Prof. Dr. Gregor Thüsing, LL.M. (Harvard)
Institut für Arbeitsrecht und Recht der Sozialen Sicherheit, Universität Bonn
Adenauerallee 8a, 53113 Bonn

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

STELLUNGNAHME
17/1377

A40

„Daten-, Arbeits- und Gesundheitsschutz in der digitalen Arbeitswelt“

Sachverständigenanhörung, Enquetekommission I, Landtag NRW, 1. April 2019

„Digitale Transformation der Arbeitswelt in Nordrhein-Westfalen“ lautet der Titel des im vergangenen Jahr von der SPD-Fraktion gestellten Antrags, der zur Einsetzung dieser Enquetekommission geführt hat (LT-Drucks. 17/2405). Nachfolgend möchte ich – meinem wissenschaftlichen Forschungsschwerpunkt entsprechend – zu den arbeits- und datenschutzrechtlichen Fragen des zu dieser Thematik vorgegeben Katalogs Stellung nehmen.

Mit dem 25. Mai 2018 hat das Datenschutzrecht eine wesentliche Änderung erfahren. Seit diesem Tage ist die Datenschutz-Grundverordnung (kurz DS-GVO) anwendbar, die unmittelbar in allen Mitgliedstaaten gilt, es diesen aber nichtsdestotrotz ermöglicht, mittels sog. Öffnungsklauseln in einem fest abgesteckten Rahmen „spezifischere Vorschriften“ zu erlassen, die den grundsätzlichen Anwendungsbereich des Unionsrechts entfallen lassen oder aber ergänzend hinzutreten. Wenn nun über die digitale Transformation der Arbeitswelt gesprochen wird, muss Art. 88 DS-GVO in den Blick genommen werden, der Datenverarbeitungsvorgänge im Beschäftigungskontext adressiert und mitgliedstaatliche Abweichungsmöglichkeiten vorsieht. Darauf basierend hat der deutsche Bundesgesetzgeber § 26 BDSG erlassen, der an § 32 BDSG a.F. anknüpft und diesen mit wenigen, vor allem sprachlichen Änderungen fortführt (ausführlich dazu *Thüsing/Schmidt*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2018, § 26 BDSG). Damit hat er zugleich zahlreiche und durchaus laut vorgetragene Forderungen nach der Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes in den Wind geschlagen (kritisch zur Schaffung einer einzelnen Norm zur Regelung des gesamten Datenschutzes für Beschäftigte bereits *Thüsing*, NZA 2009, 865). Und auch wenn der aktuelle Koalitionsvertrag von CDU/CSU und SPD (19. Legislatur) in den Zeilen 6068-6088 davon spricht, man wolle die Öffnungsklausel des Art. 88 DS-GVO nutzen und prüfe die Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes: wahrscheinlich ist das nicht – weder angesichts der Historie des BDSG a.F. noch angesichts fehlender politischer wie juristischer Debatten dahingehend. Man scheint sich schlicht damit abgefunden zu haben. Eine erneute politische Debatte um ein Beschäftigtendatenschutzgesetz – so sehr man es sich auch wünschen mag – scheint angesichts schneller Beantwortung harrender Rechtsfragen nicht zum richtigen Zeitpunkt zu kommen.

Die spezifischeren Anforderungen, die § 26 BDSG für Datenverarbeitungen zu Zwecken des Beschäftigungsverhältnisses aufstellt, und die nun so hinzunehmen sind, erlegen Arbeitgebern feste Pflichten auf, was bei diesen im Verhältnis zum alten Datenschutzrecht zu einer deutlich gestiegenen Sensibilität in Fragen des Beschäftigtendatenschutzes geführt haben dürfte. Dies auch, weil der nordrhein-westfälische Landesgesetzgeber parallel dazu § 18 DSG NRW erlassen hat, der – wenn auch im Detail abweichend – eine vergleichbare Regelung für Datenverarbeitungsvorgänge auf Landesebene enthält. Wenn also im Rahmen des Katalogs danach gefragt wird, wie eine hohe Sensibilität im Umgang mit personenbezogenen Daten in der Arbeitswelt erreicht bzw. wie eine solche gesteigert werden kann, so muss geantwortet werden, dass die stark angehobenen Sanktionsmechanismen der DS-GVO (bis zu 20 Mio. € oder 4 % des Vorjahresumsatzes) hierzu bereits zur Genüge beigetragen haben dürften. Als Maßnahmen bieten sich demnach weniger rechtliche (und rein landesrechtlich auch kaum zu realisierende) als vielmehr tatsächliche Schritte an, wie etwa Informationskampagnen, Schulungen oder Hinweise der Berufskammern und Aufsichtsbehörden (zB solche, die die LDI NRW auf ihrer Homepage veröffentlicht). All dies gilt für die datenschutzrechtlichen Hürden, die es hierbei zu überwinden gilt; genauso und vielleicht noch mehr aber für Fragen der Daten- und Cybersicherheit. Ohne diese ist effektiver Datenschutz nicht denkbar. Dementsprechend könnten die in NRW für die Datensicherheit zuständigen Behörden besonders kleineren Unternehmen, denen die Umsetzung erfahrungsgemäß schwerer fällt, mehr Unterstützung anbieten. Exemplarisch kann die Verschlüsselung personenbezogener Daten in E-Mails und vor allem in Personalakten angeführt werden, die von Art. 32 DS-GVO u.a. gefordert wird. Erneut können Hinweise der zuständigen (Landes-)Behörden hierbei größere Klarheit schaffen, so wie es im Hinblick auf die Datensicherheit das Kurzpapier Nr. 8 der Datenschutzkonferenz vom 26. Juli 2017 – wenn auch noch recht oberflächlich – getan hat. Ebenso können Hilfestellungen bei der Sicherung von Firewalls sinnvoll sein. Nicht zuletzt verbleibt aber auch die von der NRW-Landesregierung im CDU/FDP-Koalitionsvertrag auf S. 63 avisierte Möglichkeit der Schaffung eines vielleicht bloß unterstützenden, landeseigenen Cyber Security Competence Centers.

Weiterhin beantwortet werden muss, welche personenbezogenen Daten Arbeitgeber in Nordrhein-Westfalen nach den Maßstäben des neuen Datenschutzrechts verarbeiten können. Am Anfang steht die Erkenntnis, dass eine Verarbeitung von Beschäftigtendaten dem Grundsatz nach verboten ist, und nur bei Eingreifen eines Erlaubnistatbestandes zulässig wird, Art. 6 Abs. 1 i.V.m. Art. 5 Abs. 1 lit. a) DS-GVO. So war es nach altem Recht und so ist es auch nach neuem. Welcher Erlaubnistatbestand dies indes im Einzelfall genau ist, hängt wiederum von der Art des betreffenden personenbezogenen Datums ab. Insoweit ist zu unterscheiden:

- Bei Grunddaten (bspw. Name oder Anschrift) gilt § 26 BDSG bzw. § 18 DSG NRW. Danach ist eine Verarbeitung von Beschäftigtendaten zulässig, wenn diese für die Begründung des Beschäftigungsverhältnisses oder nach Begründung für dessen Durchführung oder Beendigung *erforderlich* ist. Unter dem Begriff der Erforderlichkeit ist eine umfassende Verhältnismäßigkeitsprüfung zu verstehen, die praktische Konkordanz zwischen dem Informationsinteresse des Arbeitgebers einerseits und dem Interesse des Beschäftigten am Schutz seines informationellen Selbstbestimmungsrechts andererseits herstellt (näher *Thüsing/Rombey*, NZA 2018, 1105, 1107 ff.).

  Weiterhin wird mit § 26 BDSG bzw. § 18 DSG NRW die Möglichkeit, per Kollektivvereinbarung einen eigenständigen Erlaubnistatbestand zu schaffen, gesetzlich fixiert. Insoweit bietet sich den Betriebsparteien die Gelegenheit, im Rahmen einer Betriebsvereinbarung die Zulässigkeit einer Datenverarbeitung selbst herbeizuführen und etwaigen Rechtsunsicherheiten vorzubeugen. Der Betriebsrat wird damit in seiner Eigenschaft als „Wächter des Persönlichkeitsrechts der Beschäftigten" gestärkt; nichts anderes gilt für den Personalrat und entsprechend durch diesen abzuschließende Dienstvereinbarungen. Inwieweit es in diesem Rahmen allerdings denkbar ist, vom Schutzniveau der DS-GVO und des BDSG bzw. des DSG NRW abzuweichen, gehört freilich zu den umstrittensten Fragen des neuen Beschäftigtendatenschutzrechts.

  Den Trias an Rechtfertigungsmöglichkeiten komplettiert die Einwilligung des von der Datenverarbeitung betroffenen Beschäftigten, an deren Freiwilligkeit hohe Anforderungen zu stellen sind. Sowohl der Bundes- als auch der Landesgesetzgeber haben dem Rechtsanwender insoweit Kriterien an die Hand gegeben, die die Feststellung derselben erleichtern sollen. Für Unternehmen in Nordrhein-Westfalen empfiehlt es sich jedoch häufig nicht, in den „Häuserkampf der Einwilligung" zu ziehen, da diese ob ihrer jederzeitigen Widerrufbarkeit und strengen Wirksamkeitsvoraussetzungen für den Regelfall mit zu vielen Rechtsrisiken belastet sein dürfte. Als Faustregel der Debatte kann gelten: Vor Begründung des Beschäftigungsverhältnisses wird die Einwilligung eine Datenverarbeitung regelmäßig nicht legitimieren können, während im bestehenden Beschäftigungsverhältnis schon eher von deren Wirksamkeit auszugehen sein wird, soweit eines der in § 26 Abs. 2 BDSG oder § 18 Abs. 2 DSG NRW nicht abschließend genannten Kriterien erfüllt ist, also bspw. der Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erreicht oder aber Arbeitgeber und Beschäftigter gleichgelagerte Interessen verfolgen.

- Bei besonderen Kategorien personenbezogener Daten dagegen, die datenschutzrechtlich zu Recht als sensibel eingestuft werden (zB Herkunft, religiöse Überzeugung, Gewerkschaftszugehörigkeit, aber auch das im Fragenkatalog genannte Datum über den Gesundheitszustand eines Beschäftigten), gelten strengere Voraussetzungen. Insoweit findet § 26 Abs. 3 BDSG bzw. § 18 Abs. 3 DSG NRW jeweils i.V.m. Art. 9 DS-GVO Anwendung. Danach ist zur Rechtfertigung eine besondere Interessenabwägung notwendig sowie ferner, dass die Verarbeitung der sensiblen Daten der Ausübung von Rechten oder der Erfüllung von Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit oder des Sozialschutzes dient.

Insgesamt zeigt sich: Richtung und Tendenz der Anpassung innerbetrieblicher Abläufe an die datenschutzrechtlichen Anforderungen können nur im Einzelfall, je nach Unternehmen und je nach Datenverarbeitungsvorgang bestimmt werden. Eine abstrakte Lösung hierfür kann es nicht geben. Besonders deutlich wird dies, wenn man auf Big-Data-Anwendungen blickt, deren Nutzung nicht nur in der digitalen Arbeitswelt, sondern auch im Gesundheitssektor gesellschaftlich, aber eben auch rechtlich, kontrovers diskutiert wird. Dabei wird das Spannungsverhältnis zwischen Big Data und dem Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO deutlich. Riesige Datenmenge unterschiedlicher natürlicher Personen zu analysieren, hat große Vorteile und führt zu neuen Erkenntnissen, birgt aber genauso große Rechtsrisiken, besonders dann, wenn künstliche Intelligenz zum Einsatz kommt (ausführlich *Thüsing/Rombey*, NZS 2019, 201). Entsprechende Anwendungen vermögen es fraglos, eine positive Wirkung auf die Wertschöpfung eines Unternehmens zu entfalten, müssen aber nichtsdestoweniger datensparsam ausgestaltet sein. Dass ein Spannungsverhältnis gibt, heißt jedoch nicht, dass dieses nicht aufzulösen wäre. So werden bereits Big-Data-Modelle entwickelt, die per Anonymisierung gänzlich auf den Personenbezug der Daten verzichten, diesen zumindest auf das absolut Notwendige beschränken oder aber – gerade bei unternehmerischer Wertschöpfung – allein sachbezogene Daten verarbeiten, die dem Datenschutzrecht nicht unterfallen (s. für die USA, die hier deutlich weiter sind, *Price/Cohen*, Nature Medicine 25 (2019), 37). Ebenso ist es möglich, die Notwendigkeit der Verarbeitung selbst riesiger Datenmengen im Einzelfall darzulegen. Ähnliche Probleme stellen sich beim Zweckbindungsgrundsatz, der in Big-Data-Konstellationen ebenso sorgfältig beachtet werden muss. Es ist nur wichtig, dass Unternehmen sich dessen bewusst sind. Nicht zuletzt deshalb mag eine politische Diskussion über all dies zwar durchaus hilfreich sein; umgesetzt werden müssen die entsprechenden Erkenntnisse dagegen in der Praxis. Mithin ist es vornehmlich an den Unternehmen in Nordrhein-Westfalen, ihre innerbetrieblichen Abläufe an den obigen Maßstäben auszutarieren.