbindung fordert, dass personenbezogene Daten für festgelegte, eindeutige und **legitime Zwecke** erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise

weiterverarbeitet werden dürfen. Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gem. Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken. Die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, müssen eindeutig und **rechtmäßig** sein sowie zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen (vgl. Erwägungsgrund 39). Eine zweckfreie Datenerhebung „auf Vorrat" ist unzulässig (Wortmann ArbRB 2018, 83 f.).

Praxishinweis:
Zur einer nachträglichen **Zweckänderung** geben Art. 6 Abs. 4 DSGVO i.V.m. Erwägungsgrund 50 den europäischen Rechtsrahmen vor. Danach gilt u.a.: Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung u.a. prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen (Stichwort: **vergleichbarer Zweck**, vgl. Wortmann ArbRB 2018, 83).

3. Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)
Der Grundsatz der Datenminimierung fordert, dass personenbezogene Daten dem Zweck **angemessen**, **erheblich** und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen (Stichwort: **Datensparsamkeit**).

4. Richtigkeit (Art. 5 Abs. 1 lit. d DSGVO)
Der Grundsatz der Richtigkeit fordert, dass personenbezogene Daten **sachlich richtig** und erforderlichenfalls auf dem **neuesten Stand** sind. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

5. Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)
Der Grundsatz der Speicherbegrenzung fordert, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen **nur so lange ermöglicht, wie** es für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO verarbeitet werden.

Praxishinweis:
Die Grundsätze der Datenminimierung und Speicherbegrenzung erfordern bei einem regelkonformen Verständnis die beständige bzw. **turnusmäßige Prüfung** der personenbezogenen Datenbestände darauf, ob unnötige Daten oder Daten in unnötiger Weise wider die Zweckbindung verarbeitet werden. Auch die Löschung überflüssiger Daten wird von diesen Grundsätzen umfasst, was in Bezug auf den Beschäftigtendatenschutz zur **Überprüfung der Personalakten** (analoge Akte und E-Akte) verpflichtet. Personalakten ausgeschiedener Arbeitnehmer sind auszudünnen bzw. bei Fortfall der Zweckbindung zu entsorgen, was **Löschroutinen** in den Unternehmen **erfordert** (vgl. Wortmann ArbRB 2018, 83 ff.).

6. Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO)

Der Grundsatz der Integrität und Vertraulichkeit fordert, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten **gewährleistet**, einschließlich **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

VI. Beschäftigtendatenschutz (§ 26 BDSG n.F.)

Der Beschäftigtendatenschutz richtet sich zunächst nach den Regelungen der DSGVO, die für jedes Rechtsverhältnis gelten. Nach Art. 88 Abs. 1 DSGVO **können die Mitgliedstaaten** durch **Rechtsvorschriften oder** durch Kollektivvereinbarungen **spezifischere Vorschriften** zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses **vorsehen**. Weitere Erläuterungen zur Einführung eines Beschäftigtendatenschutzes durch die Mitgliedstaaten enthält Erwägungsgrund 155 der DSGVO. Der deutsche Gesetzgeber hat von dieser **Öffnungsklausel** mit § 26 BDSG n.F. Gebrauch gemacht.

Hinweis:
Für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes und der Länder – einschließlich der Kommunen – gelten besondere bundes- und landesspezifische Regelungen (z.B. beamtenrechtliche Vorschriften). Die Regelungen des § 26 BDSG n.F. finden insoweit keine Anwendung (vgl. DSK, Kurzpapier Nr. 14 zum Beschäftigtendatenschutz).

§ 26 BDSG n.F., der zum 25.5.2018 gleichzeitig mit dem Gültigwerden der DSGVO in Kraft tritt, greift erkennbar auf die bisherige Regelung des § 32 BDSG a.F. zurück. Die Neuregelung ist jedoch deutlich umfangreicher und regelt mehr Aspekte des Beschäftigtendatenschutzes als das bislang in Deutschland geltende Recht. Wie § 32 Abs. 1 BDSG a.F. regelt § 26 Abs. 1 BDSG n.F., zu welchen Zwecken und **unter welchen Voraussetzungen personenbezogene Daten** vor, im und nach dem Beschäftigungsverhältnis **verarbeitet werden dürfen**. Nach der Gesetzesbegründung sind bei der Erforderlichkeitsprüfung entsprechend den bisherigen Anforderungen der Rechtsprechung zu § 32 BDSG die widerstreitenden **Grundrechtspositionen** zur Herstellung praktischer Konkordanz gegeneinander **abzuwägen**.

Personenbezogene Daten von Beschäftigten dürfen **für Zwecke des Beschäftigungsverhältnisses verarbeitet** werden, wenn dies für die Entscheidung über die Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses erforderlich ist (§ 26 Abs. 1 S. 1 BDSG n.F.). Diese Regelung entspricht weitestgehend § 32 Abs. 1 S. 1 BDSG a.F. Die Voraussetzungen für die Verarbeitung von personenbezogenen Daten zur **Aufdeckung von Straftaten von Beschäftigten** finden sich nunmehr in § 26 Abs. 1 S. 2 BDSG n.F. Sie decken sich mit denen des § 32 Abs. 1 S. 2 BDSG a.F. Angesichts des Wortlauts von § 26 BDSG n.F. bleibt die Frage, ob Daten auch zur Aufklärung konkreter Verdachtsmomente in Bezug auf schwerwiegende Pflichtverletzungen erhoben werden dürfen, wenn diese nicht die Grenze zur Straftat überschreiten (sog. **Sperrwirkung des Datenschutzrechts**). Diese Rechtsfrage hat grundlegende Bedeutung für Compliance-Kontrollen und Internal-Investigations. Der Zweite Senat des BAG hat insoweit mit seiner Entscheidung vom 29.6.2017 (2 AZR 597/16, ZAP EN-Nr. 682/2017) für Rechtssicherheit gesorgt, indem er die von der Vorinstanz (LAG Baden-Württemberg, Urt. v. 20.7.2015 – 4 Sa 61/15) angenommene Sperrwirkung verneint. Er führt hierzu u.a. aus (*Anm.: Zitate teilweise eingekürzt*):

„Nach § 32 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses u.a. dann erhoben, verarbeitet oder genutzt werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist. Zur Durchführung gehört die Kontrolle, ob der Arbeitnehmer seinen Pflichten nachkommt, zur Beendigung im Sinne der Kündigungsvorbereitung die Aufdeckung einer Pflichtverletzung, die die Kündigung des Arbeitsverhältnisses rechtfertigen kann. Der Wortlaut des § 32 Abs. 1 S. 1 BDSG enthält keine Einschränkung, es müsse der Verdacht einer im Beschäftigungsverhältnis verübten Straftat bestehen. Sofern nach § 32 Abs. 1 S. 1 oder S. 2 BDSG zulässig erhobene Daten den Verdacht einer Pflichtverletzung begründen, dürfen sie für die Zwecke und unter den Voraussetzungen des § 32 Abs. 1 S. 1 BDSG auch verarbeitet und genutzt werden (vgl. BAG, Urt. v. 20.10.2016 – 2 AZR 395/15, Rn 40; BAG, Urt. v. 22.9.2016 – 2 AZR 848/15, Rn 37 f.). Der Begriff der Beendigung umfasst dabei die Abwicklung eines Beschäftigungsverhältnisses (BT-Drucks 16/13657, S. 21). Der Arbeitgeber darf deshalb alle Daten speichern und verwenden, die er zur Erfüllung der ihm obliegenden Darlegungs- und Beweislast in einem potentiellen Kündigungsschutzprozess benötigt.

Eine „Sperrwirkung" des § 32 Abs. 1 S. 2 BDSG gegenüber der Erlaubnisnorm in Satz 1 der Bestimmung in Fällen, in denen der Arbeitgeber „nur" einen – auf Tatsachen gestützten und ausreichend konkreten – Verdacht einer schwerwiegenden Pflichtverletzung des Arbeitnehmers hat, nicht aber den einer im Beschäftigungsverhältnis begangenen Straftat, lässt sich weder aus dem Wortlaut von § 32 Abs. 1 BDSG, noch seiner Systematik oder seinem Sinn und Zweck bzw. der Gesetzeshistorie ableiten.

Eine Datenerhebung zur Aufklärung des (konkreten) Verdachts einer schweren Pflichtverletzung erfolgt „für Zwecke des Beschäftigungsverhältnisses" i.S.d. § 32 Abs. 1 S. 1 BDSG. Die Bestimmung kodifiziert ebenso wie Satz 2 der Norm die von der Rechtsprechung aus dem verfassungsrechtlich geschützten allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abgeleiteten allgemeinen Grundsätze zum Datenschutz im Beschäftigungsverhältnis (BAG, Urt. v. 17.11.2016 – 2 AZR 730/15, Rn 29; BT-Drucks 16/13657, S. 21). Dabei nimmt die Gesetzesbegründung zur Konkretisierung des Maßstabs der Erforderlichkeit einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Durchführung oder Beendigung eines Beschäftigungsverhältnisses auf die Entscheidungen des BAG vom 22.10.1986 (5 AZR 660/85) und 7.9.1995 (8 AZR 828/93) Bezug. Diesen zufolge dürfe sich der Arbeitgeber bei seinen Beschäftigten nicht nur über Umstände informieren oder Daten verwenden, um seine vertraglichen Pflichten ihnen gegenüber erfüllen zu können, wie z.B. Pflichten im Zusammenhang mit der Personalverwaltung, Lohn- und Gehaltsabrechnung, sondern auch, um seine im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses bestehenden Rechte wahrzunehmen, z.B. durch Ausübung des Weisungsrechts oder durch Kontrollen der Leistung oder des Verhaltens des Beschäftigten (BT-Drucks 16/13657, a.a.O.). Voraussetzung ist ein berechtigtes Interesse des Arbeitgebers an der Datenerhebung, -verarbeitung oder -nutzung, das aus dem bestehenden Arbeitsverhältnis herrühren muss. Es muss ein Zusammenhang mit der Erfüllung der vom Arbeitnehmer geschuldeten vertraglichen Leistung, seiner sonstigen Pflichtenbindung oder mit der Pflichtenbindung des Arbeitgebers bestehen (BAG, Urt. v. 7.9.1995 – 8 AZR 828/93). Ein solcher Zusammenhang besteht auch dann, wenn der Arbeitgeber konkreten Verdachtsmomenten nachgeht, der Arbeitnehmer verletze in schwerwiegender Weise seine arbeitsvertraglichen Pflichten."

Die Verarbeitung von Daten zur Aufdeckung von Straftaten und schwerwiegenden Pflichtverletzungen darf erst erfolgen, wenn konkrete Anhaltspunkte für sie vorliegen. Eine **Verarbeitung „auf gut Glück" oder „auf Vorrat" ist unzulässig**. Zudem müssen sich die „Maßnahmen" gegen bestimmte, **konkreten Verdachtsmomenten** unterliegende Arbeitnehmer richten und dürfen nicht pauschal größere Gruppen von Arbeitnehmern rastern („keine Rasterfahndung").

Die in **§ 26 BDSG n.F.** getroffenen Bestimmungen zum Beschäftigtendatenschutz sind nach § 26 Abs. 7 BDSG n.F. **auch anzuwenden**, **wenn** personenbezogene Daten von Beschäftigten **verarbeitet** werden, **ohne dass sie** in einem Dateisystem gespeichert sind oder **gespeichert werden sollen**. Die Regelung stimmt mit dem bisherigen § 32 Abs. 2 BDSG a.F. überein. Nach § 26 Abs. 6 BDSG n.F. bleiben die Beteiligungsrechte der Interessenvertretungen der Beschäftigten unberührt. Diese Regelung ist mit der Regelung des § 32 Abs. 3 BDSG a.F. identisch.

VII. Einwilligung von Beschäftigten nach neuem Recht

Arbeitgeber, die Beschäftigtendaten bisher (nur) auf der Grundlage einer Einwilligung des betroffenen Arbeitnehmers verarbeiten, sehen sich dem Risiko ausgesetzt, dass der **Erlaubnistatbestand** der „Einwilligung" ab dem 25.5.2018 seine Gültigkeit und Rechtfertigungswirkung angesichts der neuen, schärferen Rechtsvorgaben der DSGVO und des ihm folgenden BDSG n.F. verliert.

Praxishinweis:
Von daher wird angeraten, alle datenschutzrechtlich relevanten Einwilligungen und Einwilligungstatbestände (insbesondere in Betriebsvereinbarungen) auf Gesetzeskonformität zu überprüfen und bei Bedarf (vgl. weiterführend Grimm ArbRB 2018, 78 ff.; Kamps/Bonanni ArbRB 2018, 50 ff.) anzupassen.

1. Gesetzliche Grundlagen

Gemäß Art. 4 Nr. 11 DSGVO muss jede Einwilligung **freiwillig**, **auf einen bestimmten Fall bezogen**, **informiert** und **unmissverständlich** erfolgen. Art. 7 DSGVO normiert die allgemeinen Bedingungen für die Einwilligung wie folgt (vgl. ergänzend hierzu auch die passenden Erwägungsgründe 32 – Einwilligung, 42 – Beweislast und Erfordernisse einer Einwilligung, 43 – Zwanglose Einwilligung, die die Anforderungen an eine wirksame Einwilligung beträchtlich verschärfen):

Art. 7 DSGVO – Bedingungen für die Einwilligung:

1. *Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.*
2. *Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.*
3. *Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.*
4. *Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.*

In Bezug auf die **Einwilligung als Erlaubnistatbestand** regelt § 26 Abs. 2 BDSG n.F. für die Verarbeitung von Beschäftigtendaten:

§ 26 BDSG – Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses:

Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

2. Problemstellung in der Praxis

Mit Blick auf diese aktuellen rechtlichen Vorgaben stellt sich die Einwilligung sowohl aus rechtlicher als auch aus praktischer Sicht als **schwierig zu handhabender Erlaubnistatbestand** dar, um eine fortlaufende gesetzeskonforme Verarbeitung von Daten im Sinne eines „Verbots mit Erlaubnisvorbehalt" sicherzustellen. **Pauschale Einwilligungen**, die erkennbar nicht auf der freien Entscheidung des Betroffenen fußen (Stichwort: klares Ungleichgewicht, Erwägungsgrund 43), keine rechtlichen oder wirtschaftlichen Vorteile erkennen lassen, die nicht den Zweck der Datenverarbeitung bestimmen und die zugleich nicht über die jederzeitige Widerrufsmöglichkeit für die Zukunft informieren, sind nicht das Geld für das Papier wert, auf dem sie stehen. Sie **sind unwirksam**. Auch „**Freiwilligkeit**" ist im konkreten Anwendungsfall ein problembehafteter Rechtsbegriff: Wann nutzt der Arbeitgeber eine wirtschaftliche oder tatsächliche Machtposition aus? In welchen Fällen „willigt der betroffene Arbeitnehmer ein", um eine Leistung, wie etwa einen Arbeitsplatz bzw. eine Beförderung zu erhalten? Kurzum stellt sich einzelfallbezogen immer die mit einem **Beurteilungsrisiko** versehene Frage nach „freier" oder „unfreier" Einwilligung. Nach Erwägungsgrund 43 etwa gilt die Einwilligung nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

In praktischer belegschaftsorientierter Hinsicht erfordern erteilte und verweigerte Einwilligungen zudem eine stete **Differenzierung** und entsprechende **Dokumentation** den einzelnen Arbeitnehmer betreffend. Durch die jederzeitige **Widerrufsmöglichkeit** wird die Handhabbarkeit des Erlaubnistatbestands Einwilligung dabei zusätzlich erschwert; zudem ist sie mit Blick auf **Zugangsprobleme**, Übermittlungs- und Erfassungsfehler potentiell stark fehlerbehaftet.

Checkliste:

Mit Blick auf die vorstehenden unbefriedigenden Befunde erweisen sich Einwilligungen für Standardprozesse im Bereich der **Personaladministration** als höchst arbeitsaufwendig und tendenziell ungeeignet, da sie eine belegschaftseinheitliche Behandlung und Bearbeitung nicht sicherstellen (vgl. Kamps/Bonanni ArbRB 2018, 50 f.). Im Sinne einer strukturierten Aufarbeitung des Themas Einwilligung und BDSG n.F. bietet sich ein **Vorgehen nach** folgenden **Sachthemen** an:

- ☐ Due Diligence, Bestandsaufnahme einwilligungsbezogener Tatbestände,
- ☐ Verzicht auf pauschale Einwilligungstatbestände wegen fehlender Datenzweckbindung und nicht gegebener Transparenz (Überprüfung von Arbeitsverträgen, Vertragsergänzungen und Nebenabreden),
- ☐ kritische Überprüfung der dokumentierten, inhaltlichen Freiwilligkeit der Einwilligung,
- ☐ Einhaltung der neuen, schärferen gesetzlichen Anforderungen, insbesondere hinsichtlich Zweckbindung,
- ☐ Ausweichen auf andere, alternative Rechtsgrundlagen bzw. Erlaubnistatbestände möglich?
  - ☐ Wenn ja: Umstellung, Information der Arbeitnehmer und restriktiver Einsatz des Instruments Einwilligung oder gänzlicher Verzicht auf diesen Erlaubnistatbestand.
  - ☐ Wenn nein: weiter mit nächstem Punkt.
- ☐ Beendigung/Einstellung rechtswidriger Verarbeitungsvorgänge,
- ☐ Löschung nicht rechtskonform verarbeiteter Daten,
- ☐ Einführung von regelmäßigen Terminen zur Prüfung des weiteren Vorliegens bzw. des Widerrufs von Einwilligungen (Compliance).

VIII. Datenschutz-Folgenabschätzung (§ 67 BDSG n.F.)

Hier stellt sich zunächst die Frage, was unter einer Datenschutz-Folgenabschätzung (engl. Privacy Impact Assessment, kurz: DSFA), wie sie Art. 35 DSGVO und § 67 BDSG n.F. vorschreiben, zu verstehen ist. Und welche **datenschutzrechtlichen bzw. finanziellen Sanktionsrisiken** gehen mit einer (nicht oder fehlerhaft durchgeführten) DSFA einher? § 67 Abs. 1 BDSG n.F. bestimmt: Hat eine Form der

Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche **vorab** eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen. Die Folgenabschätzung hat nach § 67 Abs. 4 BDSG n.F. den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und
4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

Ausgehend von den gesetzlichen Anforderungen ist eine DSFA sehr strukturiert anzugehen. Sie bedingt eine **systematische Beschreibung der Datenverarbeitungsvorgänge** und muss die **Zwecke der Verarbeitung bestimmen**. Dazu müssen technische und Organisationsprozesse, Verfahrensabläufe, IT-Systeme und Produkte sowie Datenflüsse und Systemgrenzen im Detail bewertet und auf Risiken analysiert werden. In der DSFA müssen die **Interessen an der Datenverarbeitung sowie** ihre **Erforderlichkeit** und **Verhältnismäßigkeit** nachvollziehbar beschrieben werden.

Hinweis:
Weil die DSFA am 25.5.2018 die Vorabkontrolle nach § 4d Abs. 5 BDSG a.F. ersetzt, könnte man auf den Gedanken verfallen, dass es sich bei ihr um „alten Wein in neuen Schläuchen" handelt. Das ist jedoch ein Trugschluss. Besonders die **ausführlichen Nachweis- und Dokumentationspflichten der Risikobewertung** sowie die **Meldepflichten** bringen viel Arbeit mit sich und bergen rechtlichen Zündstoff. Ist die Datenverarbeitung mit einem hohen Datenschutzrisiko verbunden, besteht eine Meldepflicht bei der zuständigen Aufsichtsbehörde, bevor mit der Verarbeitung der Daten begonnen wird.

In jedem Fall muss das **Datenschutzrisiko der Betroffenen** durch die Datenverarbeitung bestimmt werden. Eine **umfassende Risikoanalyse** bildet die Grundlage für die Beantwortung der Frage, ob für Datenverarbeitungsprozesse eine DSFA erforderlich ist (vgl. Erwägungsgrund 91). Die Risikobewertung (engl. risk assessment, vgl. Erwägungsgrund 77) kann mittels Verträgen und Dokumentationen zur Auftragsdatenverarbeitung sowie dem nach Art. 30 DSGVO zu führenden Verarbeitungsverzeichnis sowie in Ansehung der Minimierung der Risiken durch technische und organisatorische Maßnahmen (vgl. Erwägungsgrund 78, § 71 Abs. 2 BDSG n.F.) vorgenommen werden. Durch Pseudonymisierung und Verschlüsselung sowie über ISO-Zertifizierungen kann die geforderte Sicherheit der Datenverarbeitung erhöht werden (vgl. Art. 32 DSGVO).

Auf der Grundlage der DSGVO sind **Datenschutzrisiken** nach folgenden „**objektiven Kriterien**" zu ermitteln (vgl. Erwägungsgrund 76 und § 71 Abs. 1 BDSG n.F.):

- Eintrittswahrscheinlichkeit (Stichworte: Risiko-Quellen intern und extern, wie z.B. Hacker, IT-Administratoren, Wettbewerber, etc.),
- Verwendung neuer Technologien,
- mögliche Schwere des Schadens aufgrund von Verarbeitungsart, -umfang, -umständen und -zweck.

Wird nach der Risikoanalyse eine DSFA erforderlich, die dann immer noch ein hohes Datenschutz-Restrisiko der Verarbeitungsvorgänge identifiziert, ist die **zuständige Aufsichtsbehörde zu Rate zu ziehen** (vgl. Art. 36 DSGVO, Erwägungsgrund 84 und 94).

IX. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO, § 70 BDSG n.F.)

Der **Dokumentationsaufwand** nach Art. 30 DSGVO und § 70 BDSG n.F. ist beträchtlich und wird die betroffenen Unternehmen in der Praxis vor erhebliche Probleme stellen. Der Norm zufolge hat der Verantwortliche ein **Verzeichnis aller Kategorien von Verarbeitungstätigkeiten** zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,
2. die Zwecke der Verarbeitung,
3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. ggf. die Verwendung von Profiling,
6. ggf. die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7. Angaben über die Rechtsgrundlage der Verarbeitung,
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. eine allgemeine Beschreibung der technischen/organisatorischen Maßnahmen gem. § 64 BDSG n.F. (*Anm.: Anforderungen an die Sicherheit der Datenverarbeitung*).

X. Sanktionen

Mit Inkrafttreten der DSGVO besteht die Möglichkeit, **deutlich höhere Bußgelder** zu verhängen als es bisher der Fall war. Während nach dem bisherigen BDSG a.F. Bußgelder von bis zu 300.000 € möglich waren, beträgt die maximale Geldbuße im Rahmen von Art. 83 Abs. 5 DSGVO 20 Mio. Euro oder bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher der Beträge der höhere ist.

Hinweis:
Verzichtet man auf eine DSFA oder führt sie nicht korrekt durch, riskiert man ein Bußgeld von bis zu 10 Mio. Euro oder 2 % des gesamten weltweiten Jahresumsatzes des Unternehmens, je nachdem, welcher der Beträge der höhere ist (Art. 83 Abs. 4 lit. a DSGVO).

Kurzgefasst können nicht ernst genommene Pflichten und Verstöße im Bereich der DSGVO und des BDSG n.F. äußerst teuer kommen, was den Handlungsbedarf und den **Ernst der Lage bei Nichthandeln auf Arbeitgeberseite** unterstreicht.

XI. Ausblick

Die DSGVO und das ihr folgende BDSG n.F. können in ihrer Bedeutung nicht überschätzt werden, wie der Fall „Facebook und Cambridge Analytica" jüngst einmal mehr verdeutlicht. Mit der DSGVO und dem BDSG n.F. sollen die Grundrechte der Betroffenen, insbesondere das allgemeine Persönlichkeitsrecht (Art. 1 Abs. 1, 2 Abs. 1 GG) gestärkt und der Datensammelwut Einhalt geboten werden. Ob die gesetzlichen Bestimmungen mit dem Tempo des technischen Fortschritts und der zunehmenden Digitalisierung aller Lebensbereiche Schritt halten können und tragfähige sowie sachgerechte Lösungen in einer globalisierten Welt bieten, bleibt abzuwarten.

Angesichts der Komplexität der gesetzlichen Regelungen (DSGVO, Erwägungsgründe und BDSG n.F.), ihres Zusammenspiels und der fehlenden praktischen Erfahrung im Umgang mit dem neuen Rechtsumfeld ist sichergestellt, dass für die Anwaltschaft **Datenschutzrecht** im Allgemeinen und für die Fachanwälte für Arbeitsrecht der **Beschäftigtendatenschutz** im Besonderen ein „**echter Wachstumsmarkt**" mit hervorragenden Perspektiven ist. Die Lösung und Beherrschung rechtlicher und wirtschaftlicher Risiken verkauft sich der Erfahrung nach gut und stetig.