Vereinbarkeit der vorliegenden IT-Richtlinien von Thor mit dem europäischen und deutschen Datenschutzrecht und der Konzernbetriebsvereinbarung vom 7.2.2018

Gutachtliche Stellungnahme

von

Prof. Dr. Wolfgang Däubler, Universität Bremen

I. Überblick über die vorliegenden Richtlinientexte

IT-1: Richtlinie für IT-Nutzer

Die Richtlinie enthält u. a. auch Auszüge aus anderen Richtlinien wie z. B. IT-2 (Informationssicherheit)

In Abschnitt I heißt es gegen Ende:

„Weitere Einzelheiten erhalten Nutzer in der *vollständigen Richtlinie*, auf die unter dem jeweiligen zusammengefassten Punkt verwiesen wird."

Der Text dieser „vollständigen Richtlinie" **liegt nicht vor** und kann daher auch nicht auf seine Vereinbarkeit mit dem Datenschutzrecht hin überprüft werden.

Unter „II Geltungsbereich" heißt es im letzten Absatz:

„Diese Richtlinie ist in anderen bei Thor anwendbaren Richtlinien und Verfahren integriert, unter anderem in solchen *bezüglich Sicherheit, Privatsphäre, Datenschutz, Aufbewahrung von Unterlagen und Personalakten,* in jedem Fall jedoch zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten."

Richtlinien bezüglich „Privatsphäre, Datenschutz, Aufbewahrung von Unterlagen und Personalakten" **liegen nicht vor**. Ist dies so zu verstehen, dass insoweit neue Richtlinien erarbeitet werden können?

In Abschnitt III F 5 a der Richtlinie ist von einer Richtlinie über die **Speicherung von Datensätzen** die Rede; diese liegt gleichfalls nicht vor.

Zur IT-1 ist ein dreiseitiges Papier (E – Änderung des Standardbetriebsverfahrens) mit Änderungs- und Ergänzungsvorschlägen erarbeitet worden..

IT-2: Informationssicherheit

Teile dieser Richtlinie wurden unter Richtlinie IT-1 bereits behandelt. Außerdem liegen Änderungsvorschläge von EHG vor.

IT-3: Nutzung von E-Mail und Internet

Auch hier finden sich einige Punkte schon unter IT-1. Zur IT-3 liegen Änderungsvorschläge von E. vor. Unter III D 3 ist von einer **„Richtlinie für Geschäftsethik“** die Rede; diese liegt nicht vor.

IT-4: Einhaltung von Softwarelizenzbestimmungen

IT-5: Erwerb von Hardware und Software sowie von Beratungsdienstleistungen Dritter

IT-6: Entwicklung von Anwendungen/Programmen und Änderungsmanagement

IT-7: Anwendungs-, Computer- und Netzwerküberwachung

IT-8: Sicherungen von Anwendungssystemen

IT-9: Verfahren zur Notfallwiederherstellung (mit Anhängen)

IT-10: Datenbankverwaltung und Support

IT-11: Betriebssystemsoftware

IT-12: IT-Mobilgeräte

Hierzu liegt ein Änderungsvorschlag von EHG vor.

IT-13: Zahlungskarten

IT-14: Reaktion auf Sicherheitsvorfälle

Hierzu liegt ein Änderungsvorschlag von E. vor.

Außerdem liegt das Papier **„Anerkennung der Thor-Richtlinien für die allgemeine Nutzung von IT-Ressourcen und IT-Mobilgeräten“** vor, das sich auf IT-1 und IT-12 bezieht.

II. Vereinbarkeit der IT-1 mit geltendem Datenschutzrecht und der Rahmenkonzernbetriebsvereinbarung sowie offene Fragen

1. Definitionen

Unter III A 1 werden zu den IT-Ressourcen auch mobile Geräte wie Laptops und Tablets gerechnet. Auch werden am Ende Smartphones erwähnt. Damit ist das Verhältnis zur Richtlinie IT-12 aufgeworfen, die zu den „Mobilgeräten“ nur Smartphones und Tablets, nicht aber Laptops zählt. Dies betrifft aber keine datenschutzrechtliche Frage, sondern allein die Systematik der Richtlinien. Insoweit kann hier ein Hinweis genügen.

2. Nutzung der IT-Ressourcen mit Geräten, die nicht von T. zur Verfügung gestellt werden

T. will seine IT-Ressourcen verständlicherweise dadurch schützen, dass ein Zugriff grundsätzlich nur mit von T. zur Verfügung gestellten Geräten möglich sein soll (III B). Ausnahmen sind zugunsten von Arbeitnehmern, Besuchern und Vertragspartnern möglich, bedürfen jedoch der Überprüfung und der Genehmigung durch die jeweilige Unternehmenseinheit und das IT-Management. Eine solche Genehmigung ist von der Erfüllung zahlreicher Voraussetzungen abhängig.

T. hat als Arbeitgeber und als Eigentümer seiner IT-Ressourcen das Recht, die Bedingungen für den Zugriff mit Hilfe der Geräte Dritter festzulegen. E. schlägt vor, dass ein solcher Zugriff für Mitarbeiter generell untersagt sei. Damit kommen die Beschäftigten nicht in die Situation, eigene Geräte für einen Zugriff verwenden zu können, was im Einzelfall zur Folge haben könnte, dass in Störungsfällen eigene Daten mitgelöscht werden, die sich auf dem Gerät befinden. Soweit dies akzeptabel erscheint, sollten in der Tat die Arbeitnehmer von der Benutzung ihrer eigenen Geräte von vorne herein ausgenommen werden. Das Modell „Byod“ (Bring your own device“) ist eine Möglichkeit, doch besteht keine Notwendigkeit, davon effektiv Gebrauch zu machen.

Soweit die Arbeitgeberseite eine Notwendigkeit sieht, dass Arbeitnehmer Zugriff auch mit Geräten vornehmen können, die nicht von T. zur Verfügung gestellt wurden,

Beispiel: Das normalerweise benutzte Gerät geht verloren oder ist defekt. Für eine Übergangszeit benutzt der Arbeitnehmer ein eigenes Gerät, weil der Arbeitgeber kein geeignetes Ersatzgerät zur Verfügung hat

so sollte ausdrücklich darauf hingewiesen werden, dass es sich um zeitlich begrenzte Ausnahmefälle handelt und wie bei ihrem Auslaufen zu verfahren ist.

Mögliche Regelung: Der Arbeitnehmer wird verpflichtet, alle dienstlichen Daten dem Arbeitgeber zur Verfügung zu stellen, sie auf sein neues Dienstgerät zu übertragen und anschließend auf dem privaten Gerät zu löschen.

3. Das Problem der Nutzer-ID

Nach III C 1 erhält jeder Nutzer seine eigene Kennung für die Anmeldung im Thor-Netzwerk. Solche Nutzer-IDs dürfen nicht gemeinsam mit anderen Personen genutzt werden.

Was den einzelnen Arbeitnehmer betrifft, so handelt es sich insoweit um eine arbeitsbezogene Vorgabe, gegen die keine Bedenken bestehen. Anders verhält es sich jedoch mit dem Betriebsrat. Nach der Rechtsprechung des BAG hat der Betriebsrat das Recht, über die Konfiguration der von ihm benutzten Geräte selbst zu entscheiden. So kann er unabhängig vom Arbeitgeber festlegen, ob es eine personalisierte Anmeldung für jedes Betriebsratsmitglied gibt oder ob eine einheitliche für alle gleiche Nutzeranmeldung praktiziert wird.

BAG v. 18.7.2012 – 7 ABR 59/96 – RDV 2012, 295; ebenso LAG Berlin-Brandenburg v. 4.3.2011 – 10 TaBV 1984/10 – DB 2011, 882

Ob die eine oder die andere Alternative gewählt wird, obliegt der freien Entscheidung des Betriebsrats im Rahmen der Organisation seiner Arbeit. Auf eine solche Geschäftsführungsbefugnis kann der Betriebsrat nicht verzichten; sie ist ihm vom Gesetz vorgegeben. Insoweit muss Abschnitt III C 1 um eine Ausnahme für den Betriebsrat ergänzt werden. Man könnte etwa formulieren:

„Der Betriebsrat kann beschließen, dass seine Mitglieder und nachrückende Ersatzmitglieder dieselbe Nutzer-ID verwenden, wenn sie auf die Geräte und Dateien zugreifen wollen, die dem Betriebsrat zur Verfügung stehen."

4. Eigentum an Daten und freies Verfügungsrecht des Arbeitgebers – Vereinbarkeit mit der DSGVO?

a) Regelung in den Richtlinien

Abschnitt III F 1 der IT-1 übernimmt eine wesentliche Passage aus der IT-3 (Nutzung von E-Mail und Internet) und bestimmt:

„Bei der Nutzung der elektronischen Kommunikationssysteme des Unternehmens ...ist keine Vertraulichkeit garantiert. Alle Informationen (einschließlich Nachrichten. Kontakten, Datendateien, Bildern, Videos und Tonaufnahmen), die über die elektronischen Kommunikationssysteme erstellt, gesendet oder empfangen werden, sind als den amtlichen Unterlagen von Thor Industries zugehörig zu betrachten. Das Unternehmen hat die Möglichkeit und behält sich das Recht vor, alle Informationen, die über diese Systeme verarbeitet werden, abzurufen, abzuhören, auf diese zuzugreifen, sie zu prüfen und offenzulegen, einschließlich des Rechts, diese Informationen gegenüber Strafverfolgungsbehörden oder Dritten offenzulegen. Hierzu zählt die Überwachung und /oder Protokollierung von Nachrichten/Daten in Echtzeit, die Prüfung von Protokollen des E-Mail-, Sprach- und Internetverkehrs sowie die Durchsuchung von E-Mail- oder Voicemail-Ordnern, internetbezogenen Ordnern und auf der Festplatte oder im privaten Netzwerk abgelegten Ordnern des Nutzers."

Der Wortlaut des Abschnitts III A der IT-3 weicht davon insoweit ab, als alle Informationen, die über das E-Mail-System oder die Netzwerkinfrastruktur des Unternehmens erstellt, gesendet oder empfangen werden, „Eigentum des Unternehmens" sind. Worauf diese Differenz zurückzuführen ist, lässt sich nicht erkennen.

Im Ergebnis macht es aber keinen Unterschied, ob man die Informationen als „Teil der amtlichen Unterlagen“ des Unternehmens oder als sein Eigentum betrachtet. In beiden Fällen wird dem Unternehmen automatisch das Recht eingeräumt, mit diesen Informationen so zu verfahren, wie es dies für richtig hält. Dies wird besonders deutlich in dem ausdrücklich vorbehaltenen Recht, auf die Daten zuzugreifen und beispielsweise Telefongespräche abzuhören oder sie nicht nur an Strafverfolgungsbehörden, sondern auch an beliebige Dritte weiter zu geben. Dem Unternehmen als de „Dateneigentümer“ wird das Recht eingeräumt, mit ihnen nach Belieben zu verfahren – eine Befugnis, die § 903 BGB im deutschen Recht nur dem Sacheigentümer gewährt.

b) Die Kollision mit dem europäischen Recht

Weder die DSGVO noch das BDSG-neu kennt ein Eigentum an Daten. Diese sind nicht eigentumsfähig, da sie nicht mit einer Sache zu vergleichen sind, die einer Person ausschließlich zugeordnet ist. Vielmehr gibt es in Bezug auf Daten nur Verfügungsbefugnisse; der sog. Verantwortliche kann im gesetzlich vorgesehenen Rahmen die Daten verarbeiten, sie beispielsweise an einen andern weitergeben oder sie aus einer Datei zu löschen. Dafür bedarf er aber einer besonderen Rechtsgrundlage: Nur wenn die DSGVO oder das BDSG eine entsprechende Erlaubnis enthalten, darf in bestimmter Weise mit den Daten „umgegangen“ werden, dürfen sie beispielsweise an andere übermittelt oder gelöscht werden. Eine „freie Verfügungsmacht“ besteht nicht.

Die im Datenschutzrecht enthaltenen Erlaubnisse setzen durchweg voraus, dass die Verarbeitung zu einem bestimmten Zweck erfolgt. Eine „zweckfreie“ Nutzung, genauer: eine Nutzung zu beliebigen Zwecken ist nach Art. 5 Abs. 1 Buchstabe b DSGVO ausgeschlossen. Was speziell Beschäftigtendaten betrifft, so dürfen sie nach § 26 Abs. 1 Satz 1 BDSG-neu nur zum Zwecke der Begründung, Durchführung und Beendigung des Arbeitsverhältnisses verwendet werden. Von Bedeutung ist weiter der Grundsatz der Datentransparenz (Art. 5 Abs. 1 Buchstabe a DSGVO), wonach für den einzelnen nachvollziehbar sein muss, was mit seinen daten geschieht. Dies ist nicht der Fall, wenn sich der Arbeitgeber jede Form des Zugriffs und jede ihm sinnvoll erscheinende Verwendung vorbehält.

Die Verarbeitung von Daten unterliegt außerdem dem Verhältnismäßigkeitsprinzip. So können beispielsweise Arbeitnehmerdaten nur insoweit gespeichert und verarbeitet werden,

als es zur Begründung, Durchführung und Beendigung des Arbeitsverhältnisses „erforderlich“ ist. Informationen, die der Arbeitgeber für diese Zwecke gar nicht benötigt, dürfen auch nicht erhoben und gespeichert werden.

Soweit ein Informationssystem auch Niederlassung im Nicht-EU-Ausland einbezieht, sind die Übermittlung und der Abruf von personenbezogenen Daten nur im Rahmen der Art. 44 DSGVO zulässig.

Abschnitt III F 1 kann angesichts dieser datenschutzrechtlichen Rahmenbedingungen in Europa nicht aufrechterhalten werden.

c) Mögliche Regelungen

Die Abänderungsvorschläge von E. betreffen allein den Zugriff auf „erfasste“ Daten, eine Voraussetzung, die beispielsweise beim Abhören von Telefongesprächen nicht gegeben ist, da die Gesprächsinhalte noch nicht erfasst sind. Davon abgesehen, erscheint es nicht zielführend, die Formulierung des ersten Absatzes unverändert zu lassen, also von einem unbeschränkten „Dateneigentum“ auszugehen und dann im zweiten Absatz lediglich die Nutzung für bestimmte Zwecke zuzulassen. Dies bringt die Gefahr mit sich, dass in bestimmten Konstellationen (die nichts mit den Zwecken des Abs. 2 zu tun haben) eben doch wieder auf das stehen gebliebene Grundprinzip zurückgegriffen wird.

Als Alternative käme eine Formulierung in Betracht, die auf das in der EU und in Deutschland geltende Datenschutzrecht verweist und außerdem die Konzernrahmenbetriebsvereinbarung einbezieht. Man könnte etwa formulieren:

„Bei der Erhebung und Verarbeitung personenbezogener Daten und bei der Nutzung der elektronischen Kommunikationssysteme des Unternehmens sind die EU-Datenschutz-Grundverordnung, das seit 25. Mai 2018 geltende Bundesdatenschutzgesetz, andere Datenschutznormen sowie die Rahmenkonzernbetriebsvereinbarung vom 7. Februar 2018 in ihrer jeweiligen Fassung zu beachten.“

Dies hat den Vorteil, dass man nicht alle denkbaren Formen der Datenverarbeitung aufzählen muss; stattdessen kann von den Möglichkeiten Gebrauch gemacht werden, die das staatliche Recht und die Rahmenkonzernbetriebsvereinbarung lassen.

d) Drohende Sanktionen

Die Ersetzung der Bestimmung über das „Dateneigentum“ und die freie Verfügbarkeit über alle im System befindlichen Daten dient nicht nur dem Schutz der Beschäftigten. Auch Kunden und Geschäftspartner erwarten, dass mit ihren Daten nach präzisen Regeln verfahren wird. Für ein solches Bekenntnis zum hier geltenden Datenschutzrecht spricht auch ganz entscheidend das Interesse des gesamten Unternehmens: Würde man die bisherige Regelung in der IT-1 beibehalten, würde dies alsbald die Aufsichtsbehörde für den Datenschutz auf den Plan rufen. Sie hat nach Art. 51 ff. DSGVO die Aufgabe, für die Einhaltung des Datenschutzrechts zu sorgen und unterliegt dabei keinerlei Weisungen. Art. 57 DSGVO umschreibt ihre Aufgaben im Einzelnen, Art. 58 DSGVO enthält einen umfangreichen Katalog von Befugnissen, die bis zum Verbot bestimmter Datenverarbeitungen reichen. Von entscheidender Bedeutung ist jedoch Art. 83 DSGVO, der die Verhängung von Geldbußen regelt. Zahlreiche Verstöße können von der Aufsichtsbehörde nach Art. 83 Abs. 4 mit Geldbußen bis zu 10 Mio. Euro oder von bis zu 2 % des weltweit erzielten Unternehmensumsatzes geahndet werden. Art. 83 Abs. 5 nennt eine Reihe weiterer Verstöße, die Geldbußen von bis zu 20 Mio. Euro oder – soweit der Betrag höher ist – bis zu 4 % des weltweit erzielten Jahresumsatzes betragen können. Im Text der DSGVO ist zwar von „Unternehmen“ die Rede, doch wird von zahlreichen Autoren in der Literatur der Standpunkt vertreten, dass damit der „Konzernumsatz“ gemeint sei. Voraussetzung sei lediglich, dass die Töchter nicht völlig selbständig agieren. Es gehe wie im Kartellrecht um Sanktionen gegen eine „wirtschaftliche Einheit“, was sich in der Tat aus den Erwägungsgründen zur DSGVO ergibt.

> So Boehm, in: Simitis/Hornung/Spiecker (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019, Art. 83 Rn. 40 ff.; Gola, in: Ders. (Hrsg.), DSGVO. Kommentar, 2. Aufl., München 2018, Art. 83 Rn. 19; Golla, in: Auernhammer (Begr.), DSGVO BDSG, Kommentar, 5. Aufl., Köln 2017, Art. 83 Rn. 26; Nemitz, in: Ehmann/Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl., München 2018, Art. 83 Rn. 42; Sommer, in: Däubler/Wedde/Weichert/Sommer, EU-

Datenschutz-Grundverordnung und BDSG-neu, Kompaktkommentar, Frankfurt/Main 2018, Art. 83 Rn. 25; unentschieden Bergt, in: Kühling/Buchner (Hrsg.), DSGVO – BDSG, Kommentar, 2. Aufl., München 2018, Art. 83 Rn. 43, 43a; Popp, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Aufl. Baden-Baden 2018, Art. 83 Rn. 7

Realistischerweise ist damit zu rechnen, dass sich die Aufsichtsbehörden der herrschenden Meinung in der Literatur anschließen werden, zumal das Bayerische Landesamt für Datenschutz bereits diesen Standpunkt vertritt. Beträgt der Konzernumsatz beispielsweise 8 Mrd. Euro, so kann das Bußgeld bis zu 320 Mio. Euro betragen. Es liegt auf der Hand, dass zumindest in den Anfangsjahren dieser Rahmen höchstens in Extremfällen ausgeschöpft wird, doch können die finanziellen Sanktionen dennoch außerordentlich schmerzlich sein. Das Risiko einer solchen Entwicklung sollte von vorne herein durch entsprechende Anpassung der Richtlinien verhindert werden.

5. Löschungsgrundsätze

Abschnitt III F 5 der IT-1 enthält unter der Überschrift „Organisation“ u. a. sog. Bereinigungsrichtlinien, die von den E-Mail-Systemen automatisch durchgesetzt werden. Nach Buchstabe a der Bestimmung dürfen E-Mails im standardmäßigen Posteingang und im Ordner für gesendete Objekte nicht länger als 365 Zage aufbewahrt werden. E-Mails im standardmäßigen Spam-Ordner, im Ordner für Entwürfe und für gelöschte Objekte dürfen nicht länger als 30 Tage aufbewahrt werden. Diese Fristen gelten nicht, soweit in der „Richtlinie für die Speicherung von Datensätzen“ nichts anderes vorgeschrieben ist.

Die Beurteilung dieser Regelung stößt auf die Schwierigkeit, dass die Richtlinie für die Speicherung von Datensätzen nicht vorliegt. Insoweit muss ein kurzer Hinweis auf die Rechtslage nach der DSGVO genügen.

Art. 17 DSGVO enthält eine sehr differenzierte Regelung über die Löschung von gespeicherten Daten. Dabei wird zwischen der Löschung auf Verlangen der betroffenen Person und der Löschung aufgrund einer Verpflichtung des Verantwortlichen unterschieden. Außerdem gibt es Löschungsverbote; sog. Geschäftsbriefe, die auch die Form eines E-Mails haben können, müssen z. B. nach § 257 HGB und nach § 137 AO sechs oder zehn Jahre

aufbewahrt werden, dürfen also nicht früher gelöscht werden. Eine generelle Löschungspflicht nach 365 bzw. 30 Tagen dürfte mit den Löschungsbestimmungen des Art. 17 DSGVO auf den ersten Blick schwerlich vereinbar sein. Allerdings muss der Erhalt der Richtlinie abgewartet werden, ehe eine definitive Stellungnahme möglich ist. Diese kann bei Bedarf gerne ausgearbeitet werden.

Eine pragmatische Lösung wird von E. im Zusammenhang mit der IT-3 vorgeschlagen. Danach werden Mails, die älter als drei Monate sind, archiviert, sofern 80 % der maximalen Speicherkapazität des E-Mail-Postfachs erreicht sind. Dabei wird mit den ältesten Mails begonnen. Die Aufbewahrungsdauer im Archiv soll unbegrenzt sein. Damit soll aber ersichtlich nicht der Anspruch einzelner Beschäftigter abgeschnitten werden, unter bestimmten Voraussetzungen die Löschung von Daten zu verlangen. Auch wäre noch zu klären, unter welchen Voraussetzungen einzelne Personen auf das Archiv zugreifen können.

6. Situation bei Kündigung eines Arbeitnehmers und anderer Formen der Beendigung des Arbeitsverhältnisses

Abschnitt III I behandelt unter der etwas missverständlichen Überschrift „Kündigung des Zugriffs“ die Frage, wie bei der Kündigung von Nutzern im Einzelnen zu verfahren ist. Es geht also nicht darum, dass einem Beschäftigten lediglich der Zugriff entzogen wird; vielmehr geht es um Fälle des Ausscheidens aus dem Unternehmen. Dabei sollte klargestellt werden, ob es nur um die Kündigung des Arbeitnehmers durch den Arbeitgeber oder auch um die sog. Eigenkündigung des Arbeitnehmers geht.

Nach Ziffer 1 ist der System-/Sicherheitsadministrator so schnell wie möglich, spätestens jedoch zwei Tage nach der Kündigung von dieser in Kenntnis zu setzen, wobei die Mitteilung vorzugsweise durch den Vorgesetzten oder die Personalabteilung erfolgen sollte. Ob dies zu einersofortigen Sperrung des Zugriffs auf die betrieblichen IT-Ressourcen führt, ist nicht ausdrücklich angesprochen, aber wahrscheinlich, da nach Ziffer 2 alle IT-Ressourcen zurückgegeben werden müssen.

Der Wortlaut des Abschnitts I lässt keinen eindeutigen Rückschluss zu, ob mit den aufgestellten Regeln nur der Fall einer Kündigung des Arbeitnehmers durch den Arbeitgeber

oder ob auch die Eigenkündigung durch den Arbeitnehmer erfasst ist. Dies sollte zur Vermeidung von Missverständnissen klargestellt werden. Offen ist weiter, wie bei sonstigen Formen der Beendigung des Arbeitsverhältnisses zu verfahren ist: Was geschieht nach Abschluss eines Aufhebungsvertrags, wie ist der Fall zu behandeln, dass ein Arbeitnehmer in Rente geht? Ist auch das Auslaufen eines befristeten Arbeitsverhältnisses erfasst? Wie wird mit den IT-Ressourcen im Falle des Tages des Beschäftigten verfahren?

Unterstellt, in allen diesen Fällen würde Abschnitt I. zugrunde gelegt, so wäre zunächst der Zeitpunkt zu klären, bis zu dem der System- oder Sicherheitsadministrator spätestens in Kenntnis zu setzen ist.

Bei Ziffer 2 werden auch die auf einer Thor-Ressource gespeicherten persönlichen Daten von der Herausgabepflicht erfasst. Dagegen ist nichts einzuwenden, wenn der Arbeitnehmer die Möglichkeit hat, seine persönlichen Daten vorher zu löschen oder auf einen anderen Datenträger zu übertragen. Wäre dies nicht der Fall, läge ein unverhältnismäßiger Eingriff in die Persönlichkeitssphäre vor, da kein überwiegendes Arbeitgeberinteresse erkennbar ist, weshalb nicht-dienstliche Daten des Arbeitnehmers zur Kenntnis genommen oder gelöscht werden dürfen.

Gegen Ziffer 3 bestehen keine Bedenken. Benutzt ein ausscheidender Arbeitnehmer IT-Ressourcen, die er nicht von T. erhalten hat, so sind die dort befindlichen dienstlichen Daten zurückzugeben oder – auf Verlangen des Arbeitgebers – zu löschen. Nur so kann ein künftiger Missbrauch verhindert werden.

III. Vereinbarkeit der IT-2 - 14 mit geltendem Datenschutzrecht und der Rahmenkonzernbetriebsvereinbarung

1. IT-2: Informationssicherheit

Die bei der IT-2 auftauchenden datenschutzrechtlichen Fragen waren zum größeren Teil schon im Rahmen der IT-1 zu behandeln.

Bezüglich der „Eigentümerschaft an Informationen (III B) ist auf die Ausführungen oben unter II 4 zu verweisen.

Was die Nutzer-ID angeht (III C 1), so ist oben unter II 3 auf die notwendige Ausnahme zugunsten des Betriebsrats hingewiesen worden.

Die in III C 3 vorgesehene Deaktivierung nach 30 Tagen wird nicht jeder denkbaren Situation gerecht. So erlaubt etwa das Mutterschutzgesetz eine Abwesenheit von 6 + 8 = 14 Wochen, was automatisch zu einer Deaktivierung führen würde. Dasselbe gilt dann, wenn ein Arbeitnehmer einen längeren Urlaub als 30 Tage nimmt, was unschwer eintreten kann, da es sich um Kalendertage handelt und sechs Wochen Urlaub 42 Kalendertage umfassen. Hier wären jedenfalls Abwesenheiten aufgrund Mutterschaft und Urlaub ausdrücklich von der 30-Tage-Regelung auszunehmen.

Bei den Passwörtern (III D) wäre unter Ziffer 7 das Wort „aufschreiben“ zu streichen. Es kann jemandem verboten werden, sein Passwort irgendwo zu notieren, doch darf es dann nicht für andere zugänglich sein.

Was den in III I. erwähnten Fall des gekündigten Nutzers angeht, so ist auf die Ausführungen zu II 6 zu verweisen. Anders als in der IT-1 ist hier allerdings ausdrücklich bestimmt, wie nach der Meldung einer Kündigung zu verfahren ist. Es heißt:

„Alle Zugriffsmöglichkeiten auf Unternehmensinformationen müssen dann so schnell wie möglich ausgeschaltet werden, jedoch spätestens zwei (2) Werktage nach der Benachrichtigung, sofern eine weitere Nutzung des Kontos durch den gekündigten Nutzer nicht ausdrücklich vom Management genehmigt wurde.“

Konkret bedeutet dies, dass während des Laufs der Kündigungsfrist ein Zugriff im Regelfall ausgeschlossen ist. Während dieses Zeitraums hat der gekündigte Arbeitnehmer jedoch im Regelfall einen Beschäftigungsanspruch, der ohne Zugriff auf IT-Ressourcen nicht realisiert werden kann.

> Einen Beschäftigungsanspruch während des Laufs der Kündigungsfrist bejahen ausdrücklich BAG Urt. v. 19.8.1976 – 3 AZR 173/75 – AP Nr. 4 zu § 611 BGB

Beschäftigungspflicht und BAG GS Beschl. v. 27.2.1985 – GS 1/84 – NZA 1985, 702

Diese arbeitsrechtliche Rahmenbedingung hat das Management zu beachten, wenn es eine Weiternutzung genehmigt. Sinnvoll wäre es, die Genehmigung als Regelfall vorzusehen und eine Ausnahme für den Fall vorzusehen, dass der Arbeitgeber ein berechtigtes Interesse an der Nicht-Beschäftigung hat.

Die Ziffern (1) bis (4) der Abänderungsvorschläge von E. sind zu befürworten. Was Ziffer 5 betrifft, so müsste der Satz

„Bei den Ermittlungen und Entscheidungen werden die lokalen Gesetze berücksichtigt und es wird eine Einbeziehung des EHG-Betriebsrats in Betracht gezogen“

stringenter formuliert werden. Das deutsche Recht (das sich hinter dem Ausdruck „lokales Recht“ verbirgt) muss nicht nur „berücksichtigt“, sondern „beachtet“ werden. Außerdem ist der zuständige Betriebsrat nach BetrVG zu beteiligen; dies darf nicht nur „in Betracht gezogen“ werden.

Die Ergänzungen unter (6) sind zu befürworten. Dasselbe gilt für Ziffer (7) und (8).

2. IT-3: Nutzung von E-Mail und Internet

Auch bei dieser Richtlinie ergeben sich zahlreiche Fragen, die schon bei IT-1 behandelt wurden.

Dies gilt etwa für den Umgang mit Daten, die als Eigentum des Unternehmens betrachtet werden (III A). Dazu oben II 4.

Dasselbe gilt für die in III E angesprochene Aufbewahrung von E-Mails. Dazu oben II 5.

Die Änderungsvorschläge von E. unter (2), (3) und (4) sind zu befürworten. Was (1) betrifft, so ist auf die Ausführungen unter II 4 zu verweisen.

3. IT-4 bis IT-11

Die genannten Richtlinien betreffen nicht den Beschäftigtendatenschutz. Dies schließt nicht aus, dass z. B. Fragen des gewerblichen Rechtsschutzes bestehen, doch liegen diese außerhalb des Untersuchungsfelds dieses Gutachtens.

4. IT-12: IT-Mobilgeräte

Unklar ist, weshalb sich die Richtlinie nur auf Smartphones und Tablet-Computer, nicht aber auf Laptops bezieht. Dass diese bereits an anderer Stelle erwähnt sind, trifft zu, doch sind dort die besonderen Gefahren, die sich aus der Natur als beweglicher Gegenstand ergeben, nicht behandelt.

Unter III B 3 ist davon die Rede, die Mitarbeiter müssten die anwendbaren Gesetze des Bundes, der Länder und Gemeinden einhalten. Dies ist etwas missverständlich, da insbesondere im Datenschutz auch das Unionsrecht (DSGVO) zu beachten ist, und überdies in Europa Gemeinden keine Zuständigkeit für die hier geregelten IT-Fragen haben. Sinnvoll wäre, von der Beachtung des geltenden Recht, insbesondere des Unionsrechts und des nationalen Rechts zu sprechen.

Die Möglichkeit der Remote-Löschung, wenn das Gerät nicht mehr herausgegeben werden kann, ist zu befürworten.

Die Ergänzung zu III D 4 durch E. ist nachhaltig zu begrüßen; sie ist aus datenschutzrechtlichen Gründen geboten.

5. IT-13 und IT-14

Während die IT-13 (Zahlungskarten) keine spezifischen Probleme des Beschäftigtendatenschutzes aufzuwerfen scheint, gerät IT-14 (Reaktion auf Sicherheitsvorfälle) in Widerspruch zu der entsprechenden Regelung in der DSGVO, die eine Einschaltung der Aufsichtsbehörde und unter gewissen Voraussetzungen auch der betroffenen Person vorsieht. Die einschlägigen Vorschriften müssen etwas näher erläutert werden.

a) Die bisherige deutsche Regelung

Im Jahre 2009 wurde § 42a in das deutsche BDSG eingefügt, der den Sinn hatte, Maßnahmen der Schadensbegrenzung bei „Datenvorfällen“ zu begrenzen. Voraussetzung war, dass bestimmte Daten unrechtmäßig an Dritte übermittelt wurden oder diesen sonst wie zur Kenntnis gekommen waren, und zugleich »schwerwiegende Beeinträchtigungen« für die Rechte oder schutzwürdigen Interessen der Betroffenen drohten.

> Dies ist beispielsweise der Fall, wenn Adressdaten mit der Überschrift „Insassen einer Heilanstalt“ versehen sind – so Gola CuA 2/2010 S. 33

Trat eine solche Situation (verschuldet oder unverschuldet) ein, war zunächst die Aufsichtsbehörde zu informieren. Dies galt sogar dann, wenn nur »tatsächliche Anhaltspunkte« für eine derartige Datenpanne bestanden.

> Beispiel: Ein Laptop ging verloren (Gola CuA 2/2010 S. 33)

War die Sicherheitslücke geschlossen, mussten auch die Betroffenen ins Bild gesetzt werden, damit sie weitere Schutzmaßnahmen ergreifen konnten. War dies wegen ihrer großen Zahl nicht möglich oder nicht zumutbar, so musste durch zwei mindestens eine halbe Seite umfassende Anzeigen in bundesweit erscheinenden Tageszeitungen auf den Vorfall hingewiesen werden.

> Einzelheiten bei Schierbaum, CuA 2/2011 S. 28 ff.

Dies hat für die verantwortliche Stelle eine vergleichbare Bedeutung wie der Rückruf eines Produkts wegen nachträglich aufgetretener schwerer Mängel.

> Ernst, DuD 2010, 472

§ 42a BDSG alter Fassung wirkte deshalb auch präventiv im Sinne einer vollständigeren Datensicherung.

> Ernst, DuD 2010, 472. Zu den Bemühungen der Unternehmen um »Data Leakage

Prevention« s. Höller, CuA 4/2014 S. 33

Etwa zweieinhalb Jahre nach Inkrafttreten der Vorschrift hat die Bundesregierung dem Parlament einen Bericht erstattet, wonach insgesamt 305 Fälle nach § 42a angezeigt wurden, von denen aber nur 177 alle Tatbestandsmerkmale der Vorschrift erfüllt hatten.

BT-Drucksache 17/12319; dazu auch ZD Heft 7/2013 S. VII.

b) Das nunmehr geltende Recht des DSGVO

Die DSGVO hat den Grundgedanken des § 42a BDSG a.F. einschließlich des fehlenden Verschuldenserfordernisses beibehalten, jedoch einige Veränderungen vorgenommen. Zum einen ist die Interventionsschwelle niedriger, da schon die »Verletzung des Schutzes personenbezogener Daten« die Informationspflicht auslöst, ohne dass »schwerwiegende Beeinträchtigungen« drohen müssten. Stattdessen wird eine Ausnahme dann gemacht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem »Risiko für die Rechte und Freiheiten natürlicher Personen« führt.

Um welche Daten geht es? Nach Art. 33 Abs. 1 DSGVO geht es – zweiter Unterschied zum bisherigen Recht – um alle personenbezogenen Daten, während bisher nur sensitive Daten (einschließlich Daten zu strafbaren Handlungen und Ordnungswidrigkeiten) sowie solche erfasst waren, die einem Berufsgeheimnis unterlagen. Dazu kamen Daten zu Bank- und Kreditkartenkonten**.** Nach der jetzt erfolgten Erweiterung werden diese selbstredend weiterhin erfasst, doch sind auch sonstige, scheinbar harmlose Daten einbezogen.

Ereignet sich ein Datenschutzverstoß, so muss die Aufsichtsbehörde nach näherer Maßgabe des Art. 33 Abs. 2 DSGVO davon informiert werden. Zu beschreiben sind u. a. die Art der Datenschutzverletzung sowie ihre wahrscheinlichen Folgen.

Näher Schierbaum CuA 6/2018 S. 34

Dies kann in einem Unternehmen eine nicht leicht zu bewältigende Aufgabe sein, ebenso ist eine Behörde gut beraten, wenn sie sich auf einen solchen Fall vorbereitet.

Vgl. Ehmann/Kranig, ZD 2018, 199, 201: Simulation einer Mitteilung in dem hypothetischen Fall, dass ein nicht gesicherter Laptop in einem öffentlichen Verkehrsmittel abhanden kommt.

Der Verantwortliche muss außerdem nach Art. 33 Abs. 5 DSGVO alle Fakten dokumentieren, die im Zusammenhang mit der Datenschutzverletzung stehen, damit sie der Aufsichtsbehörde im Falle einer näheren Befassung mit dem Problem zur Verfügung stehen.

Besteht ein „hohes Risiko“ für die persönlichen Rechte und Freiheiten der betroffenen Person, so hat der Verantwortliche diese unverzüglich von der Verletzung zu unterrichten. Diese Verpflichtung besteht nicht, wenn der Verantwortliche durch seine nachfolgenden Maßnahmen für die nötige Datensicherheit gesorgt hat (Art. 34 Abs. 3 DSGVO). Im Einzelfall kann die Aufsichtsbehörde verlangen, dass dies nachgeholt wird, wenn das hohe Risiko für die betroffene Person in Wahrheit nicht beseitigt ist (Art. 34 Abs. 4 DSGVO).

Die Einschaltung der Aufsichtsbehörde ist unter diesen Umständen der Normalfall. Unterbleibt sie, kann nach Art. 83 Ab. 4 DSGVO ein Bußgeld von bis zu 10 Mio. Euro oder – soweit höher – bis zu 2 % des Weltkonzernumsatzes verhängt werden.