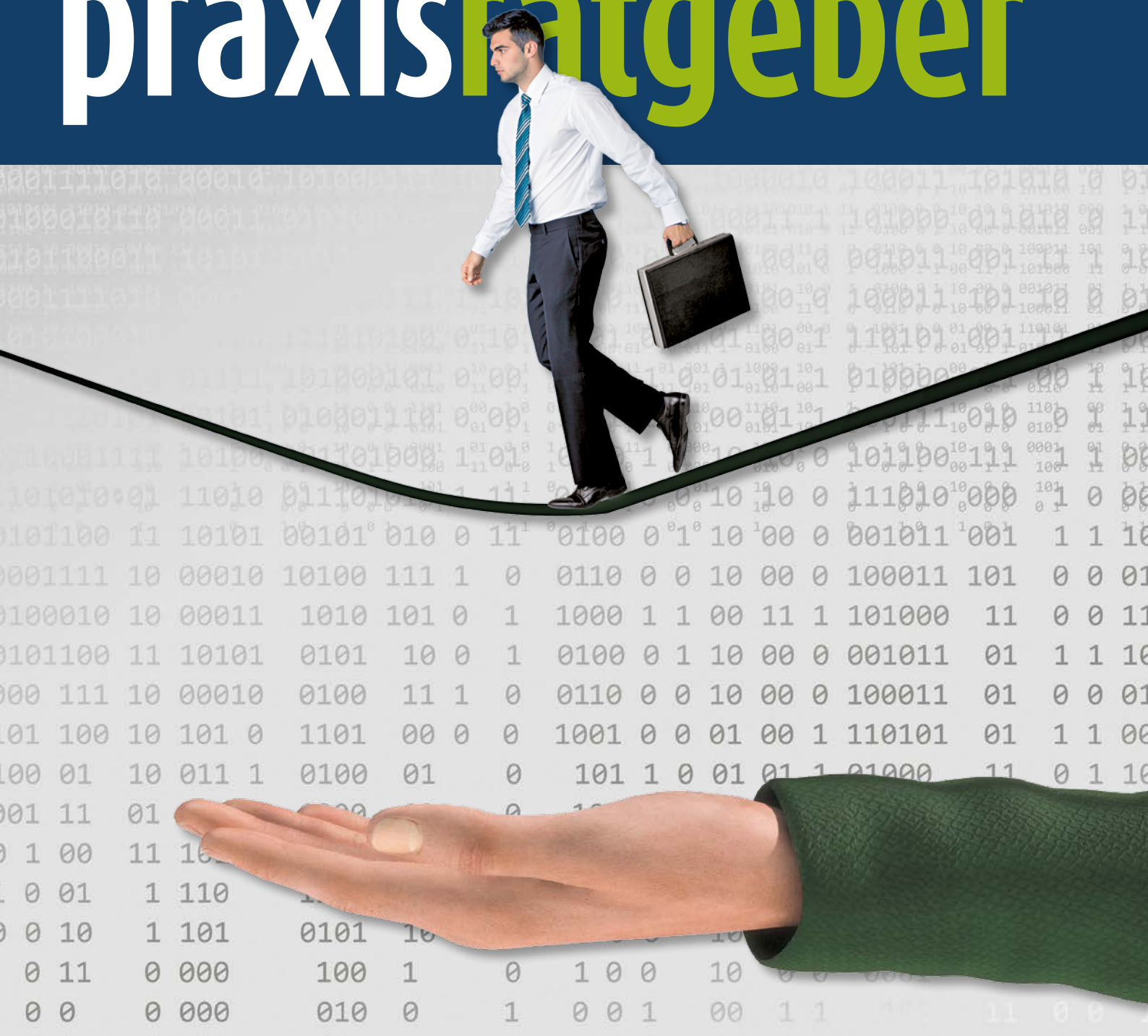
EINE SONDERVERÖFFENTLICHUNG VON personalmagazin UND unique

05.2018

praxisratgeber



Balanceakt Datenschutz

Wie Datenschutz bei der Arbeitnehmerüberlassung gelingt und wie Dienstleister dabei unterstützen

GRUNDSATZ Welche Rolle der Datenschutz bei der Arbeitnehmerüberlassung spielt S. 8

GRUNDLAGE Welche datenschutzrechtlichen Vorgaben Entleiher beachten müssen S. 12

GRUNDFRAGE Welche Kriterien für die Wahl des passenden Dienstleisters wichtig sind S. 16

unique

Ausgezeichnete Personaldienstleistungen

Kunden loben...

- ✓ die Auswahl der Kandidaten
- ✓ die Qualität der Dienstleistung
- ✓ die Fachkompetenz
- ✓ die rechtssicheren & praktikablen Lösungen
- ✓ den Service & die Betreuung
- ✓ das Preisleistungsverhältnis

Deutschlandweit an über 80 Standorten.

Unique Personalservice GmbH
info@unique-personal.de

www.unique-personal.de

Liebe Leserinnen und Leser,

„Wir sehen nun klarer“, meinte Gregor Thüsing, Professor für Arbeitsrecht, zum neuen Datenschutzrecht. Damit spielte er – im Interview mit dem Personalmagazin vor einigen Monaten – auf einige rechtliche Fragen an, die im Gesetz nun klargestellt sind. Den Praktikern, die dem Datenschutz nicht ganz so nahestehen, würde diese Aussage beim Blick in die DSGVO und das BDSG wohl schwerer fallen. Auf vielen Feldern sind die Vorgaben nämlich komplex und aufwendig. Unternehmen müssen nicht nur Prozesse anpassen, sondern vor allem das Bewusstsein für den sensiblen Umgang mit personenbezogenen Daten steigern, um kostspielige Verstöße zu vermeiden. In der Zeitarbeit gibt es zudem die spezielle Dreieckskonstellation, bei der datenschutzrechtlich auch der Entleiher als Verantwortlicher gilt. Mit unserem Partner Unique haben wir daher in diesem Praxisratgeber die datenschutzrechtlichen Besonderheiten bei der Arbeitnehmerüberlassung aufbereitet. Damit Sie am Heftende klarer sehen.

„Das Bewusstsein für den sensiblen Umgang mit personenbezogenen Daten muss in Unternehmen weiter zunehmen.“

Michael Miller, Redaktion Personalmagazin

Michael Miller, Redaktion Personalmagazin

INHALT

04 Vorbereitung ist alles
Weshalb Unternehmen die vorhandene Zeit gut nutzen und sich ausreichend auf das neue Datenschutzrecht vorbereiten müssen

06 „Datenschutz ist ein hohes Gut“
Der sensible Umgang mit personenbezogenen Daten muss zu den Kernkompetenzen von Personaldienstleistern zählen, erklärt Bénédicte Autem von Unique

08 Datenschutz in der Zeitarbeit
Welche datenschutzrechtlichen Besonderheiten sich im Zusammenhang mit der Arbeitnehmerüberlassung ergeben

12 Keine rein innere Angelegenheit
Das neue Datenschutzrecht nimmt nicht nur die Personaldienstleister in die Pflicht, auch die Einsatzunternehmen haben auf bestimmte Vorgaben zu achten

16 Den passenden Partner finden
Weil das neue Datenschutzrecht hohe Strafen bei Verstößen vorsieht, ist die Auswahl des richtigen Personaldienstleisters wichtig. Welche Kriterien dabei eine Rolle spielen

IMPRESSUM

VERLAG Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, D-79111 Freiburg
Kommanditgesellschaft, Sitz und Registergericht Freiburg, HRA 4408
Komplementäre: Haufe-Lexware Verwaltungs GmbH, Sitz und Registergericht Freiburg, HRB 5557; Martin Laqua
Beiratsvorsitzende: Andrea Haufe
Geschäftsführung: Isabel Blank, Sandra Dittert, Jörg Frey, Birte Hackenjos, Dominik Hartmann, Markus Reithwiesner, Joachim Rotzinger, Dr. Carsten Thies
Steuernummer: 06392/11008
USt-ID: DE 812398835

REDAKTION Reiner Straub (Herausgeber), Michael Miller

ABONNENTEN-SERVICE UND VERTRIEB
E-Mail: zeitschriften@haufe.de, Tel. 0800 5050445 (kostenlos)

ANZEIGEN Klaus Sturm, Tel. 0931 2791-733
E-Mail: klaus.sturm@haufe-lexware.com

GRAFIK/LAYOUT Kerstin Bertsch

DRUCK Senefelder Misset, Doetinchem

TITELBILD ra2studio/shutterstock.de; Orlando Florin Rosu/fotolia.de; vaslex/fotolia.de

VERBREITUNG Der Praxisratgeber ist eine gemeinsame Sonderveröffentlichung von Personalmagazin und der Unique Personalservice GmbH. Er ist der Ausgabe Mai 2018 des Personalmagazins beigeheftet. Aktuelle Informationen zu den Zeitschriften- und Online-Angeboten der Haufe-Gruppe finden Sie unter:
www.haufe.de/mediacenter

Vorbereitung ist alles

ÜBERSICHT. Pflichten, Prozesse, Pönale: Das Datenschutzrecht bringt für Unternehmen mehr Aufwand. Was die neuen Regeln – auch für die Zeitarbeitsbranche – bedeuten.

Von **Michael Miller** (Red.)

Eigentlich war – das sollte man meinen – ausreichend Zeit vorhanden, um die neuen Vorgaben der EU-Datenschutzgrundverordnung (DSGVO) umzusetzen. Schließlich sind die Vorschriften bereits seit 25. Mai 2016 in Kraft. Die DSGVO ersetzt die bisherige EU-Richtlinie aus dem Jahr 1995 und soll in ganz Europa einen einheitlichen Schutz im Umgang mit personenbezogenen Daten gewährleisten. Zudem gilt die DSGVO – im Unterschied zur Richtlinie – unmittelbar. Das bedeutet, der Einzelne kann sich direkt darauf berufen, es braucht also kein weiteres Gesetz aus Berlin, um die 99 Artikel der EU-Verordnung umzusetzen.

Zugegeben: Der deutsche Gesetzgeber hat sich mit den Neuerungen im Datenschutz mehr Zeit gelassen als der europäische. Schließlich hat der Bundestag das „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“ inklusive neuem Bundesdatenschutzgesetz (BDSG) erst Ende April 2017 beschlossen. Dennoch scheint es genug Zeit zur Vorbereitung zu sein. Schließlich sind beide Gesetze – die DSGVO und das neue BDSG – doch „erst“ ab 25. Mai 2018 anzuwenden.

Weil jedoch das neue Datenschutzrecht umfangreich und komplex ist, benötigen die Unternehmen diese lange Vorbereitungszeit tatsächlich – um Pflichten sicherzustellen und rechtssichere Prozesse zu implementieren. Zumal das Thema gerade bei kleineren Unternehmen nicht von Anfang an ganz oben auf der Agenda stand. Dass sich die Vorkehrungen lohnen, steht außer Frage: Die Rechtsfolgen bei Datenschutzverstößen haben es nämlich künftig – anders als bislang – in sich, orientieren sich die Bußgelder doch an Millionenbeträgen oder am globalen Umsatz (den Hinweis zu den Sanktionen lesen Sie auf Seite 9). Zudem ist für die Einhaltung der Grundsätze der DSGVO (lesen Sie dazu den Hinweis auf Seite 5) eine Beweislastumkehr vorgesehen (Art. 5 Abs.2). Das bedeutet: Das Unternehmen muss beweisen, einen vorgeworfenen Verstoß gegen das Datenschutzrecht nicht begangen zu haben. Dadurch wird entsprechenden Dokumentationen eine größere Bedeutung zukommen.

DSGVO nimmt Beschäftigte aus

Auch inhaltlich bringt das neue Datenschutzrecht Veränderungen – etwa im Bereich des Beschäftigtendatenschutzes. Andererseits bleibt gerade in dieser Teildisziplin eine grundlegende Revolution aus. Beim Blick speziell auf den Beschäftigtendatenschutz fällt sogar auf, dass dieses Feld in der DSGVO prinzipiell außen vor ist. Regelungen dazu werden vielmehr den nationalen Gesetzgebern überlassen (Art. 88 DSGVO). Jedoch sind natürlich die Grundsätze und das Schutzniveau der DSGVO zu achten.

Arbeitgeber müssen also dem Thema „Datenschutz“ eine hohe Aufmerksamkeit entgegenbringen – angesichts der empfindlichen Bußgelder und angesichts dessen, dass der deutsche Gesetzgeber mit dem neuen BDSG für den Beschäftigtendatenschutz (und andere Bereiche) auch nationale Vorschriften erlassen hat. Es lohnt sich also – soweit noch nicht geschehen – den Datenschutz im Betrieb grundsätzlich anzugehen und die internen Prozesse und Dokumentationen entsprechend umzusetzen. Höchste Zeit ist es in jedem Fall.

Zeitarbeit künftig weiterhin möglich

Bleibt noch die Frage, weshalb sich gerade Unternehmen der Zeitarbeitsbranche und deren Kunden mit dem Datenschutz beschäftigen sollten. Schließlich betreffen die neuen Regeln ja alle Unternehmen. Zumal sich gerade Einsatzunternehmen doch vermeintlich entspannt zurücklehnen könnten, zählen die Leiharbeitnehmer zweifellos nicht zu den eigenen Arbeitnehmern. Vielmehr sind sie dem Dienstleister unterstellt.

Klar ist zunächst: „Arbeitnehmerüberlassung ist auch künftig vollumfänglich möglich“, wie es Bénédicte Autem, Vorsitzende der Geschäftsführung der Unique Personalservice GmbH, im Interview (ab Seite 6) formuliert. Der neue Datenschutz wird das Instrument nicht grundlegend beeinträchtigen, allerdings gibt es im Zusammenhang mit der Arbeitnehmerüberlassung einige datenschutzrechtlichen Besonderheiten zu beachten. Das ist schlicht darauf zurückzuführen, dass bei der Arbeitnehmerüberlassung drei Parteien involviert sind: Der Personaldienstleister als Vertrags-Arbeitgeber, der Leiharbeitnehmer sowie das Einsatzunternehmen als „Quasi-Arbeitgeber“.

Die datenschutzrechtlichen Herausforderungen ergeben sich daher zum Beispiel, wenn der Entleiher Daten über

den Leiharbeitnehmer vom Verleiher benötigt, zum Beispiel um eigene gesetzliche Pflichten zu erfüllen. Oder: Der Leiharbeitnehmer muss bei seiner Tätigkeit im Einsatzunternehmen mit dessen betrieblichen Daten umgehen und damit Pflichten des Entleihers gegenüber Kunden oder Arbeitnehmern erfüllen.

Es kann also durchaus Situationen geben, in denen der Entleiher datenschutzrechtlich Verantwortung für oder gegenüber dem Leiharbeitnehmer übernehmen muss. Darauf sollten Unternehmen – Dienstleister wie Einsatzbetrieb – natürlich vorbereitet sein. Auch das Gesetz nimmt explizit das Einsatzunternehmen in die Pflicht, etwa indem es Leiharbeitnehmer als Beschäftigte des Entleihers im datenschutzrechtlichen Sinne bezeichnet. Details zu den datenschutzrechtlichen Rechten und Pflichten des Einsatzunternehmens im Zusammenhang mit der Zeitarbeit lesen Sie ab Seite 8 und Seite 12.

Weitere Änderungen möglich

Beim Blick in die Zukunft zeigt sich, dass gerade die aktuellen Regeln zum Beschäftigtendatenschutz noch nicht das letzte Wort darstellen könnten. Schließlich hat die neue Regierung im aktuellen Koalitionsvertrag vereinbart, „die Schaffung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz“ zu prüfen. Ein solches Gesetz könnte konkrete Regelungen zur privaten E-Mail-Nutzung, zur Verwendung von GPS-Daten im Arbeitsverhältnis, zur Videoüberwachung oder zu biometrischen Authentifizierungssystemen enthalten.

Natürlich ist der aktuelle Koalitionsvertrag bewusst vage formuliert, sodass alle Möglichkeiten denkbar sind. Ob ein eigenständiges Beschäftigtendatenschutzgesetz – das im Übrigen bereits vor einigen Jahren kurz vor der Umsetzung scheiterte – tatsächlich kommt, ist derzeit nicht vorherzusagen. Wenn ja, so bleibt jedoch zu hoffen, dass auch ausreichend Vorbereitungszeit für Unternehmen eingeplant wird. ■

BEGRIFFE

Acht Prinzipien der Datenverarbeitung

In Art. 5 Abs. 1 gibt die Datenschutzgrundverordnung (DSGVO) acht Grundsätze vor, die bei jeder Datenverarbeitung sicherzustellen sind. Der datenschutzrechtlich Verantwortliche muss die Einhaltung dieser Prinzipien gewährleisten und dies im Zweifel auch nachweisen können.

Rechtmäßigkeit

Im Grundsatz der Rechtmäßigkeit zeigt sich, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn eine Rechtsgrundlage (Art. 6 DSGVO) hierfür besteht.

Treu und Glauben

Der Grundsatz von Treu und Glauben lässt sich als Rücksichtnahmepflicht und damit als Ausprägung des bisher bekannten Grundsatzes der Verhältnismäßigkeit verstehen.

Transparenz

Der Grundsatz Transparenz meint, dass Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden dürfen. In Art. 12 wird dieser Grundsatz hinsichtlich der Betroffenenrechte präzisiert.

Zweckbindung

Nach dem Grundsatz der Zweckbindung dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden.

Datenminimierung

Nach dem Grundsatz der Datenminimierung dürfen personenbezogene Daten nur dann verarbeitet werden, wenn dies zur Erreichung des Zweckes angemessen und erheblich ist.

Richtigkeit

Personenbezogene Daten müssen sachlich richtig sein und gegebenenfalls auf den aktuellen Stand gebracht werden.

Speicherbegrenzung

Personenbezogene Daten dürfen nur solange gespeichert werden, wie dies für die Erreichung des Zwecks unbedingt notwendig ist. Entfällt der Zweck, müssen die Daten entweder vollständig gelöscht oder anonymisiert werden.

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung ein.

Datenschutz als Kernkompetenz

INTERVIEW. Auch Personaldienstleister und ihre Kunden müssen sich auf das neue Datenschutzrecht einstellen. Worauf künftig in der Zusammenarbeit zu achten ist.

personalmagazin: *Ab Ende Mai haben alle Unternehmen in Deutschland die EU-Datenschutzgrundverordnung sowie die neuen Regeln des Bundesdatenschutzgesetzes anzuwenden. Was bedeuten diese Änderungen für Personaldienstleister?*

Bénédicte Autem: Personaldienstleister sind zunächst ja auch Arbeitgeber und sind damit natürlich genauso betroffen wie alle anderen Unternehmen. Weil wir unsere Mitarbeiter dabei schon immer vollumsorglich betreuen, gehört der sensible Umgang mit vertraulichen Daten zu unseren Kernkompetenzen. Die Mitarbeiter vertrauen uns bei der Berechnung und Zahlung von Löhnen oder Pfändungen. Auch bei gesundheitlichen Einschränkungen bis hin zu privaten Problemen sind wir erster Ansprechpartner und Hilfesteller. Das liegt auch daran, dass wir eben dem Thema Datenschutz schon seit Jahren einen hohen Stellenwert im Unternehmen einräumen. Wir investieren stetig in die Kompetenz und Zeit unserer Datenschutzbeauftragten und ich lasse mich zum Beispiel persönlich über den aktuellen Stand regelmäßig informieren.

Die europäische Datenschutzrichtlinie basiert in weiten Teilen auf dem deutschen Datenschutz. Unternehmen, die wie wir den Anforderungen des deutschen Datenschutzes bereits seit Langem nachkommen, sind da natürlich gut aufgestellt. Sie erfüllen bereits einen Großteil der Regelungen. Blickt man jedoch speziell auf unsere Branche, so gibt es einige große Anbieter und Tausende kleinere Personaldienstleister. Gerade letztere Unternehmen haben alleine aufgrund ihrer Struktur und der Prioritäten der jeweiligen Inhaber dem Datenschutz bis dato nicht die erforderliche Aufmerksamkeit geschenkt. Letztlich wird es jedoch für alle Unternehmen und Dienstleister, die bei null anfangen oder bei null angefangen haben, eine große Herausforderung werden, datenschutzrechtlich bis zum 25. Mai 2018 bereit zu sein.

> „Mit dem neuen Datenschutzrecht kommt es einmal mehr auf einen Partner an, der alles richtig macht – um existenzgefährdende Bußgelder zu vermeiden.“

personalmagazin: *Wie wird sich das neue Datenschutzrecht auf die Zusammenarbeit zwischen Ihnen als Personaldienstleister und Ihren Kundenunternehmen auswirken?*

Autem: Diese neuen Vorschriften zeigen einmal mehr, dass es auf die Auswahl des richtigen Partners ankommt. Erneut verschärft der Gesetzgeber Regelungen, auch wenn es dieses Mal – anders als noch bei der Reform des Arbeitnehmerüberlassungsgesetzes – alle Unternehmen betrifft. Durch die Vereinheitlichung datenschutzrechtlicher Vorgaben innerhalb der EU werden jedoch die Risiken von Bußgeldern für alle Unternehmen Realität. Ich verstehe uns als Partner und Dienstleister, der seine Kunden informiert, abholt und auch in ihrem Interesse mitdenkt. Gerade wenn die Verantwortung wie beim Datenschutz auf den Schultern aller Beteiligten liegt, ist es besonders wichtig, sich aufeinander verlassen zu können.

DAS UNTERNEHMEN

Als Full-Service-Anbieter unter den Personaldienstleistern bietet Unique den Unternehmen innovative und effiziente Konzepte für alle HR-Fragestellungen. Das Leistungsspektrum umfasst klassische Arbeitnehmerüberlassung, Personalvermittlung sowie Großkundenlösungen. Spezialisiert ist das Unternehmen auf Branchenlösungen für Industrie, Handwerk, Logistik, Handel, Dienstleistung, den kaufmännischen Bereich und Gesundheit. Unique ist deutschlandweit mit rund 80 Niederlassungen präsent und beschäftigt über 8.000 Mitarbeiter. In mehr als 40 Jahren hat der Personaldienstleister seine Erfahrungen auf dem Arbeitsmarkt ausgebaut und wurde das fünfte Jahr in Folge zum Top-Personaldienstleister ausgezeichnet. Unique ist ein Tochterunternehmen der börsennotierten USG People B. V. und damit Teil der Recruit Gruppe, einer der weltweit viertgrößten Unternehmensgruppen unter anderem für HR-Dienstleistungen.

BÉNÉDICTE AUTEM ist Vorsitzende der Geschäftsführung der Unique Personalservice GmbH und der USG People Germany GmbH.

personalmagazin: *Wie werden sich aus Ihrer Sicht die rechtlichen Veränderungen, die mit der EU-Datenschutzgrundverordnung und dem neuen Bundesdatenschutzgesetz einhergehen, auf die Branche der Personaldienstleister insgesamt auswirken?*
Autem: Arbeitnehmerüberlassung ist ja weiterhin vollumfänglich möglich. Der Gesetzgeber verlagert jüngst die Verantwortung auch auf den Entleiher. Früher hatte zum Beispiel ein inhabergeführter Personaldienstleister, der mit entsprechend „weicher Hüfte" Risiken auf sich nahm und „lösungsorientiert" dachte, gegebenenfalls einen Wettbewerbsvorteil. Heute kommt es dagegen darauf an, einen Partner zu haben, der alles richtig macht, um eigene Risiken oder existenzgefährdende Bußgelder zu vermeiden.
Größere Unternehmen können und müssen sich entsprechende interne Strukturen, Prozesse und dedizierte Fachkräfte sowie Qualitätsmanagements- oder Revisionsabteilungen leisten. Nur so können diese den an sie gestellten zahlreichen Anforderungen der Börsenaufsicht, Prüfbehörden, Wirtschaftsprüfer oder Zertifizierer gerecht werden. Für kleinere Unternehmen stellt der neue Trend der Gesetzgebung und die immer weiter steigende Komplexität eine größere Herausforderung dar. Eine Konsolidierung des Markts kann die Folge sein. Eine weitere Möglichkeit für kleinere Unternehmen besteht darin, sich in Partnerverbänden Know-how zu leisten. In jedem Fall bleibt zu hoffen, dass alle Dienstleister spätestens jetzt Wege finden, ihre Leistungen mit dem angemessenen Anspruch an rechtliche Anforderungen anzubieten.

personalmagazin: *Nicht nur wegen der neuen gesetzlichen Regelungen, auch aufgrund der Digitalisierung wird das Thema „Datenschutz" zunehmend wichtiger, zum Beispiel bei der Auswahl oder in der Kommunikation mit Bewerbern. Welche Entwicklung sehen Sie durch die Digitalisierung für die Personaldienstleisterbranche und welche Rolle wird hierbei das Thema „Datenschutz" spielen?*
Autem: Wir treiben die Digitalisierung gerade in der Rekrutierung voran. Als modernes Unternehmen investieren wir in Systeme und Tools mit dem Ziel, die Bewerberansprache und den Bewerberprozess zeitgemäß zu optimieren. Unsere Mitarbeiter und Bewerber verstehen wir ebenfalls als unsere Kunden. Im Bereich der Rekrutierung sind die Regelungen des Datenschutzes besonders zu beachten. Sie können gerade hier im Widerspruch zu dem Wunsch stehen, Daten zu sammeln. Bei der Mitarbeiterentlohnung und in anderen Bereichen der Personalarbeit liegt immer ein konkreter Grund oder zum Beispiel eine steuerrechtliche Anforderung vor, um Daten zu verarbeiten. Dies ist grundsätzlich auch bei der Rekrutierung gegeben. Allerdings spielen hier das Timing und die Löschung von Daten eine besondere Rolle. Gerade deshalb benötigt man in diesem Bereich automatisierte Systeme und Prozesse, die digital unterstützen, um die rechtlichen Bedingungen des Datenschutzes einzuhalten. Wir arbeiten zum Beispiel mit einer Spezialsoftware, vollintegrierten Systemen und Datenbanken. So können wir – auch bei einem sehr hohen Volumen an Bewerber- und Mitarbeiterdaten – eine hohe Qualität sowie gleichzeitig die Einhaltung des Datenschutzes sicherstellen.

> „Als modernes Unternehmen investieren wir in neue Systeme, die die Bewerberansprache und den Bewerberprozess optimieren und den Datenschutz beachten."

personalmagazin: *Vor Kurzem haben sich Union und SPD auf eine große Koalition verständigt. Welche Auswirkungen haben die im Koalitionsvertrag niedergelegten Pläne der neuen Regierung auf die Branche, insbesondere die geplante Beschränkung der sachgrundlosen Befristung?*
Autem: In unserem Hause nutzen wir das Instrument der Befristung von Arbeitsverträgen aufgrund der Bewerberknappheit eher selten. Wir versuchen alles dafür zu tun, gute Mitarbeiter langfristig für uns zu begeistern und auch an uns zu binden. Ein spannender Aspekt ist, wie das Gesetz mit dem Wunsch seitens des Mitarbeiters umgeht. In den jungen Generationen Y oder Z verspüren wir manchmal den Wunsch nach wenig oder kurzfristiger Bindung.
Unter dem Strich halte ich eine gesetzliche Regelung für wenig zielführend. Der Bewerbermarkt hat in den letzten Jahren deutlich seine Kraft zur Selbstregulierung gezeigt. Bewerber haben die Auswahl und Unternehmen bewerben sich bei Mitarbeitern. ■

Das Interview führte **Michael Miller.**

Datenschutz in der Zeitarbeit

ÜBERBLICK. Ab Ende Mai gilt ein neues Datenschutzrecht. Im Zusammenhang mit der Arbeitnehmerüberlassung ergeben sich dabei Besonderheiten für die Unternehmen.

Von **Jan Peter Schiller**

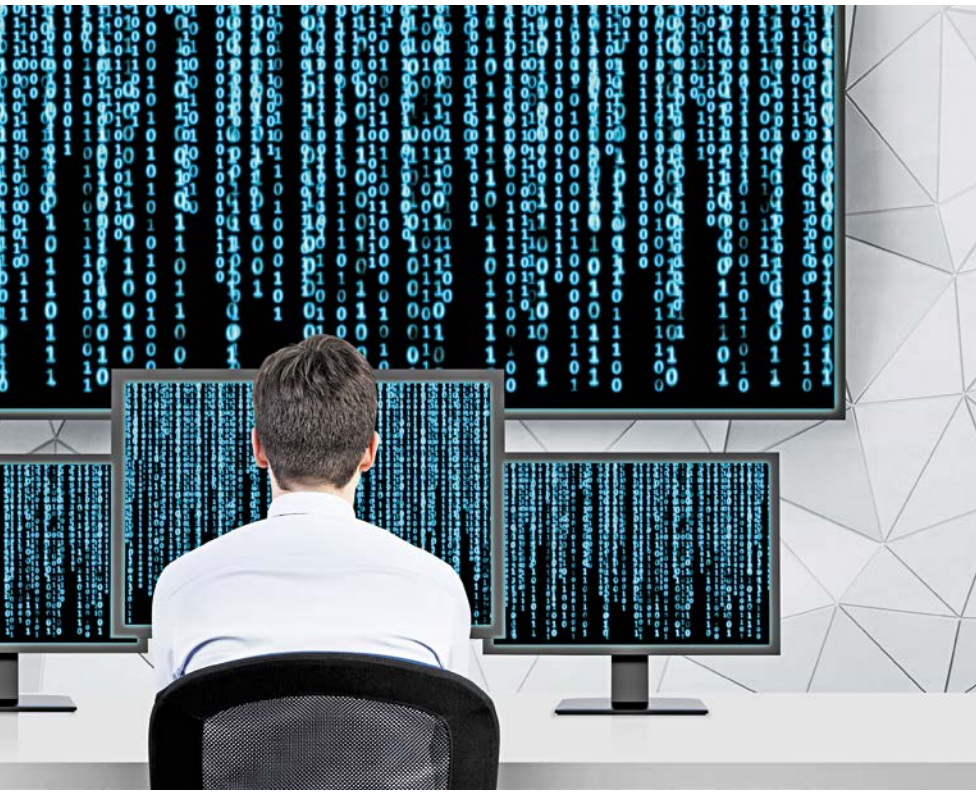
Am 25.Mai 2018 ist es so weit: Die neue Datenschutzgrundverordnung (DSGVO) ist europaweit anzuwenden. Sie sorgt mit den zahlreichen Neuerungen und insbesondere mit einem deutlich verschärften Sanktionsrahmen (siehe den Hinweis zu Sanktionen auf Seite 9) für Katerstimmung in vielen Unternehmen. Dieser Beitrag erläutert wichtige rechtliche Aspekte zum Datenschutz für die Dienstleister der Zeitarbeitsbranche sowie für deren Kundenunternehmen.

Die neue DSGVO und das neue BDSG

Ende Mai tritt nicht nur die DSGVO als unmittelbar geltendes Recht in allen Mitgliedsstaaten der EU in Kraft, sondern auch eine vollständige Neufassung des Bundesdatenschutzgesetzes (BDSG-neu) in Deutschland. Der Unionsgesetzgeber hat darauf verzichtet, den Beschäftigtendatenschutz in der DSGVO umfassend zu regeln. Stattdessen hat er mit Art. 88 DSGVO eine bereichsspezifische Öffnungsklausel geschaffen. Diese erlaubt es nationalen Gesetzgebern, den Beschäftigtendatenschutz selbst zu regeln – natürlich unter Beachtung der grundlegenden Prinzipien der DSGVO. Der deutsche Gesetzgeber hat – als bislang nur einer von zweien in der EU – diesen Auftrag angenommen und ein neues BDSG erlassen. Darin findet sich § 26 BDSG-neu, der den Bereich des Beschäftigtendatenschutzes regelt und den bisherigen § 32 BDSG ersetzt.

Künftig wird es für alle Unternehmen von außerordentlicher Bedeutung sein, die Vorgaben der DSGVO und des BDSG-neu einzuhalten und dies durch ein entsprechendes Datenschutzmanagement sicherzustellen. Der Hauptgrund liegt darin, dass durch die DSGVO insbesondere die Geldbußen bei datenschutzrechtlichen Verstößen erhöht wurden. Dadurch wird sich auch der Stellenwert des Datenschutzes in Unternehmen ändern: vom „Mauerblümchen“ zu einem Kernthema.

Für Unternehmen in der Zeitarbeitsbranche ergeben sich aufgrund des Dreiecksverhältnisses zwischen Dienstleister, Entleiher und Leiharbeitnehmer Besonderheiten, die es zu beachten gilt.



© IMAGEFLOW / SHUTTERSTOCK.DE

Datenmengen: In der Zeitarbeit gibt es bei deren Verarbeitung einige Besonderheiten.

Rechtsgrundlage immer nötig

Die DSGVO übernimmt einen Grundsatz des deutschen Datenschutzrechts auch auf europäischer Ebene: Die Verarbeitung personenbezogener Daten bedarf stets einer Rechtsgrundlage. Dieses

SANKTIONEN

Das droht bei Datenschutz-Verstößen

Bisher haben Behörden die Verstöße gegen Bestimmungen des Datenschutzes oft nicht konsequent oder mit unempfindlichen Strafen geahndet. Das dürfte sich nun durch mehr Personal und höhere Bußgelder ändern.

Sowohl für den Dienstleister als auch für den Entleiher von Zeitarbeitskräften sind die Neuerungen der DSGVO und des BDSG-neu von erheblicher Bedeutung. Denn zum einen haben die Aufsichtsbehörden bereits angekündigt, künftig konsequent gegen Verstöße vorgehen zu wollen und auch personell aufzustocken. Zum anderen sieht die DSGVO eine weitgehende Erweiterung der Haftung sowie eine erhebliche Verschärfung der Geldbußen vor. Diese können nunmehr je nach Qualität und Reichweite des Verstoßes – je nachdem, welcher Betrag höher ist – entweder

- bis 10 Millionen Euro oder bis zwei Prozent des weltweiten Konzernumsatzes des vergangenen Geschäftsjahrs (Stufe 1 bei formellen Verstößen) oder
- bis zu 20 Millionen Euro oder vier Prozent des weltweiten Konzernumsatzes des vergangenen Geschäftsjahrs (Stufe 2 bei materiellen Verstößen) betragen.

sogenannte „Verbot mit Erlaubnisvorbehalt“ bedeutet, dass jede Datenverarbeitung zunächst einmal verboten ist – es sei denn, der Verantwortliche kann sich auf eine gültige Rechtsgrundlage stützen. Diese Rechtsgrundlage kann sich im Beschäftigungskontext ergeben entweder aus

- gesetzlichen Regeln (§ 26 BDSG-neu oder Art. 6 Abs. 1 lit. f DSGVO),
- einer Einwilligung oder
- einer Betriebsvereinbarung, unter Beachtung gewisser Einschränkungen.

Konsequenz: Ein Verstoß gegen dieses Prinzip würde zu einer materiell unzulässigen Datenverarbeitung führen. Diese wäre nach Stufe 2 (siehe Hinweis auf dieser Seite oben) bußgeldbewehrt.

Wann Zeitarbeiter Beschäftigte sind

Im neuen Datenschutzrecht findet sich nunmehr eine wichtige Klarstellung für die Zeitarbeitsbranche: Auch Leiharbeitnehmer zählen zu den Beschäftigten im Sinne des BDSG-neu (§ 26 Abs. 8 Nr. 1 BDSG-neu). Sie sind somit nicht nur im Verhältnis zum Dienstleister, sondern auch im Verhältnis zum Einsatzunternehmen als Beschäftigte anzusehen. Dies bedeutet, dass die Datenverarbeitung nicht nur beim Verleiher, sondern eben auch beim Entleiher den Regelungen des Beschäftigtendatenschutzes nach Art. 88 DSGVO in Verbindung mit § 26 BDSG-neu unterliegen.

§ 26 BDSG: Daten zulässig verarbeiten

Wie nach dem bisherigen § 32 BDSG ist eine Verarbeitung personenbezogener Daten nach § 26 Abs. 1 BDSG-neu möglich, wenn diese für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Erforderlich ist eine Datenverarbeitung wiederum, wenn

- der Arbeitgeber rechtlich zur Speicherung verpflichtet ist oder
- hinsichtlich bestimmter Daten eine Meldepflicht für den Arbeitgeber an Behörden besteht, wie zum Beispiel hinsichtlich der Schwerbehindertenquote, oder
- sie den berechtigten Interessen des Arbeitgebers entspricht und die Interessen der Beschäftigten dahinter zurücktreten müssen.

Die Frage der Erforderlichkeit ist je nach Einzelfall zu bewerten. Bei den üblichen Personalstammdaten ist ein solches Interesse wohl ohne Weiteres anzunehmen.

Schwieriger wird es bei umfangreicher Erfassung von Daten über die Leistung und das Verhalten des Beschäftigten – insbesondere bei einer Standort- und Videoüberwachung oder auch bei der Verarbeitung sensibler Daten, wie zum Beispiel zur Gesundheit oder Religion. In diesen Fällen muss stets ein konkreter Tätigkeitsbezug bestehen und die Verarbeitung muss auf ein absolutes Mindestmaß beschränkt werden.

Konsequenz: Verstöße durch ausufernde, also unverhältnismäßige Datenverarbeitung sind nach Stufe 2 (siehe nebenstehende Hinweise zu den Sanktionen) bußgeldbewehrt.

Auch das Einsatzunternehmen muss sich bei der Verarbeitung der Daten von Leiharbeitnehmern streng an diesem Maßstab der Erforderlichkeit orientieren. Daher ist es zum Beispiel nicht zulässig, komplette Personalakten über Zeitarbeitskräfte anzulegen. Zudem müssen Entleiher die Daten der Leiharbeitnehmer nach Beendigung des Überlassungsverhältnisses löschen. Eine Ausnahme besteht dann, wenn die Daten noch benötigt werden, um etwa Nachweise gegenüber Behörden zu führen.

Entleiher ist selbst Verantwortlicher

Wichtig ist zunächst die Klarstellung, dass das Einsatzunternehmen nicht im Rahmen einer Auftragsverarbeitung für den Dienstleister tätig wird, sondern im Verhältnis zu den Leiharbeitnehmern selbst als datenschutzrechtlich Verantwortlicher anzusehen ist. Dies bedeutet, dass sowohl Verleiher als auch Entleiher sämtliche Vorgaben der DSGVO umsetzen müssen. Hierzu gehören vor allem umfangreiche Informations- und Transparenzpflichten (Art. 13 DSGVO).

So muss der Dienstleister bereits bei der Erhebung der personenbezogenen Daten des Leiharbeitnehmers diesen darauf hinweisen, dass er die Daten später an einen Dritten, nämlich den Entleiher, weitergeben wird. Aber auch das Einsatzunternehmen muss die Leiharbeitnehmer darüber informieren, wie er mit den über sie erhaltenen (Art. 14 DSGVO) und eventuell zusätzlich selbst erhobenen Daten (Art. 13 DSGVO) verfährt.

Konsequenz: Verstöße gegen diese Informations- und Transparenzpflichten

PFLICHT

Datenschutzbeauftragten bestellen

Die DSGVO hat den Datenschutzbeauftragten nach dem Vorbild des BDSG nunmehr europaweit eingeführt. Auch die Voraussetzungen, wann dieser zu bestellen ist, sind nun weitgehend vereinheitlicht.

Die DSGVO orientiert sich bei den Voraussetzungen für einen Datenschutzbeauftragten im Unternehmen an einem risikobezogenen Ansatz – ohne konkrete Schwellenwerte hinsichtlich der Mitarbeiterzahl. Der Bundesgesetzgeber hat im BDSG-neu jedoch von einer Öffnungsklausel Gebrauch gemacht. Dadurch gilt zusätzlich der bereits geltende Schwellenwert von in der Regel mindestens zehn Personen, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG-neu).

Wichtig und leicht zu übersehen ist: Unternehmen, die Datenverarbeitungen durchführen, welche einer Datenschutzfolgenabschätzung unterliegen, müssen unabhängig von diesem Schwellenwert einen Datenschutzbeauftragten bestellen (§ 38 Abs. 1 Satz 2 BDSG-neu). Dieser kann als interner oder externer Datenschutzbeauftragter, im Konzern auch als Konzerndatenschutzbeauftragter bestellt werden (Art. 37 Abs. 2 DSGVO).

unterfallen der Bußgeldstufe 2 (siehe Hinweise zu den Sanktionen auf der vorherigen Seite 9).

Daten auch wieder löschen

Datenbestände sind sowohl beim Dienstleister als auch beim Einsatzunternehmen zu löschen, wenn diese nicht länger benötigt werden, also ihr Zweck entfallen ist. Ein legitimer Zweck kann sich insbesondere daraus ergeben, dass Rechtsvorschriften die Speicherung der Daten für einen bestimmten Zeitraum verlangen, wie es zum Beispiel bei § 7 Abs. 2 Satz 4 AÜG („Der Verleiher hat seine Geschäftsunterlagen drei Jahre lang aufzubewahren.“) oder den steuer- und sozialversicherungsrechtlichen Aufbewahrungsfristen der Fall ist. Solange eine solche Aufbewahrungsfrist läuft, kann der Leiharbeitnehmer die Löschung der Daten nicht verlangen.

Nach Ablauf der Frist müssen die gespeicherten Daten jedoch gelöscht werden, wenn die Speicherung nicht durch andere Zwecke oder eine Einwilligung des Betroffenen erlaubt wird. Einer entsprechenden Löschungsaufforderung bedarf es nicht. Die – grundsätzlich mögliche – Weiterverarbeitung von Daten zu einem anderen als dem ursprünglichen Erhebungszweck (Art. 6 Abs. 4 DSGVO) ist derzeit noch wenig konturiert. Sie sollte daher als Rechtsgrundlage für eine Verarbeitung nur zurückhaltend und unter Einholung rechtlicher Beratung im Einzelfall verwendet werden.

Zulässige Bewerberdatenbanken

Auch Bewerber gelten datenschutzrechtlich als Beschäftigte (§ 26 Abs. 8 Satz 2 BDSG-neu). Die Verarbeitung von Daten, die für die Begründung des Beschäftigungsverhältnisses erforderlich sind, ist also zulässig (§ 26 Abs. 1 BDSG-neu). Für Zeitarbeitsunternehmen besonders relevant ist die Frage, ob personenbezogene Daten, die im Zusammenhang mit der Anbahnung eines Beschäftigungsverhältnisses gespeichert wurden, in einen Bewerberpool aufgenommen werden dürfen. Dann könnten sie bei einer passenden Anfrage die Bewerber wieder kontaktieren.

Eine solche Speicherung ist aber – zumindest auf Grundlage von § 26 Abs. 1 BDSG-neu – nicht zulässig, da die Begründung des Beschäftigungsverhältnisses auf die Bewerbung hin nicht stattgefunden hat. Die Daten wären somit grundsätzlich nach Abschluss des Bewerbungsverfahrens zu löschen.

Konsequenz: Ein Verstoß hiergegen ist nach Stufe 2 (siehe Hinweise zu Sanktionen auf Seite 9) bußgeldbewehrt.

Die Aufnahme in eine Bewerberdatenbank ist allerdings zulässig, wenn der Bewerber in diese vorher eingewilligt hat. Zwar ist eine Einwilligung (siehe Hinweise dazu auf Seite 11) grundsätzlich schriftlich zu erteilen; für den Fall, dass die Bewerbung online erfolgt, ist jedoch auch eine digitale Einwilligung zulässig. Wichtig ist dabei:

- Die Einwilligung muss ausdrücklich erfolgen, also etwa über das Anklicken einer Schaltfläche. Ein bloßer Hinweis, dass mit Absenden der Bewerbungsunterlagen auch eine Aufnahme in einen Bewerberpool verbunden ist, der im Nachgang widersprochen werden kann, ist nicht ausreichend.
- Die Einwilligung muss freiwillig erfolgen, die Nichterteilung darf also keine negativen Auswirkungen im laufenden Bewerbungsverfahren haben.
- Die Einwilligung muss „informiert“ erteilt werden. Dem Einwilligenden müssen die in Art. 13 DSGVO aufgeführten Informationen spätestens bei Erteilung der Einwilligung vorliegen.
- Es muss nicht zuletzt darauf hingewiesen werden, dass die Einwilligung jederzeit für die Zukunft widerruflich ist.

Für bestehende Einwilligungen ist zu beachten, dass diese nach der DSGVO keinen Bestandsschutz genießen. Entsprechen sie nicht den Vorgaben, werden sie am 25. Mai 2018 unwirksam. Dies sollte also überprüft und gegebenenfalls durch eine Erneuerung der Einwilligungserklärung behoben werden.

Verfahrensverzeichnis erstellen

Zwar nicht gänzlich neu, aber deutlich weitreichender als nach bisheriger Rechtslage schreibt die DSGVO den Ver-

antwortlichen die Führung eines Verfahrensverzeichnisses vor (Art. 30 DSGVO). Neu ist in diesem Zusammenhang, dass auch Auftragsverarbeiter (etwa externe Cloud-Dienstleister oder interne Shared-Service-Stellen wie HR oder Payroll) ein solches Verzeichnis führen müssen. Darin müssen sämtliche Datenverarbeitungsvorgänge genau – unter anderem hinsichtlich ihres Zwecks der verarbeiteten Datenkategorien, Löschfristen und der Datenübermittlung an Dritte – beschrieben werden. Eine Ausnahme gibt es für Unternehmen mit weniger als 250 Beschäftigten. Diese ist jedoch wenig wert, gilt sie doch nur für Unternehmen, die maximal gelegentlich personenbezogene Daten verarbeiten (Art. 30 Abs. 5 DSGVO). Auf Personaldienstleister zum Beispiel dürfte die Ausnahme keinesfalls zutreffen, denn die Verarbeitung der Daten der Bewerber und Leiharbeitnehmer erfolgt permanent. Die Führung eines Verfahrensverzeichnisses ist hier dringend anzuraten.

Konsequenz: Ein Verstoß gegen die Führung eines Verfahrensverzeichnisses unterfiele Bußgeldstufe 1 (siehe Hinweise zu Sanktionen auf Seite 9).

Folgen für Datenschutz abschätzen

Ebenfalls nicht gänzlich neu, aber auch weitreichender als bislang: Die DSGVO sieht vor, dass Verantwortliche eine sogenannte Datenschutzfolgenabschätzung (das aktuelle BDSG nennt dies „Vorabkontrolle“) im Vorfeld von solchen Verarbeitungen durchzuführen haben, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge haben. Beispiele sind eine besonders umfangreiche Datenverarbeitung oder die Verarbeitung von sensiblen Daten (Art. 35 DSGVO).

Im Falle von Bewerberdaten kann dies in Betracht kommen, wenn diese nicht nur gespeichert, sondern systematisch und automatisiert analysiert werden, um zum Beispiel eine Bewertung der Fähigkeiten der Bewerber oder ein sogenanntes Profiling vorzunehmen. Im Rahmen der Datenschutzfolgenabschätzung muss der Verantwortliche eventuelle Gefahren für die Freiheiten und Rechte der Betroffenen analysieren und entsprechende Maßnahmen zur Sicherheit der Daten treffen.

Konsequenz: Ein Unterlassen unterfiele Bußgeldstufe 1 (siehe Hinweis zu den Sanktionen auf Seite 9).

Auch DSGVO ohne Konzernprivileg

Bei Zeitarbeitsunternehmen, die in einem Konzernverbund organisiert sind, ist der konzerninterne Versand von Daten der Bewerber und Zeitarbeitskräfte oft an der Tagesordnung. Dabei ist zu berücksichtigen, dass die DSGVO (wie auch das BDSG) kein Konzernprivileg kennt. Der Datenversand innerhalb eines Konzerns ist also grundsätzlich unzulässig, es sei denn, es gibt hierfür eine Rechtsgrundlage. In der Praxis dürfte diese wohl am besten als Einwilligung ausgestaltet werden, da der Versand der Daten an Konzernunternehmen zur Durchführung des Arbeitsverhältnisses mit dem Vertragsarbeitgeber zumindest im Regelfall nicht erforderlich sein dürfte. Die in Betracht kommende Rechtsgrundlage ist im Einzelfall anhand des jeweiligen Zwecks und der konkret übermittelten Daten zu prüfen.

Konsequenz: Ein Verstoß unterliegt der Bußgeldkategorie 2 (siehe Hinweise zu den Sanktionen auf Seite 9).

Neuen Datenschutz ernst nehmen

Die Reform des Datenschutzrechts stellt Personaldienstleister und deren Kunden vor neue Herausforderungen. Mit Blick auf die hohen Bußgelder, die im Fall eines Datenschutzverstoßes drohen, kann jedem Dienstleister und Einsatzunternehmen nur dringend angeraten werden, die Änderungen im Datenschutzrecht ernst zu nehmen und sich rechtzeitig um eine gesetzeskonforme Umsetzung zu kümmern. ■

EINWILLIGUNG

Elemente	Erklärung
Freiwilligkeit	• im Beschäftigungsverhältnis grundsätzlich möglich • Abwägung der Umstände • Indizien: insbesondere wirtschaftlicher Vorteil, gleich gelagerte Interessen
Hinweispflicht	• in Textform, zum Beispiel per E-Mail • Informationen gemäß Art. 13 DSGVO • auf Widerrufsrecht nach DSGVO
Form	• grundsätzlich Schriftform, soweit keine besonderen Umstände • Abgrenzung bei Einbindung in einen Vertrag (Art. 7 Abs. 2 DSGVO)
Sonderfall	• gilt auch für besondere personenbezogene Daten (Herkunft, Gesundheit, Gewerkschaft, biometrische Daten et cetera) • Einwilligung muss sich ausdrücklich darauf beziehen
Zeitarbeit	• Einwilligung zur Weitergabe der benötigten Daten (insbesondere Name, Vorbeschäftigungsdauer) vom Verleiher an Entleiher nicht erforderlich • Einwilligung zur Weitergabe weiterer Daten erforderlich und nur unter Wahrung der Freiwilligkeit möglich

QUELLE: CMS HASCHE SIGLE

JAN PETER SCHILLER ist Rechtsanwalt und Fachanwalt für Arbeitsrecht bei CMS Hasche Sigle in Köln.

Keine innere Angelegenheit

ÜBERBLICK. Ob Erklärung oder Unterweisung: Das neue Datenschutzrecht nimmt nicht nur die Dienstleister in die Pflicht. Auch für Entleiher gibt es eigene Aufgaben.

Von **Philipp Geyer** und **Philipp Schneider**

Auch wenn viele Grundsätze erhalten bleiben, die neue EU-Datenschutzgrundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSG) werden inhaltlich einiges ändern. Daher sollte auch noch mehr ins Bewusstsein rücken, wie Unternehmen künftig mit personenbezogenen Daten der bei ihnen Beschäftigten umgehen. Bereits der Bußgeldkatalog der DSGVO (siehe Hinweis auf Seite 9) zeigt, dass es sich lohnt, datenschutzrechtlichen Fragen eine erhöhte Aufmerksamkeit entgegenzubringen. Auch die gesteigerte gesellschaftliche Wahrnehmung der Thematik ist nicht zu unterschätzen. Dadurch nimmt die Wahrscheinlichkeit eines Imageschadens zu, der auch rechtlich unbescholtene Betriebe ereilen kann. Unternehmen müssen sich der Gefahren bewusst sein. Im Falle der Arbeitnehmerüberlassung gilt dies für Personaldienstleister genauso wie für Einsatzunternehmen.

Gerade der Entleiher sollte das Datenschutzbewusstsein stärken. Auch wenn nämlich die eingesetzten Leiharbeitnehmer streng genommen nicht zur eigenen Belegschaft zählen, sondern arbeitsvertraglich Arbeitnehmer des Dienstleisters sind: Unter dem Blickwinkel des Datenschutzrechts sind sie auch Beschäftigte des Einsatzunternehmens, was § 26 Abs. 8 des neuen BDSG klarstellt. Daraus folgt eine eigene datenschutzrechtliche Verantwortung des Entleihers. Zudem liegt bei der Arbeitnehmerüberlassung gerade keine Auftragsdatenverarbeitung vor. Eine entsprechende vertragliche Vereinbarung zwischen Verleiher und Entleiher ist daher nicht erforderlich.

BETROFFENENRECHTE

LEIHARBEITNEHMER

Datenerhebung beim Verleiher	Datenerhebung beim Entleiher
Auskunftsanspruch des Leiharbeitnehmers kann gegenüber Verleiher oder Entleiher gelten. Auch der Entleiher ist eine verantwortliche Stelle im Sinne des § 1 Abs. 4 Nr. 1, 26 Abs. 8 Nr. 1 BDSG-neu. Es bleibt jedoch abzuwarten, inwieweit Leiharbeitnehmer diesen Anspruch geltend machen.	
Auskunftsanspruch des Leiharbeitnehmers gegen den Verleiher über gespeicherte Daten gemäß Art. 13, 14 DSGVO	**Zusätzlich Auskunftsanspruch** des Leiharbeitnehmers gegen den Entleiher über die wesentlichen Arbeitsbedingungen (Arbeitszeit, Verdienst et cetera), § 13 AÜG
Übertragbarkeitsanspruch des Leiharbeitnehmers zur Übertragung seiner Daten an einen zukünftigen Arbeitgeber oder Auftraggeber, Art. 20 DSGVO (Datenportabilität)	
Löschen der Daten beim Verleiher	**Löschen der Daten beim Entleiher**
Speicherung nur, solange sie für legitimen Zweck benötigt werden. Löschpflichten nach Art. 17 DSGVO werden zum Beispiel verletzt, wenn alle Daten pauschal zehn Jahre aufbewahrt werden.	
Löschpflichten für Verleiher: § 7 Abs. 2 Satz 4 AÜG spricht von aufbewahren; Digitale Kopie der Unterlagen ist hierfür wohl ausreichend. Die Aufbewahrungsfrist beträgt drei Jahre ab dem Zeitpunkt, ab dem die Unterlagen entstehen (dann ist es eine Frage der Erforderlichkeit).	**Erweiterte Löschpflichten:** Diese bestehen gegenüber dem Entleiher mit Blick auf die Personalakte etwa nach Ablauf der Dreimonatsfrist (§ 1 Abs. 1b Satz 2 AÜG). Es gibt auch andere prüfungsbedingte Gründe, Daten länger (bis zu zehn Jahren) aufzuheben.

QUELLE: CMS HASCHE SIGLE/UNIQUE

Datenverarbeitung bedarf Grundlage

Bußgeldrahmen und Aufmerksamkeit werden sich also ändern. Gleich bleibt dagegen ein Grundsatz des Datenschutzrechts: Die Verarbeitung oder Nutzung personenbezogener Daten ist grundsätzlich verboten, solange keine Rechtsgrundlage dafür existiert. Im Zusammenhang mit der Arbeitnehmerüberlassung wird man auf der Suche nach solchen

Rechtfertigungen zum Beispiel im Arbeitnehmerüberlassungsgesetz (AÜG) fündig. Aber auch der Auffangtatbestand des § 26 im neuen BDSG (ähnlich dem bislang geltenden § 32 BDSG) wird häufig als Rechtsgrundlage der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses dienen. Nicht zuletzt kann auch die Einwilligung des Betroffenen selbst eine solche Grundlage sein. Jedoch ist neben den Voraussetzungen hierfür (Näheres dazu auf Seite 11) zu berücksichtigen, dass der Betroffene die Einwilligung jederzeit widerrufen kann. Er kann also die Rechtsgrundlage recht schnell wieder entziehen.

Daher bleibt die gute Nachricht: Arbeitnehmerüberlassung ist weiterhin uneingeschränkt erlaubt. Nach § 26 des neuen BDSG können die für die Zwecke eines Beschäftigungsverhältnisses erforderlichen Daten auch künftig ausgetauscht und verarbeitet werden (Näheres dazu auf Seite 9). Dabei müssen Dienstleister wie Einsatzunternehmen darauf achten, die in Art. 5 DSGVO niedergelegten Grundsätze (siehe Hinweis auf Seite 5) zu beachten. Zudem beinhaltet die Arbeitnehmerüberlassung ein berechtigtes Interesse, entsprechende Daten auszutauschen.

Rechtsgrundlagen aus dem AÜG

Abseits des künftigen § 26 BDSG ergibt sich eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten des Leiharbeitnehmers zum Beispiel auch aus der Konkretisierungspflicht des § 1 Abs. 1 Satz 6 AÜG. Danach haben Dienstleister und Einsatzunternehmen vorab den Leiharbeitnehmer, der überlassen werden soll, genau zu benennen. Auch die gesetzliche Überlassungshöchstdauer von 18 Monaten aus § 1 Abs. 1b AÜG kann die Rechtsgrundlage dafür bilden, personenbezogene Daten des Leiharbeitnehmers zu verarbeiten und zu speichern. Schließlich muss der Einsatzbetrieb einwandfrei bestimmen können, dass ein und derselbe Leiharbeitnehmer – auch wenn er den Dienstleister wechselt – nicht länger als bis zur geltenden Obergrenze im Unternehmen eingesetzt wurde. Andernfalls – also bei Überschreiten der Überlassungshöchstdauer – drohen dem Einsatzbetrieb empfindliche Konsequenzen. Und auch § 8 Abs. 4 AÜG, wonach der Leiharbeitnehmer nach einer bestimmten Frist hinsichtlich des Arbeitsentgelts mit einem vergleichbaren Stammmitarbeiter gleichgestellt werden muss (Equal Pay), kann eine solche Rechtsgrundlage zur Datenverarbeitung darstellen. Eine Übersicht der bei der Arbeitnehmerüberlassung oft übermittelten personenbezogenen Daten finden Sie auf Seite 15.

Nicht nur Rechte, auch Pflichten

Neben Rechtsgrundlagen enthält das AÜG im Zusammenhang mit dem Datenschutzrecht auch Rechte des Leiharbeitnehmers, die das Einsatzunternehmen zu beachten hat (siehe Grafik auf Seite 12). So sind etwa die bereits erwähnten, auf Basis der Überlassungshöchstdauer gespeicherten Daten drei Monate nach Ende des Einsatzes wieder zu löschen. Danach beginnt nämlich die Berechnung der Überlassungshöchstdauer wieder von vorne, § 1 Abs. 1b Satz 2 AÜG. Die Daten sind für den vorgesehenen Zweck (Berechnung der Einsatzdauer) also nicht mehr nötig. Ebenso sind zum Beispiel weitergereichte Bewerbungsunterlagen zu löschen, wenn der Kandidat letztlich nicht eingestellt wurde.

Allerdings: Auch wenn ein Zweck wegfällt, könnte ein anderer Grund zur Datenverarbeitung weiterhin bestehen. Daher sollten Entleiher – bevor sie Daten löschen – prüfen, ob es nicht andere berechtigte Gründe gibt, die Daten zu speichern. Sind etwa die Namen, Einsatzzeit und Qualifikation des Leiharbeitnehmers in der Rechnung aufgeführt, müssen diese zum Beispiel für spätere Betriebsprüfungen länger aufbewahrt werden. Gleiches gilt für die Speicherung der Daten von Zugangsberechtigungen. Auch eine Vereinbarung mit dem Betriebsrat zur Übernahme von Leiharbeitnehmern kann dazu berechtigen, Daten länger aufzubewahren. Daher gilt: Erst prüfen, dann löschen – um zu verhindern, dass wichtige Daten schlicht gelöscht werden, obwohl sie für spätere Prüfungen noch benötigt würden.

Neben alledem hat das Einsatzunternehmen auch den in der DSGVO erfassten Informationsrechten des Leih-

RECHTSGRUNDLAGEN

Spezialgesetze (AÜG und SGB)	Auffangtatbestand des § 26 BDSG neue Fassung
• **§ 1 Abs.1 Satz 6 AÜG:** Verleiher muss dem Entleiher unter anderem den Namen des Leiharbeitnehmers mitteilen • **§ 1 Abs.1 Satz 6, § 8 AÜG:** Ab Konkretisierung der Person des Leiharbeitnehmers sind die Vorbeschäftigungszeiten mitzuteilen • **§ 69 Abs. 1 SGB:** behördeninterne Weitergabe der Sozialdaten, wenn es zur Durchführung des AÜG oder eines darauf beruhenden Verfahrens erforderlich ist.	**Für Entleiher:** • Führung eigener Personalakte über LAN nur soweit berechtigtes Interesse (§ 26 BDSG und linker Kasten) • Erhebung nicht erforderlicher Daten nur mit Einwilligung oder bei überwiegendem Interesse (Art. 6 Abs. 1 f) DSGVO) **Für Verleiher:** • Verleiher als Arbeitgeber darf erforderliche Daten erheben • Bei der Erforderlichkeit der Datenweitergabe an Kunden muss differenziert werden: - Bei Auftragserteilung sind diesem die für ihn wichtigen Bewerberstammdaten zu übermitteln - Weitergabe weiterer Daten (Sozialversicherung, Lohnsteuer, Kindergeld, Sparverträge et cetera) nur mit Einwilligung des Leiharbeitnehmers

QUELLE: CMS HASCHE SIGLE

arbeitnehmers nachzukommen. Dieser ist beispielsweise darüber zu informieren, wie das Einsatzunternehmen mit den personenbezogenen Daten umgeht, die es vom Leiharbeitnehmer selbst (Art. 13 DSGVO) oder vom Personaldienstleister (Art. 14 DSGVO) erhalten und gespeichert hat.

Wer schult den Leiharbeitnehmer?

Neben diesen Rechten und Pflichten muss der Entleiher aber natürlich auch die Wahrung des eigenen Datenschutzes im Betrieb regeln – und die Leiharbeitnehmer müssen entsprechend eingebunden werden. Hierfür kommen klassischerweise die Datenschutzunterweisung sowie die Verpflichtung auf das Datengeheimnis zum Einsatz.

Dabei stellt sich zunächst die Frage, inwiefern das Einsatzunternehmen hier tätig werden muss. Schließlich könnten die Datenschutzpflichten auch dann sichergestellt sein, wenn sich jeder Arbeitgeber – also Dienstleister und Einsatzunternehmen – zunächst alleine um die eigenen Mitarbeiter kümmert. Allerdings ist an dieser Stelle erneut darauf hinzuweisen, dass die eingesetzten Leiharbeitnehmer datenschutzrechtlich auch Beschäftigte des Entleihers sind. Letztlich sieht der Gesetzgeber wohl den Dienstleister ebenso wie das Einsatzunternehmen in der Pflicht. Praktisch dürfte es jedoch sinnvoll sein, eine Schulung von Leiharbeitnehmern im Einsatzunternehmen vor Ort durchzuführen. Schließlich kann der Entleiher die datenschutzrechtlichen Gegebenheiten, die jeweilige Praxis mit personenbezogenen Daten und den jeweiligen Schutzbedarf am besten einschätzen.

Verpflichtung auf Datengeheimnis

Auch wenn eine Verpflichtung auf die Wahrung des Datengeheimnisses in der DSGVO nicht ausdrücklich vorgeschrieben ist, so lässt sich diese aus dem in Art. 5 Abs. 1 DSGVO beschriebenen Grundsatz der Integrität und Vertraulichkeit dennoch ableiten – zumal in Deutschland § 53 des neuen BDSG eine solche Verpflichtung auf das Datengeheimnis explizit vorsieht.

Zusätzlich zu den eigenen Arbeitnehmern haben Einsatzunternehmen dabei auch Aushilfen, Praktikanten, freie Mitarbeiter sowie Leiharbeitnehmer zu berücksichtigen – wenn sie mit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten betraut sind. Selten kann jedoch ein solcher in § 53 des neuen BDSG vorgesehener Umgang mit Daten komplett ausgeschlossen werden. Daher empfiehlt es sich, die Verpflichtung auf das Datengeheimnis grundsätzlich und als festen Bestandteil des Einstellungsprozesses bei jedem Mitarbeiter – oder Leiharbeitnehmer – vor Tätigkeitsbeginn vorzunehmen.

Inhalt der Datenschutzunterweisung

Ob in Form von Schulungen, eines Merkblatts oder mittels einer persönlichen Unterweisung: Mit einer entsprechenden Datenschutzunterweisung kann der Arbeitgeber mehreren Informationspflichten – auch gegenüber eingesetzten Leiharbeitnehmern – gleichzeitig nachkommen und den Datenschutz im Betrieb sicherstellen. Zu den wichtigen Inhalten einer solchen Unterweisung gehören:

- **Datenschutzbeauftragter:** Mit der Unterweisung sollte das jeweilige Unternehmen, als Verantwortlicher für die jeweilige Datenverarbeitung, den Mitarbeitern mitteilen, wer der zuständige Ansprechpartner für Fragen zum Umgang mit personenbezogenen Daten ist. Zudem sollten die Mitarbeiter über die Funktion des Datenschutzbeauftragten informiert werden und wissen, dass dieser das innerbetriebliche Kontrollorgan zu sämtlichen Fragen rund um den Datenschutz ist.
- **Umgang mit Daten:** Das Unternehmen als Verantwortlicher im datenschutzrechtlichen Sinne sollte den Mitarbeitern praxisnah den korrekten Umgang mit personenbezogenen Daten im jeweiligen Arbeitsumfeld veranschaulichen. Das umfasst auch Informationen dazu, wie zum Beispiel Papierakten, Passwörter für IT-Systeme, mobile Datenträger (USB-Sticks, Laptops, betriebliche Smartphones), Internet oder E-Mail-Systeme datenschutzrechtlich korrekt zu nutzen sind.
- **Meldepflicht:** Weiterhin sind Anweisungen an die Mitarbeiter empfehlenswert, die das Verhalten im Fall von Datenverstößen vorgeben. Das bedeutet, dass die Mitarbeiter – sofern es zu einem Datenverstoß kommt – zumindest den Datenschutzbeauftragten und gegebenenfalls seine Fachkollegen unverzüglich informieren sollten. Schließlich sieht die DSVGO in Art. 33 Abs. 1 Satz 1 DSGVO strikte Meldefristen für Unternehmen vor, im Grundsatz „möglichst binnen 72 Stunden“. Ein Datenschutzverstoß liegt zum Beispiel vor, wenn personenbezogene Daten versehentlich per Mail oder Post an einen falschen Adressaten versendet wurden. Auch wenn ein Laptop oder ein anderer Datenträger verloren geht oder gestohlen wurde, muss immer eine Meldung erfolgen.

Datenschutz geht auch Entleiher an

Bei allen Änderungen, die das neue Datenschutzrecht nun bringen wird, zeigt sich auch: Die Einhaltung der datenschutzrechtlichen Vorschriften macht am Betriebstor keinen Halt und sie betrifft gerade nicht den Vertragsarbeitgeber alleine. Daher kommt dem Datenschutz im Zusammenhang mit der Arbeitnehmerüberlassung eine besondere Bedeutung zu. Aber nicht nur das Einsatzunternehmen muss seinen Pflichten nachkommen, es muss sich selbstverständlich auch auf seine Dienstleister verlassen können. ■

PHILIPP GEYER ist kaufmännischer Geschäftsführer und Leiter HR bei der USG People Germany GmbH.
PHILIPP SCHNEIDER ist betrieblicher Datenschutzbeauftragter bei der USG People Germany GmbH.

SCHUTZSTUFEN

Schadenspotenzial abschätzen

Personenbezogene Daten sind auch im Zusammenhang mit der Arbeitnehmerüberlassung vor Missbrauch, Fehlhandlungen oder technischem Versagen zu schützen. Dabei kann das folgende Schutzstufenkonzept helfen.

Technische und organisatorische Maßnahmen (TOM) sind nötig, um das Recht des Betroffenen auf informationelle Selbstbestimmung sicherzustellen. Um zu beurteilen, ob diese TOM angemessen sind, ist unter anderem der Grad der möglichen Beeinträchtigung schutzwürdiger Belange näher zu bestimmen. Hierbei kann die Einordnung in folgende Schutzstufen helfen – auch wenn eine solche Klassifizierung alleine wohl nicht ausreicht, um direkt die erforderlichen und angemessenen TOM abzuleiten. Dafür bedarf es vielmehr einer umfassenden Datenschutzfolgenabschätzung.

Datentyp	Risikoeinstufung (unkritisch – kritisch)					Bedeutung im Zusammenhang mit einer Arbeitnehmerüberlassung
	A	B	C	D	E	
Allgemeine, frei zugängliche Daten des Beschäftigten (Beispiel: Name, Vorname, Adresse, Telefonnummer)						Die Daten sind unkritisch, weil frei zugänglich. Es ist kein berechtigtes Interesse nötig. Die Einschätzung ist unabhängig davon, ob es sich um Arbeitnehmerüberlassung handelt oder nicht.
Allgemeine, nicht frei zugängliche Daten des Beschäftigten (Beispiel: Name, Vorname, Adresse, Telefonnummer, Geburtsdatum)						Diese Daten erfordern ein berechtigtes Interesse des Einsichtnehmenden. **Bedeutung:** Bei der Arbeitnehmerüberlassung ergibt sich dies aus der Pflicht, einen Mitarbeiter vor Einsatzbeginn eindeutig zu identifizieren (zum Beispiel: für Equal Pay oder Höchstüberlassungsdauer).
Sozialversicherungsnummer						
Einkommensbestandteile						Die unsachgemäße Handhabung dieser Daten kann das Ansehen des Betroffenen beeinträchtigen. **Bedeutung:** Für die Arbeitnehmerüberlassung müssen diese Daten jedoch ausgetauscht werden. So ist beispielsweise das Einkommen bei Faktorpreisen das Hauptkriterium für die Preisfindung. Auch die geleisteten Stunden bilden die Grundlage für die Rechnung.
Stunden (produktiv und unproduktiv)						
Beurteilungen/Zeugnisse						
Pfändungen						Die unsachgemäße Handhabung dieser Daten kann die Existenz des Betroffenen beeinträchtigen. **Bedeutung:** Bei der Arbeitnehmerüberlassung werden diese Daten regelmäßig nicht augestauscht. Pfändungen erreichen zum Beispiel im Regelfall den Arbeitgeber direkt und nicht den Entleiher. Für den Austausch von Gesundheitsdaten kann ein berechtigtes Interesse bestehen, wenn dies für die Arbeitssicherheit im Einsatz relevant ist.
Gesundheitsdaten						

Frei zugängliche Daten, der Einsichtnehmende muss kein berechtigtes Interesse geltend machen.
Beispiel: Daten aus Telefonbüchern, Adressbüchern, Wahlvorschlagsverzeichnissen

Daten, deren Kenntnisnahme an ein berechtigtes Interesse der Einsichtnehmenden gebunden ist – auch wenn deren unsachgemäße Handhabung keine besondere Beeinträchtigung erwarten lässt.
Beispiel: beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen

Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").
Beispiel: Daten zum Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten

Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz").
Beispiel: Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Gesundheitsdaten, Schulden, Pfändungen

Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte. Diese Daten werden in der Arbeitnehmerüberlassung in der Regel nicht vorkommen.
Beispiel: Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, wie etwa Gerichtsurteile oder Dokumente eines Zeugenschutzprogramms

QUELLE: LFD NIEDERSACHSEN/UNIQUE

Den passenden Partner finden

CHECK. Bei Datenschutzverstößen droht nun der Gesetzgeber mit drakonischen Geldbußen. Deshalb lohnt die Zusammenarbeit mit einem kompetenten Dienstleister.

Von **Philipp Geyer** und **Jessica C. Ehmke**

In den vergangenen Jahren scheint sich eine neue Linie in der Gesetzgebung abzuzeichnen: hin zur „pauschalen" Verantwortung mehrerer beteiligter Unternehmen, verbunden mit drastischen Bußgeldern bei Rechtsverstößen. Zumindest die Personaldienstleister und deren Kunden konnten das Gefühl einer solchen Entwicklung bekommen. Denn seit der Reform des Arbeitnehmerüberlassungsgesetzes (AÜG) zum April 2017 werden zum Beispiel nicht nur die Personaldienstleister, sondern erstmals auch die Einsatzunternehmen vermehrt in die Pflicht genommen.

AÜG-Reform als Vorläufer für mehr Verantwortung bei höheren Strafen?

So kann auch der Entleiher für – auch unbeabsichtigte – Rechtsverstöße, zum Beispiel gegen die Überlassungshöchstdauer oder die Kennzeichnungs- und Konkretisierungspflicht im Arbeitnehmerüberlassungsvertrag, verantwortlich gemacht werden. Bei Fehlern drohen ihm neben einem Arbeitsvertrag mit dem Leiharbeitnehmer und Nachzahlungen an die Sozialversicherungsträger auch ein Bußgeld von mehreren Zehntausend Euro.

Diese Tendenz scheint sich nun fortzusetzen – allerdings nicht nur in einzelnen Branchen, sondern für alle Unternehmen. Denn auch die neue EU-Datenschutzgrundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSG-neu) folgen diesem Muster. Auch hier können mehrere Beteiligte – im Bereich der Zeitarbeit erneut vor allem die Personaldienstleister und die Einsatzunternehmen – als Verantwortliche eingebunden sein, verbunden mit teils

© LIGHTSPRING / SHUTTERSTOCK.DE

Was zusammen passt: Für Unternehmen wird die Wahl des richtigen Dienstleisters noch wichtiger.

existenzbedrohenden Bußgeldern bis zu mehreren Millionen Euro (lesen Sie mehr zu Sanktionen auf Seite 9). Auch die gesetzlichen Formulierungen scheinen bewusst offen gewählt. Dies erweckt nicht selten den Anschein, dass bei Rechtsverstößen zumindest ein Schuldiger gesucht und gefunden werden kann.

Größere Wahrnehmung und mehr Kontrollen zu erwarten

Der Mechanismus „mehr Verantwortliche bei höhere Strafen“ ist aus Sicht des Gesetzgebers nachvollziehbar: Dadurch sind möglichst viele Akteure aufgerufen, sich an die Regelung zu halten, beziehungsweise diese zu gewährleisten. Flankierend dazu drohen Kontrollorgane – im Falle von AÜG-Verstößen etwa die Sozialversicherung, bei Verfehlungen im Datenschutz die Landesdatenschutzbehörden – mit häufigeren Prüfungen der Vorgänge in den Unternehmen. Die Aufstockung des Personals bei öffentlichen Prüfstellen wurde jedenfalls schon angekündigt. Zumindest beim Thema „Datenschutz“ ist nicht zuletzt aufgrund dessen hoher politischer Brisanz damit zu rechnen, dass dieses Vorhaben in die Tat umgesetzt wird.

Gerade beim Datenschutz dürfte sich künftig also einiges ändern. Zwar ist die Thematik in der öffentlichen Wahrnehmung – bis zu dem Zeitpunkt der ersten Fälle von Personen oder Unternehmen, die in der Öffentlichkeit stehen – auf wenig Interesse gestoßen. Zudem ruhte in vielen Betrieben das Thema auch deshalb, weil Prüfbehörden die Einhaltung datenschutzrechtlicher Vorgaben vielleicht zu selten kontrolliert haben. Diese Strategie sollte und dürfte vor dem Hintergrund hoher Bußgelder, gesetzlicher Mitverantwortung und des politischen Drucks auf Prüfbehörden nun jedoch ein Ende finden. Unternehmen müssen bei der Umsetzung datenschutzrechtlicher Vorgaben aufholen und prüfungssicher werden.

Weil aber auch andere Beteiligte nach dem Willen des Gesetzgebers zuneh-

MERKMALE

Was gute Dienstleister ausmacht

Bei der Auswahl des richtigen Personaldienstleisters sollten Unternehmen die folgenden Aspekte berücksichtigen und beachten. Eine Übersicht dazu, auf welche Merkmale ein Personaldienstleister Wert legen sollte und worauf es ankommt.

Rechtssicherheit

Personaldienstleister, die Mitglied in einem der beiden Branchenverbände sind, erfüllen gewisse Qualitätskriterien. Wichtig in diesem Zusammenhang ist insbesondere der Tarifvertrag der beiden Verbände mit dem Deutschen Gewerkschaftsbund (DGB). Er garantiert einen fairen Lohn – nicht zuletzt auch auf Grundlage der tariflich vereinbarten Branchenzuschläge – entsprechend der Tätigkeit und anhand von unterschiedlichen Entgeltgruppen. Daneben ist natürlich auch die Erlaubnis zur Arbeitnehmerüberlassung notwendig.

Ausfallsicherheit

Gerade bei Personaldienstleistern ist auf solide, finanzstarke Dienstleister mit guter Bonität zu achten, die bereits seit einiger Zeit am Markt bestehen. Denn als Arbeitgeber muss der Personaldienstleister Sozialversicherungsbeiträge für die Leiharbeitnehmer abführen. Bei Fehlern oder gar einer Insolvenz kann jedoch das Einsatzunternehmen gegenüber der Sozialversicherung haften.

Beschäftigungssicherheit

Nicht erst seit der AÜG-Reform (mit der gesetzlichen Equal-Pay-Regelung nach neun Monaten) ist die Bezahlung der Zeitarbeitnehmer eine wesentliche Komponente. Durch die Anwendung der Branchentarifverträge stellt der Personaldienstleister sicher, dass die Entgelte der Leiharbeitnehmer an jenes der Stammmitarbeiter im Einsatzbetrieb stufenweise angepasst wird. Eine monatliche Entlohnung, die auch in den Zeiten ohne Einsatz gezahlt wird, steht ebenso für faire Bedingungen.

Arbeitssicherheit

Der Personaldienstleister sollte den Fokus auf Arbeitssicherheit legen und sich intensiv um die erforderliche Arbeitssicherheit der jeweiligen Leiharbeitnehmer kümmern. Absprachen und Maßnahmen mit dem Einsatzunternehmen sorgen so für einen sicheren Arbeitsplatz.

Fachkompetenz

Der Personaldienstleister sollte nicht nur die Leiharbeitnehmer, sondern auch die internen Mitarbeiter im Blick behalten und großen Wert auf Ausbildung und Schulung dieses Personals legen.

Risikomanagement

Eigene und fremde Risiken erkennen und effizient managen, das fällt nicht jedem Unternehmen leicht. Zumal sich Risikobewertung und Risikomanagement nicht spontan erlernen lässt. Hier kann eine neue Sichtweise helfen, die der Personaldienstleister einbringen kann – soweit er auf die Expertise von erfahrenen Fachleuten zurückgreift. Diese können die Thematik unter verschiedenen Gesichtspunkten beleuchten und sich dementsprechend auch gegenseitig überprüfen.

Dedizierte Fachbereiche

Personaldienstleister mit eigenen Fachleuten oder spezialisierten Fachabteilungen, wie zum Beispiel der Revision, einer eigenen Rechtsabteilung oder einem Bereich zum Qualitätsmanagement, sprechen für mehr Qualität und Rechtssicherheit. Meist besteht so die nötige Erfahrung, um auch komplexen, neuen Gesetzesänderungen gerecht zu werden und diese praktikabel und verantwortungsvoll umzusetzen. Interne Prüfprozesse sorgen für die erforderliche Qualität und Rechtssicherheit. Betreut der Geschäftsführer diese Bereiche „nebenbei“ auch, so ist eine verantwortungsvolle Umsetzung dieser teils komplexen Themen nicht unbedingt gewährleistet. Zudem fehlt der kritische Kontrollblick.

Geprüfte Prozesse und Strukturen

Ein zertifizierter oder auch börsennotierter Personaldienstleister kann dem Kunden mehr Sicherheit geben. Denn je häufiger unabhängige Außenstehende (bei DIN- oder Iso-Zertifikaten, mit Wirtschaftsprüfern oder mittels Börsenaufsicht) einen Blick auf den Dienstleister werfen, desto wahrscheinlicher sind die Prozesse und Handlungen rechtskonform. Zumindest dürften jedoch weniger Themen übersehen werden, wenn einige Prüf- und Beratungsstellen auf ein Unternehmen blicken.

mend Verantwortung tragen sollen, ist für Unternehmen gerade die Auswahl von passenden, kompetenten Partnern und Dienstleistern wichtig – zumal es nahezu unmöglich erscheint, Datenflüssen klare Grenzen zu setzen. Der Gesetzgeber und der Geist der Bußgeldkataloge folgen eben diesem Dogma.

Nicht nur das Einsatzunternehmen muss also den Blick für den Umgang mit personenbezogenen Daten schärfen, auch der beauftragte Dienstleister muss dieses Bewusstsein verinnerlichen. Es ist daher zunehmend wichtig, dass auch Dienstleister datenschutzrechtliche Standards umsetzen und einhalten.

Die Auswahlkriterien für einen zuverlässigen Partner

Neben den eher klassischen Kriterien, wie zum Beispiel Bonität, Arbeitssicherheit oder Tarifbindung, gewinnen also zunehmend die Themen Rechtssicherheit und Fachkompetenz des Dienstleisters an Bedeutung (siehe Übersicht auf Seite 18). Mag in der Vergangenheit die Flexibilität mancher Dienstleister ein Verkaufsargument gewesen sein: Die eingangs skizzierten neuen Trends in der Gesetzgebung verschieben die damit verbundenen Risiken mehr und mehr in Richtung Auftraggeber, also das Einsatzunternehmen.

Personaldienstleister müssen daher in ihrer Struktur und Organisation bereit sein, die neuen gesetzlichen Regelungen zu erfüllen. Beim Thema „Datenschutz" heißt das konkret, zum Beispiel einen Datenschutzbeauftragten zu bestellen (unter bestimmten Voraussetzungen ist dies sogar verpflichtend, siehe Seite 10), Datenschutzprozesse zu implementieren oder entsprechende Richtlinien, die die Mitarbeiter verinnerlicht haben, aufzustellen (siehe Übersicht auf dieser Seite). Auch spezielle Zertifikate (DIN/ISO), regelmäßige Berichte von Wirtschaftsprüfern oder auch eigene Fachabteilungen größerer Dienstleister mit spezieller Expertise können ein wichtiges Unterscheidungskriterium darstellen.

Daher: Haben Personaldienstleister erst vor Kurzem damit begonnen, sich ausführlich mit der Umsetzung der Datenschutzbestimmungen zu befassen oder hat etwa bislang der Geschäftsführer die Funktion des Datenschutzbeauftragten lediglich nebenbei bekleidet, wird eine rechtssichere Umsetzung bis zum 25. Mai kaum mehr gelingen. Vielmehr sind Partner mit langjähriger Erfahrung, entsprechendem Know-how und längst implementierten Prozessen sicherlich besser aufgestellt und natürlich im Vorteil. ■

PHILIPP GEYER ist kaufmännischer Geschäftsführer und Leiter HR bei der USG People Germany GmbH.
JESSICA C. EHMKE ist Leiterin Marketing & Communication bei der USG People Germany GmbH.

KENNZEICHEN

Spezielle Aspekte zum Datenschutz

Auch hinsichtlich datenschutzrechtlicher Vorgaben sollten Sie auf einen kompetenten Personaldienstleister bauen, der die entsprechenden Vorgaben umgesetzt hat. Welche Aspekte speziell im Datenschutz zu berücksichtigen sind:

Datenschutzbeauftragter

Personaldienstleister verarbeiten häufig personenbezogene Daten. Wichtig ist daher eine Instanz beim Dienstleister, die die Prozesse kennt und das erforderliche Know-how hat, um zu beurteilen, ob diese Prozesse den datenschutzrechtlichen Bestimmungen genügen. Zudem ist ein Datenschutzbeauftragter der Ansprechpartner in Datenschutzfragen.

Datenschutzprozesse und -richtlinien

Existieren beim Personaldienstleister klare Prozesse und Richtlinien im Umgang mit Daten, ist dies ein guter Indikator für eine entsprechende Sensibilisierung der Mitarbeiter. Werden diese Vorgaben zu Kontroll-, Beschwerde- oder Meldeprozessen gelebt, ist dies die Basis für Rechtssicherheit, vermiedene Verstöße und Sanktionen sowie nicht zuletzt für die Verhinderung eines Imageschadens für alle Seiten.

Wahrung der Vertraulichkeit

Ihr Personaldienstleister sollte die in Art. 5 Abs. 1 DSGVO beschriebene Wahrung der Vertraulichkeit achten. Dazu zählt auch die gemäß § 53 BDSG-neu vorgeschriebene Verpflichtung auf das Datengeheimnis für alle Personen, die beim Dienstleister mit der Datenverarbeitung befasst sind. So zeigt der Dienstleister, dass bei ihm auch Ihre Daten vertraulich verarbeitet werden.

Datenschutzunterweisung

Der Personaldienstleister muss die gesetzlich vorgeschriebenen Datenschutzunterweisungen bei allen seinen mit der Datenverarbeitung befassten Mitarbeitern vornehmen. Das zeigt: Die Mitarbeiter sind mit den datenschutzrechtlichen Regelungen vertraut. Wird der Datenschutz in diesem Sinne im Unternehmen gelebt, kann auch ein verantwortungsvoller Umgang mit personenbezogenen Daten erfolgen.

Geprüfte Vertragswerke

Ein Personaldienstleister greift manchmal auf andere Dienstleister zurück, die bei der Erfüllung der vertraglichen Leistung unterstützen – beispielsweise bei der Digitalisierung von Daten. In diesen Fällen muss der Personaldienstleister prüfen und dokumentieren, nämlich die vom eingesetzten „Unter-Dienstleister" implementierten technischen und organisatorischen Maßnahmen (TOM) zum Schutz von personenbezogenen Daten. In einigen Fällen ist gleichzeitig eine Datenschutzfolgeabschätzung vorzunehmen.

Personallösungen
vom Spezialisten
Qualifizierte Fachkräfte
1A
für Industrie und Handwerk
www.technicum.de
technicum

Ihre Zukunft ist unsere Aufgabe.
persönlich &
individuell
Personallösungen für den
kaufmännischen Bereich
Arbeitnehmerüberlassung | Personalvermittlung
www.secretary-plus.de
+ secretary plus

unique | technicum | + secretary plus

„Mit der DSGVO bekommen Rechtssicherheit und Fachkompetenz bei der Wahl Ihres Personaldienstleisters eine neue und entscheidende Bedeutung. Der professionelle und rechtssichere Umgang mit personenbezogenen Daten ist unser Kerngeschäft.“

Bénédicte Autem, Vorsitzende der Geschäftsführung der USG People Germany GmbH

Wir zeigen, wie es richtig geht.

Datenschutz

Alle Antworten für Sie:
Experten-Webinar*
www.unique-personal.de/datenschutz

- ✓ Was hat sich geändert?
- ✓ Was ist zu beachten?
- ✓ Welche Lösungen gibt es?
- ✓ Woran erkenne ich den richtigen Dienstleister?

*ab Mai 2018

USG People Germany GmbH:
www.unique-personal.de www.technicum.de www.secretary-plus.de