tration datenschutzaufsichtlicher Entscheidungszuständigkeiten am Sitz der Hauptniederlassung hat beim *Parlament* wie auch beim *Rat* Fragen und Vorbehalte ausgelöst, die vor allem auf das Verhältnis der für das Unternehmen verantwortlichen Behörde zu den mit Betroffenenanliegen befassten Datenschutzbehörden zielen.

Hinzu kommen generelle Fragestellungen zum Abstimmungsprozess der europäischen Datenschutzbehörden in Einzelfällen sowie zur Reichweite von Entscheidungen des künftigen europäischen Datenschutzausschusses.

Bislang ist es weder im *Parlament* noch im *Rat* in überzeugender Weise gelungen, praxistaugliche und effiziente Mechanismen für diese Aufgabenstellungen europäischer Verwaltungszusammenarbeit zu entwickeln. Sei es die Mitwirkung des *Europäischen Datenschutzbeauftragten* bei Beratungen über Einzelfragen des mitgliedstaatlichen Vollzugs der DS-GVO, sei es das nivellierende Mehrheitsprinzip oder die z.B. vom *Europäischen Parlament* vorgeschlagene Befugnis des europäischen Datenschutzausschusses zu verbindlichen Entscheidungen in Einzelfällen. Mit der den Mitgliedstaaten durch Art. 291 AEUV vorbehaltenen Primärverantwortung für den Vollzug des Gemeinschaftsrechts sind Kooperationen, Amtshilfe und unverbindliche Abstimmungsmechanismen, aber keine umfassenden Zuständigkeitsverlagerungen auf zentrale europäische Einrichtungen vereinbar.

Wie auch in anderen Rechtsgebieten kann Bürgernähe und damit der durch Art. 16 AEUV geforderte effektive Grundrechtsschutz nicht durch Zentralisierung, sondern nur durch mit starken Befugnissen ausgestattete Behörden vor Ort gewährleistet werden.

IV. Bewältigung von Grundrechtskonflikten

Spätestens seit der breiten Debatte um die *Google*-Entscheidung des *EuGH* ist klar geworden, dass die Mechanismen der DS-GVO zur Bewältigung von Konflikten zwischen Datenschutzbelangen und anderen Grundrechtspositionen stärker differenziert werden müssen. Erinnert man sich ferner an die umfassenden Anforderungen, die der *EuGH* ebenfalls erst jüngst an die Bewältigung von Grundrechtskonflikten im Fall der Verpflichtung der Mitgliedstaaten zur Regelung der Vorratsdatenspeicherung im TK-Bereich entwickelt hatte, treten weitere Nachbesserungserfordernisse im Bereich des Presse- und Mediendatenschutzes zu Tage.

Deshalb muss in den weiteren Beratungen das Spannungsverhältnis zwischen Datenschutz, Schutz der Privatsphäre, Meinungsfreiheit und anderen Informationszugangs- und Informationsverbreitungsinteressen schon innerhalb der Verordnung zumindest i.R.d. Schutzzielbestimmungen aufgegriffen werden.

Weitere Elemente wären eine spezifische, gerade unter den Bedingungen des Internet wichtige Regelung zum Umgang mit veröffentlichten Daten sowie Verfahrensmechanismen. Neben den vom *Bundesinnenministerium (BMI)* bereits zur Diskussion gestellten Streitschlichtungsmodellen könnte auch erwogen werden, in enger Anlehnung an die *Google*-Entscheidung des *EuGH* die zeitliche Dimension in stärkerem Maße i.R.d. datenschutzrechtlichen Erforderlichkeitsbeurteilung bzw. von Interessenabwägungstatbeständen zu berücksichtigen und rechtssetzend aufzugreifen.

Angesichts der ungeminderten Dynamik der Digitalisierung und der mit ihr allzu oft einhergehenden Risiken für die informationelle Selbstbestimmung hat die Reform des europäischen Datenschutzrechts nach wie vor hohe rechtspolitische Priorität.

Nach der Zäsur der Europawahlen sollte dem weiteren Reformprozess verstärkt der Ansatz zu Grunde gelegt werden, die globale Signalwirkung verbindlicher europäischer Standards und den Fortbestand heutiger Regelungen der Mitgliedstaaten zum Datenschutz zwischen Staat und Bürger wie auch deren dezentrale Vollzugserfahrung nicht als Gegensatz, sondern als gegenseitige Ergänzung und Verstärkung zu begreifen. Unter dieser Voraussetzung sollte es gelingen, der erfolgreichen Verabschiedung der DS-GVO ein deutliches Stück näher zu kommen.

Joachim Herrmann
ist Bayerischer Staatsminister des Innern, für Bau und Verkehr.
Das Bayerische Staatsministerium des Innern, für Bau und Verkehr begleitet die Beratungen zur DS-GVO in der Ratsarbeitsgruppe DAPIX im Auftrag des Bundesrats, vgl. Beschluss des Bundesrats v. 30.3.2012, BR-Drs. 52/12 (2).

THOMAS HOEREN

Das Konzerntelefonverzeichnis – ein datenschutzrechtlicher Sündenpfuhl?

Problemstellung und rechtliche Grenzen

Adressdatenbank
Dienstelefonnummern
Personenbezogene Daten
Vorratsdatenspeicherung
Einwilligung

■ Datenschutzaufsichtsbehörden haben in den letzten Jahrzehnten immer wieder konzernübergreifende Verzeichnisse von Diensttelefonnummern kritisiert. Das hat zu großer Unsicherheit in der Praxis geführt. Was darf in eine Adressdatenbank eines Unternehmens? Kann man das Problem mit dem Betriebsrat lösen? Wo genau liegen die rechtlichen Grenzen solcher Telefonverzeichnisse? Im folgenden Beitrag werden diese Themenkomplexe praxisnah aufbereitet.

■ In Germany, it is not allowed to store the business telephone numbers of employees in a big database. The data protection authorities have prohibited the processing of these data by big corporations. The author outlines the existing decision policy of these authorities and demonstrates how and under which circumstances these databases could be built up.

I. Einführung

2002 sorgte das *Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD)* für Aufruhr. Dort hatte jemand angefragt, ob ein konzernweites Intranet-Telefonbuch zulässig sei. Dies wurde in Kiel abgelehnt.[1] Die personenbezogenen Daten der Mitarbeiter verließen den Adressatenkreis des Unternehmens, sodass sie zur Abwicklung des Vertragsverhältnisses mit den Betroffenen nicht erforderlich seien. I.R.v. § 28 Abs. 1 Nr. 2 BDSG sei zu bedenken, dass eine ausnahmslose Veröffentlichung der Betroffenendaten dem Abwägungserfordernis nicht gerecht werde, da es vielfältige schutzwürdige Interessen der Betroffenen geben könne, die einer Verbreitung entgegenstehen.

Eine Rechtfertigung komme nur über eine freiwillige Einwilligung der Betroffenen oder den Abschluss einer Gesamtbetriebsvereinbarung in Betracht. Hilfsweise könne die Planung eines konzernweiten Intranet-Telefonbuchs auch vorab bekannt gemacht und den Betroffenen ein Widerspruchsrecht eingeräumt werden.[2] Im Weiteren soll geprüft werden, ob diese Aussage heute noch Bestand haben kann.

II. Vorüberlegungen

Unstreitig sind Namen, Vornamen, dienstliche Telefonnummer und ggf. dienstliche E-Mail-Adresse personenbezogene Daten i.S.v. § 3 Abs. 1 BDSG. Mit dem Wechsel von der Papier- in die EDV-Version liegt auch eine automatisierte Verarbeitung i.S.v. § 3 Abs. 2 Satz 1 BDSG vor. Insofern verkennen viele, dass die alten Adresslisten regelmäßig nicht Gegenstand einer datenschutzrechtlichen Prüfung sein konnten, da es an einer nicht-automatisierten Datei fehlte (§ 3 Abs. 2 Satz 2 BDSG).

Die Errichtung einer solchen Datenbank fällt verarbeitungstechnisch unter den Begriff der Speicherung (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG). Die Bereitstellung über das Intranet ist eine Übermittlung i.S.v. § 3 Abs. 4 Satz 2 Nr. 3 BDSG. Insofern greift zunächst einmal das Verbot der Datenverarbeitung nach § 4 Abs. 1 BDSG. Jetzt gilt es, die gesetzliche Ermächtigung oder die Einwilligung oder ggf. auch die Möglichkeit einer Betriebsvereinbarung zu prüfen.

Auf jeden Fall verboten ist die Erstellung von Telefonverzeichnissen mit den privaten Telefonanschlüssen aller Mitarbeiter. Der *Landesbeauftrage für den Datenschutz Sachsen-Anhalt* hat solche Telefonverzeichnisse als eine Art Vorratsdatenspeicherung zu unbestimmten künftigen Zwecken beanstandet und verurteilt.[3]

Die Einwilligung des Betroffenen sei die unpraktischste Lösung, schreibt das *ULD* selbst im o.g. Schreiben. Denkbar wäre es allerdings, schon im Einstellungsvertrag eine entsprechende Regelung zu den Telefondaten aufzunehmen. Eine solche Regelung ist nicht per se sittenwidrig; Einwilligungserklärungen in Arbeitsverträgen sind auch nicht per se unfreiwillig. Anders als noch 2002 ist es heutzutage Unternehmen auch problemlos möglich, die Einwilligung der Betroffenen einzuholen. So sind sog. „Self Services" für Mitarbeiter inzwischen gängig.

Denkbar wäre i.Ü. auch eine Regelung i.R.e. Betriebsvereinbarung. Nach Auffassung des *BAG* ist eine Verarbeitung von Arbeitnehmerdaten auch zulässig, sofern sie auf der Grundlage einer Ermächtigung in einem Tarifvertrag oder in einer Betriebsvereinbarung beruht.[4] Das *BAG* geht hierbei davon aus, dass es sich bei Tarifverträgen und Betriebsvereinbarungen um „andere Rechtsvorschriften" i.S.d. § 4 Abs. 1 BDSG handelt. Eine Verarbeitung personenbezogener Daten soll auf der Grundlage einer entsprechenden kollektivrechtlichen Regelung nach Auffassung des *BAG* selbst dann gerechtfertigt sein, wenn sich diese Vereinbarung zu Lasten des Betroffenen auswirkt.[5]

III. Verarbeitung i.R.d. Arbeitsvertrags

Abseits von Einwilligung und Betriebsvereinbarung sind § 32 Abs. 1 oder § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu prüfen. Nach § 32 Abs. 1 Satz 1 dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Fraglich ist, ob und inwieweit ein konzernweites Verzeichnis von Diensttelefonnummern als für das Arbeitsverhältnis erforderlich und angemessen angesehen werden kann. Diese Fragestellung wurde in einem Arbeitsbericht der *Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer"* vom *Regierungspräsidium Darmstadt* ausführlich geprüft.[6] In der Studie wurde eine Verarbeitung für zulässig erachtet, sofern es für die Erbringung der Arbeitsleistung jedes Mitarbeiters aktuell erforderlich sei, dass jeder auf die dienstlichen Kommunikationsdaten aller anderen aufgeführten Mitarbeiter zugreifen könne. Es komme spezifisch darauf an, ob es notwendigerweise zum Berufs- und Beschäftigungsprofil gehöre, dass jeder mit jedem telefonisch kommunizieren könne. Weitere Erläuterungen fehlen in dem Bericht.

Entscheidend ist insofern also der Einzelfall. Nicht jeder Beruf ist zwingend mit der Notwendigkeit freier wechselseitiger Kommunikation über Telefone verknüpft.

IV. Verarbeitung nach Güterabwägung

Dann gilt es zu prüfen, ob die Speicherung und Übermittlung der genannten Daten nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig ist. Dabei sei unterstellt, dass diese Vorschrift überhaupt neben § 32 BDSG zur Anwendung kommen darf.[7]

Eine Rechtfertigung über die Güterabwägung wäre möglich, wenn ein solches Verzeichnis zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass der Schutz für die Interessen des Betroffenen an dem Ausschuss der Verarbeitung oder Nutzung überwiegt.

Der Kieler Datenschutzbeauftragte, *Dr. Thilo Weichert*, erwähnt hier nur sehr nebulös, „dass vielfältige schutzwürdige Interessen der Betroffenen" einer Verbreitung entgegenstehen könnten. Unklar ist, was das für schutzwürdige Interessen sein sollen. Ein Recht auf Vergessenwerden am Arbeitsplatz oder ein „right to be let alone" ist arbeitsrechtlich kaum denkbar. Erinnert sei an den Beschluss des *BVerwG* v. 12.3.2008.[8] Hier hatte das *Gericht* darauf hingewiesen, dass z.B. ein Bediensteter einer Behörde keinen Anspruch darauf habe, vom Publikumsverkehr und von der Möglichkeit, postalisch oder elektronisch von außen kontaktiert zu werden, abgeschirmt zu werden.

Noch schärfer formuliert das Gericht: „Mit der Nennung des Namens, der Dienstbezeichnung, der dienstlichen Telefonnummer und der dienstlichen E-Mail-Adresse des Beamten werden keine

---

1 Schreiben v. 22.8.2002: Firmenintranet: Einführung eines unternehmensübergreifenden Konzern-Telefonbuchs (August 2002), abrufbar unter: https://www.datenschutzzentrum.de/wirtschaft/praxis/20020822.htm.

2 Schreiben v. 22.8.2002 (o. Fußn. 1).

3 *Landesbeauftragter für den Datenschutz Sachsen-Anhalt*, 3. TB 1995-1997, Ziff. 18.7.

4 *BAG*, B. v. 27.5.1986 – 1 ABR 48/84.

5 Krit. *Rademacher/Latendorf*, CR 1989, 1105; *Wohlgemuth*, Datenschutz für Arbeitnehmer, 2. Aufl., Rdnr. 613; *Walz*, in: Simitis, BDSG, 8. Aufl., § 4 Rdnr. 16; *Fitting u.a.*, BetrVG, 27. Aufl., § 83 Rdnr. 28.

6 S. Rdnr. 6.1; der Bericht ist abrufbar unter: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/5_Beschaeftigtendatenschutz_Konzern/arbeitspapier_ad_hoc_idv.pdf.

7 Dazu *Gola/Schomerus*, BDSG, 11. Aufl. 2012, § 32 Rdnr. 33 f. m.w.Nw.

8 *BVerwG*, B. v. 12.3.2008 – 2 B 131.07.

in irgendeiner Hinsicht schützenswerten personenbezogenen Daten preisgegeben, sodass sich die Frage einer für Eingriffe in individuelle Rechte erforderlichen Ermächtigungsgrundlagen nicht stellt."

Diese Argumentation gilt nicht nur für Beamte oder Bedienstete der öffentlichen Hand. Jemand, der in einem Konzern einen Arbeitsvertrag unterschreibt, muss damit rechnen, dass seine Dienstdaten innerhalb des Konzerns genutzt werden. Ein Risiko der Persönlichkeitsverletzung oder des Missbrauchs dieser Daten ist nicht zu erkennen. Vielmehr gehört die Erreichbarkeit heutzutage zu den zwingenden Notwendigkeiten auch im Konzern. Es muss möglich sein, einen Kollegen als Ansprechpartner oder für eine Zusammenarbeit ausfindig zu machen, seine Zuständigkeit im jeweiligen Unternehmen festzustellen und ihn entsprechend zielgerecht zu kontaktieren.

Andere Datenschutzaufsichtsbehörden formulieren dementsprechend vorsichtiger und i.E. liberaler. So heißt es im Bericht der *Hessischen Landesregierung* zur Tätigkeit der Datenschutzaufsicht[9] sehr kurz und bündig: „Die Erstellung eines konzernweit verfügbaren Telefonverzeichnisses mit Namen, dienstlicher Anschrift, Aufgabengebiet, dienstlicher Telefon- und Faxnummer sowie E-Mail-Adresse ist grundsätzlich als zulässig zu bewerten, denn es entspricht der legitimen Erwartung, eine ebenso schnelle wie reibungslose konzerninterne Kommunikation herzustellen". Ähnlich sieht dies schon 1996 die *Aufsichtsbehörde in Baden-Württemberg*.[10]

Ähnlich abwägend stellt die o.g. *Ad-hoc-Gruppe* entscheidend auf das Vorliegen eines berechtigten Interesses des Arbeitgebers ab.

Dort heißt es: „Ein berechtigtes Interesse des Arbeitgebers oder anderer konzernangehöriger Unternehmen kann jedoch nur anerkannt werden, wenn zumindest ein vernünftiger Grund für ein konzernweites Verzeichnis besteht (z.B. zentrale Versendung von E-Mails zur zeitgleichen Information aller Mitarbeiter; grundsätzliches Erfordernis in der Kommunikation zwischen den Mitarbeitern verschiedener Konzernunternehmen)." Besondere Bedenken gegen ein einheitliches Konzernverzeichnis sah man seitens der *Ad-hoc-Gruppe* vor allem bei sog. Nicht-Funktionsträgern; der Text verweist als Beispiel auf die Schreibkraft oder den LKW-Fahrer. Es müsse im Hinblick gerade auf deren schutzwürdige Belange die beabsichtigte Erstellung des Verzeichnisses vorher bekannt gemacht werden, damit Betroffene besondere Gründe vortragen können, die einer Aufnahme in das Verzeichnis entgegenstehen.[11]

Auch im Bericht[12] der *Hessischen Landesregierung* wird darauf verwiesen, dass im Einzelfall eine Zugriffsbeschränkung auf Teile des Verzeichnisses geboten sein kann, soweit diese für die konzerninterne Kommunikation genügt.

V. Fazit

I.E. sei – auch zur Ehrenrettung des *ULD* – darauf verwiesen, dass für konzernweite Telefonverzeichnisse eine Freizeichnung über die Güterabwägung nicht pauschal möglich ist. Es gilt, den Einzelfall im Blick zu behalten und die jeweilige konkrete Konzernstruktur zu prüfen. Sprechen vernünftige betriebstechnische Gründe für ein solches Verzeichnis, dürfte es die Güterabwägung von § 28 Abs. 1 Satz 1 Nr. 2 BDSG überspringen.

Vorsicht ist dabei immer bei der Nutzung von Daten geboten, die sich auf Nicht-Funktionsträger beziehen. Auch bietet es sich an, die Betroffenen vorab zu informieren (ggf. auch über den Betriebsrat) und ihnen notfalls ein Widerspruchsrecht aus wichtigem Grund einzuräumen. Ansonsten bleibt die Alternative Betriebsvereinbarung, die ohnehin zur Einführung von Telefonanlagen abgeschlossen werden müsste.

Professor Dr. Thomas Hoeren
ist Direktor der Zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) in Münster und Mitherausgeber der ZD.

9 Bericht v. 26.11.2002, LT-Drs 15/4659.
10 Hinweis zum BDSG Nr. 34, Staatsanzeiger für Baden-Württemberg v. 2.1.1996, Nr. 10, S. 10; anders aber das *ULD* (o. Fußn. 1), das zwar die schnelle Kommunikation als konzernrelevantes berechtigtes Interese ansieht, aber dann den Akzent sehr stark auf das Schutzinteresse des Betroffenen legt.
11 Arbeitsbericht der *Ad-hoc-Gruppe „Konzerninterner Datentransfer"* (o. Fußn. 6).
12 Vgl. o. Fußn. 9.

CHRISTOPH BAUSEWEIN

Arbeitgeber-Persönlichkeitstests – datenschutzrechtlich zulässig?

Bewerberauswahl und Personalentwicklung mittels psychischer Eignungstests

Beschäftigtendatenschutz
Löschroutine
Bewerbungsverfahren
Erlaubnis

■ Wer per Internetsuchmaschine Informationen rund um das Stichwort „Persönlichkeitstest" sucht, wird feststellen, dass das Angebot für Persönlichkeitstests zur Bewerberauswahl bzw. Mitarbeiterbewertung überwältigend ist und sich die Anbieter auf dem Markt für derartige Personaldienstleistungen mit Werbeaussagen geradezu überschlagen. Die Datenschutzaufsichtsbehörden haben sich mit dem Thema bis dato nicht offiziell befasst. Auch die Rechtsprechung gibt nur wenig Anhaltspunkte für eine zuverlässige Bewertung. Vor diesem Hintergrund möchte dieser Beitrag Grundlagenwissen über Persönlichkeitstests vermitteln, Orientierungshilfe geben und aufzeigen, unter welchen Umständen die Durchführung von Persönlichkeitstests datenschutzrechtlich zulässig ist.

■ When searching the Internet's search engines for the topic of "personality tests" one will find that there is an overwhelmingly wide range of personality tests for choosing applicants or assessing co-workers and the suppliers on the market nearly fall over themselves with advertisement statements for those personnel services. The data protection authorities have not officially dealt with this topic to date. Adjudication also only gives few reference points for a reliable assessment. In view thereof, this article will provide basic knowledge on personality tests, give orientation and show under which circumstances the execution of personality tests is permissible in regards to data protection law.