

„Die beste Regulierung ist die, die es nicht gibt bzw. die es gar nicht braucht“

Dr. Ernesto Klengel
Wissenschaftlicher Referent
für Arbeitsrecht am HSI
der Hans-Böckler-Stiftung,
Düsseldorf

Dr. Jan Tibor Lelley
Rechtsanwalt, Fachanwalt für
Arbeitsrecht, Partner bei BUSE
Rechtsanwälte Steuerberater
Partnerschaftsgesellschaft mbB



© Karsten Schöne

Blicken wir, nach unserer ausführlichen Analyse im Titelthema der vergangenen AuA 7/23, noch einmal zurück: Die DSGVO ist nun fünf Jahre jung. Aus der Perspektive der Arbeitswelt: Sind die ersten Kinderkrankheiten durchgestanden?

Klengel: Sagen wir es so: Nicht alle Befürchtungen haben sich bewahrheitet, manche Unsicherheit besteht heute nicht mehr. Lassen Sie mich ein Beispiel geben: Betriebsräte, die betriebsverfassungsrechtliche Auskünfte verlangt haben, wurden häufig mit dem allgemeinen Hinweis beschieden, dem Verlangen stünden „Datenschutzbelange“ entgegen. Nach Entscheidungen des BAG steht nun fest, dass die Arbeitgeber nicht auf den Datenschutz verweisen können, um der betrieblichen Interessenvertretung Informationen, auf die sie nach anderen Rechtsgrundlagen Anspruch haben, vorzuenthalten. Ausnahmen können eingreifen, wenn es um besonders sensible Gesundheitsdaten geht.

Trotzdem erzeugen die nach wie vor sehr unspezifischen Regelungen zum Beschäftigtendatenschutz natürlich Rechtsunsicherheit. Diese wächst noch, wenn die allgemeinen Generalklauseln auf neue technologische Entwicklungen, insbesondere beim Einsatz von Big-Data- und KI-Systemen (Anm. d. Red.: vgl. hierzu ausführlich das Titelthema in dieser Ausgabe), angewendet werden. Wir benötigen eine konkrete Regelung für die Spielregeln des Beschäftigtendatenschutzes.

Lelley: Nach fünf Jahren seit der Einführung der DSGVO lässt sich sagen, dass einige Kinderkrankheiten überwunden wurden, aber noch nicht alle. Unternehmen haben sich allmählich an die neuen Datenschutzbestimmungen gewöhnt und ihre Prozesse entsprechend angepasst. Datenschutzbeauftragte wurden ernannt, Datenschutzrichtlinien und -verfahren wurden implementiert. Es gibt jedoch immer noch Herausforderungen, insbesondere für kleinere Unternehmen, die möglicherweise nicht über ausreichende Ressourcen verfügen. Die Einhaltung der DSGVO erfordert weiterhin kontinuierliche Anstrengungen, da neue Technologien und datenschutzrelevante Entwicklungen auftauchen. Die Zusammenarbeit zwischen Unternehmen und Datenschutzbehörden hat sich verbessert, aber es besteht immer noch Raum für weitere Fortschritte. Die DSGVO ist ein fortlaufender Prozess, bei dem weitere Erfahrungen gesammelt werden müssen, um die Datenschutzstandards kontinuierlich zu verbessern. Das gilt natürlich auch und besonders für die vertrauensvolle Zusammenarbeit zwischen Unternehmen und Betriebsrat. Gott sei Dank sehen wir es in der Praxis immer weniger, dass im Zusammenspiel von betrieblicher Mitbestimmung und Datenschutz versucht wird, auf Arbeitgeberinnen Druck auszuüben.

Die Regierung hat angekündigt, den Beschäftigtendatenschutz speziell zu regeln. Doch ein konkreter Vorschlag

lässt auf sich warten. Unterdessen hat der EuGH die hessische Rechtsgrundlage für den Beschäftigtendatenschutz verworfen, weil sie zu „unspezifisch“ sei. Wie kann sich die Praxis auf diese Unsicherheiten einstellen?

Klengel: Das Urteil in der Rechtssache C-34/21, mit dem der EuGH die Grundlage für den hessischen Datenschutz für unanwendbar erklärt hat, dürfte auf das inhaltsgleiche Bundesdatenschutzgesetz übertragbar sein – ein Fiasko für den Gesetzgeber. Umso unverständlicher ist es, dass noch immer kein Entwurf für ein Beschäftigtendatenschutzgesetz vorliegt.

In der Praxis werden sich die Auswirkungen des Urteils in Grenzen halten. Wo in Datenschutzbelehrungen die Rechtsgrundlage der Datenverarbeitung angegeben werden muss, wird nunmehr Art. 6 Abs. 1 DSGVO genannt werden müssen. Inhaltlich dürften die Datenschutzerfordernisse etwas steigen, weil der Spielraum, der bei der Anwendung nationaler Rechtsvorschriften zum Datenschutz besteht, beim Rückgriff auf die DSGVO nicht mehr gegeben ist.

Lelley: Angesichts der Unsicherheiten bzgl. des Beschäftigtendatenschutzes, insbesondere nach der „Zurückweisung“ der hessischen Rechtsgrundlage durch den EuGH, ist es wichtig, dass die Praxis angemessen reagiert. Unternehmen sollten weiterhin die allgemeinen Bestimmungen der DSGVO beachten und sicherstellen, dass sie die Grundprinzipien des Datenschutzes einhalten. Dazu gehören Transparenz, Zweckbindung, Datensparsamkeit und Datensicherheit. Es ist ratsam, die Einbindung der betrieblichen Datenschutzbeauftragten zu verstärken und die Rechtsprechung sowie Veröffentlichungen von Datenschutzbehörden aufmerksam zu verfolgen. Unternehmen können auch bewährte Verfahren und Leitlinien von Branchenverbänden nutzen, um ihre Datenschutzpraktiken zu verbessern. Es ist wichtig, dass die Mitarbeiter in Bezug auf Datenschutz geschult werden, um ein Bewusstsein für die bestehenden Anforderungen zu schaffen. Letztendlich müssen Unternehmen flexibel bleiben und bereit sein, ihre Datenschutzmaßnahmen anzupassen, sobald konkrete Vorschläge für den Beschäftigtendatenschutz vorliegen.

Stichwort Big Data: Wir erleben aktuell einen Durchbruch bei der technologischen Entwicklung von KI-Systemen. Welche Chancen und welche Herausforderungen für den Datenschutz ergeben sich durch Sprach-Tools wie ChatGPT?

Lelley: Die technologische Entwicklung von KI-Systemen wie ChatGPT eröffnet sowohl Chancen als auch Herausforderungen für den Datenschutz im Kontext von Big Data. Ich persönlich bin sicher: Die Chancen für Unternehmen und Beschäftigte überwiegen bei Weitem. Sprach-Tools ermöglichen eine effiziente und personalisierte Interaktion, was die Benutzererfahrung verbessern kann. Chancen liegen in der Automatisierung von Aufgaben, der Unter-

stützung von Kundenbetreuung und der Entwicklung innovativer Anwendungen.

Jedoch ergeben sich auch Herausforderungen bzgl. des Datenschutzes. Sprach-Tools wie ChatGPT sammeln und analysieren große Mengen an Daten, um effektiv zu funktionieren. Dies kann die Privatsphäre und Datensicherheit gefährden. Es besteht das Risiko von Datenlecks oder Missbrauch sensibler Informationen.

Es ist wichtig, dass Datenschutzbestimmungen und -richtlinien angemessen umgesetzt werden, um den Schutz personenbezogener Daten sicherzustellen. Transparente Datenverarbeitung, informierte Einwilligung, Anonymisierung und Datenminimierung sind Schlüsselprinzipien, die beachtet werden sollten. Darüber hinaus sollten ethische Richtlinien entwickelt werden, um den Einsatz von Sprach-Tools zu regulieren und sicherzustellen, dass sie keine diskriminierenden oder manipulativen Inhalte generieren.

Eine umfassende rechtliche Rahmenbedingung, effektive Aufsichtsmechanismen und bewusstseinsbildende Maßnahmen sind erforderlich, um die Chancen von Sprach-Tools zu nutzen und gleichzeitig den Schutz der Privatsphäre und den Datenschutz zu gewährleisten. Richtig ist aus meiner Sicht aber auch: Die beste Regulierung ist die, die es nicht gibt bzw. die es gar nicht braucht. Mit Blick auf schlechte Erfahrungen in der Vergangenheit ist hier viel Fingerspitzengefühl gefragt. Wir sollten verhindern, dass Europa erneut in einem wichtigen Zukunftsfeld zu einer Regulierungs- statt zu einer Innovationshochburg wird.

Klengel: Die Fähigkeiten und Einsatzmöglichkeiten von Chatbots sind beeindruckend, und wir stehen erst am Anfang der Entwicklung. Demnächst wird ChatGPT in Microsoft 365 integriert („Microsoft Copilot“): E-Mails lassen sich nach bestimmten Vorgaben der Nutzerin automatisiert verfassen, eine PowerPoint-Präsentation automatisiert aus einem Text generieren („Erstelle eine Präsentation auf Grundlage der aktuellen Geschäftszahlen!“). Sicher werden KI-Anwendungen ziemlich bald auch bei der Durchführung von Datenschutzmaßnahmen eine enorme Hilfe sein, indem sie etwa zur Vorbereitung der Erstellung von personalisierten Datenschutzhinweisen, -belehrungen und Dokumentationen herangezogen werden können. Generell hat der Einsatz KI-gestützter Tools bei der Bewältigung bürokratischer Aufgaben, etwa der Erfüllung von gesetzlichen Dokumentations- oder Berichtspflichten, großes Potenzial. Bei der Frage, ob die Textgeneratoren datenschutzkonform eingesetzt werden können, haben die Anbieter ihre Hausaufgaben noch zu erledigen, was etwa die Erhebung von Metadaten angeht oder die Datenübermittlung in Drittstaaten. Dass Daten generiert werden, die zur Leistungserfassung, aber auch zur Überwachung der Beschäftigten genutzt werden können, liegt auf der Hand. Diese Themen müssen zusammen mit dem Betriebsrat angegangen werden. ■

In dieser Rubrik sprechen wir regelmäßig über aktuelle Ereignisse und Entwicklungen, die das Arbeitsrecht betreffen und die HR-Welt umtreiben. Dabei wollen wir verschiedene Standpunkte zu Wort kommen lassen und so in den direkten Dialog gehen.