Pre-Employment-Screening 2.0

Über die Zulässigkeit der Recherche von Bewerberdaten in sozialen Netzwerken – *Annemarie Aumann**

Bei Anbahnung eines Arbeitsverhältnisses bieten soziale Netzwerke dem potentiellen Arbeitgeber die Möglichkeit, sich ein differenziertes und durchaus auch privates Bild vom Bewerber zu machen. Die rechtliche Zulässigkeit solcher Auswertungen ist indes problematisch.

I. Einführung und Fallbeispiel

Die Geschichte, der Freund eines Freundes habe seinen Traumjob nicht bekommen, weil der Arbeitgeber bei Facebook auf ein wildes Partybild gestoßen ist, hat wohl jeder schon gehört. Auch wenn es sich dabei um ein modernes Wandermärchen[1] handeln dürfte, trifft es doch ein reales Problem: Tatsächlich informierten sich bereits im Jahr 2009 36 % der deutschen Unternehmen in sozialen Netzwerken über ihre Bewerber,[2] wobei von steigenden Zahlen ausgegangen werden darf. Arbeitgeber bedienen sich dabei nicht nur berufsorientierter (wie XING, LinkedIN), sondern auch privatorientierter Netzwerke (wie Facebook, VZ-Gruppe, Pafnet). Pre-Employment-Screening nennt sich der Prozess, bei dem der Arbeitgeber den Bewerber vor einer Einstellungsentscheidung möglichst genau durchleuchtet, um angesichts strenger Arbeitnehmerschutzvorschriften sicherzustellen, dass der Kandidat die richtige Wahl ist. Der Bewerber dagegen möchte möglichst nur seine besten Eigenschaften offenlegen. Es stehen sich also das auf der Vertragsfreiheit beruhende Informationsinteresse des Arbeitgebers (Art. 2 Abs. 1 GG) und das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) des Bewerbers gegenüber.

Wie dieser Konflikt bei der Datenerhebung, -verarbeitung und -nutzung im Arbeitsverhältnis aufzulösen ist, ist derzeit im Bundesdatenschutzgesetz (BDSG) geregelt, das allerdings als in der Praxis schwer handhabbar empfunden wird.[3] 2010 brachte die Regierung daher einen Gesetzesentwurf für eine Neuregelung des BDSG in den Bundestag ein,[4] die den Datenschutz im Beschäftigungsverhältnis spezifischer regeln und damit Rechtssicherheit schaffen sollte. Allerdings ist das Gesetzgebungsverfahren ins Stocken geraten. Ob der viel kritisierte[5] Entwurf in der jetzigen Form Gesetz wird, ist zweifelhaft, insbesondere weil die Europäische Kommission inzwischen eine Datenschutz-Grundverordnung[6] vorgeschlagen[7] hat, die der Gesetzgeber wohl noch abwarten wird.[8] Der vorliegende Beitrag beschäftigt sich daher in der Hauptsache mit der aktuellen Gesetzeslage, während mögliche zukünftige Regelungen nur schlaglichtartig beleuchtet wer-

*Die Autorin ist Doktorandin am Max-Planck-Institut für Sozialrecht und Sozialpolitik. Sie dankt Prof. Richard Giesen und Ass. jur. Jacek Kielkowski für ihre wertvolle Mitarbeit. Der Beitrag entstand auf der Grundlage einer unter der Betreuung von Prof. Volker Rieble angefertigten Seminararbeit im Rahmen des Seminars: „Crossing Borders: HRM trifftArbeitsrecht".

1 Neudeutsch *urban legend*, oder auch *FOAF (Friend of a friend) tale* genannt.

2 So eine 2009 durchgeführte Studie des Dimap-Instituts, abrufbar unter http://www.bmelv.de/cln_154/SharedDocs/Downloads/Verbraucherschutz/InternetnutzungVorauswahlPersonalentscheidungen.html, zuletzt abgerufen am 12.07.12.

3 *Straube/Klagges*, ArbRAktuell 2012, 81 (81).

4 BT-Drs. 17/4230.

5 Siehe nur *Ernst*, NJOZ 2011, 953; *Thüsing*, NZA 2011, 16; *Kort*, MMR 2011, 294; *Forst*, NZA 2010, 427, alle m.w.N.

6 Dazu in diesem Heft *Sommerrock*, #

7 Vorschlag der Kommission abrufbar unter http://ec.europa.eu/justice/data-protection/document/review2012/com 2012 11 de.pdf.

8 *Straube/Klagges*, ArbRAktuell 2012, 81 (81); ebenso zweifelnd *Kania/Sansone*, NZA 2012, 360.

den. Dabei wird zunächst die rechtliche Zulässigkeit des Pre-Employment-Screenings anhand der verschiedenen möglichen Rechtsgrundlagen untersucht (II.). Insbesondere werden Orientierungshilfen zu entwickeln sein, anhand derer das generelle Erfordernis einer Verhältnismäßigkeitsprüfung im konkreten Fall mit Inhalt gefüllt werden kann (II.3.b). Im Anschluss daran werden die Konsequenzen von Verstößen gegen die vorgestellten Regelungen aufgezeigt (III.). Sodann wird im Ergebnis festzustellen sein, dass man als Bewerber gut daran tut, in sozialen Netzwerken mit persönlichen Angaben vorsichtig umzugehen (IV.).

Zum besseren Verständnis der Untersuchung diene folgendes Fallbeispiel:
P, Personalmanager der M GmbH, veröffentlicht folgende Stellenanzeige:

> **Teamleiter Quality Management (m/w)**
> **Ihre Aufgabe:** Die Leitung des Teams.
> **Ihr Know-How:** Erfahrungen in der Luftfahrtbranche; Teamfähigkeit.
>
> Um Sie kennen zu lernen, greifen wir auch auf soziale Netzwerke zu.

Daraufhin bewirbt sich B per Email. P möchte sich ein besseres Bild von B machen und dessen Angaben überprüfen. Er recherchiert daher auf den Profilen des B bei Facebook und XING und findet jeweils folgende Daten:
Ein Mannschaftsfoto des Fußballvereins X, auf dem B zu sehen ist,
Bs Mitgliedschaft in der Gruppe „Ich bin schwul, und das ist gut so!".
Variante 1: P findet die Daten bereits bei einer Suchmaschinenanfrage.
Variante 2: Bs Profil ist nur für Netzwerkmitglieder sichtbar. P registriert sich in beiden Netzwerken, um die Daten einsehen zu können.
Variante 3: Bs Profil ist nur für Kontakte zugänglich. P bietet B in beiden Netzwerken die Freundschaft/den Kontaktschluss an, B nimmt jeweils an.
Variante 4: P findet auf dem Profil des C den Status „Saufen mit B war gestern wieder geil!".
Darf P die Daten erheben und verwenden?

II. Rechtliche Zulässigkeit der Erhebung und Verwendung personenbezogener Bewerberdaten in sozialen Netzwerken

1. Zur Systematik des BDSG

Um die Zulässigkeit der Recherche von Bewerberdaten in sozialen Netzwerken prüfen zu können, sind zunächst einige einführende Worte zur Systematik des BDSG von Nöten. Dieses Gesetz ist gem. § 1 Abs. 2 Nr. 3 BDSG auf personenbezogene Daten anwendbar. Darunter sind gem. § 3 Abs. 1 BDSG Einzelangaben über die Verhältnisse einer Person zu verstehen. Dazu gehören Alter, Geschlecht, Name oder Wohnort genauso wie „softe Faktoren", also etwa Teamfähigkeit, Wechselwilligkeit oder Alkoholgeneigtheit. Im Fall kann P etwa aus dem Mannschaftsfoto auf Bs Teamfähigkeit schließen und aus der Angabe, „Saufen mit B" sei „geil", eine Alkoholgeneigtheit des B folgern.

Das BDSG unterscheidet zwischen einfachen und besonderen personenbezogenen Daten. Besondere personenbezogene Daten sind in § 3 Abs. 9 BDSG abschließend aufgezählt und beinhalten rassische und ethnische Herkunft, politische, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Sie werden anhand einzelner Erlaubnisnormen stärker geschützt. Im Beispielsfall gehört die aus der Gruppenzugehörigkeit folgende sexuelle Orientierung des B zu den besonderen personenbezogenen Daten.

Des Weiteren differenziert das BDSG zwischen Datenerhebung und -verwendung: Erheben ist das Beschaffen von Daten (§ 3 Abs. 3 BDSG), wofür gezieltes Lesen ausreicht.[9] Verwendung dagegen ist die Verarbeitung und Nutzung von Daten (Gegenschluss aus § 3 Abs. 5 BDSG). Recherchiert der Arbeitgeber, sind also die Vorschriften über die Erhebung anzuwenden, während bei der aktiven Abwägung der Rechercheergebnisse in der Einstellungsentscheidung die Vorschriften über die Verwendung einschlägig sind. Allerdings unterstellt das BDSG beide Prozesse denselben Voraussetzungen, sodass sie hier gemeinsam geprüft werden können.

Im Anschluss an die soeben vorgestellten Definitionsnormen stellt das BDSG seinem besonderen Teil als allgemeine Regel einen wichtigen Grundsatz voran: In § 4 Abs. 2 S. 1 BDSG ist der Direkterhebungsgrundsatz normiert. Er besagt, dass Daten grundsätzlich beim Betroffenen selbst zu erheben sind. Im hier zu untersuchenden Fall weicht der Arbeitgeber von diesem Grundsatz ab, indem er sich bei Dritten – nämlich in sozialen Netzwerken – informiert. Dies ist nur zulässig, wenn entweder eine Einwilligung vorliegt (dazu sogleich, II.2.) oder die zusätzlichen Anforderungen des § 4 Abs. 2 S. 2 BDSG erfüllt sind. Diese setzen in ihrer wichtigsten Alternative voraus, dass eine Rechtsvorschrift existiert, welche die Erhebung bei Dritten vorsieht. Solche Vorschriften sind insbesondere § 32 BDSG (dazu II.3.) und der dazu subsidiäre, nur teilweise anwendbare § 28 BDSG (dazu II.4).

§ 4 Abs. 2 S. 2 BDSG ermöglicht die Datenerhebung bei Dritten zudem für den Fall, dass die zu erfüllende Aufgabe dies erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Dabei dürfen zudem keine Anhaltspunkte für eine Beeinträchtigung überwiegender Interessen des Betroffenen bestehen.

9 *Gola/Schomerus,* BDSG, 10. Aufl. 2010, § 3 Rdn. 24.

2. Zulässigkeit aufgrund Einwilligung, § 4a BDSG

a) Wirksamkeitsvoraussetzungen der Einwilligung

§§ 4 Abs. 1, 4a BDSG sehen vor, dass der Bewerber in die Datenerhebung und -verwendung einwilligen kann. Auf den ersten Blick scheint dies eine ideale Lösung für den Arbeitgeber zu sein: Er könnte bereits in der Stellenanzeige darauf hinweisen, dass er sich auch in sozialen Netzwerken informieren möchte, so wie es im Beispielsfall gezeigt ist. Vorstellbar ist, dass eine daraufhin erfolgende Bewerbung als konkludente Einwilligung gesehen werden kann, so dass der Arbeitgeber ohne großen Aufwand rechtlich einwandfrei alle Informationen beschaffen und verwerten könnte, nach denen ihm der Sinn steht.

§ 4a BDSG betont allerdings zum Zwecke des Arbeitnehmerschutzes, dass die Einwilligung auf einer freien Entscheidung des Betroffenen beruhen muss, der zudem auf den Zweck des Datenumgangs hingewiesen worden sein muss. Der Bewerber muss also ohne Zwang handeln und die Tragweite seiner Entscheidung überblicken können.

Problematisch erscheint insbesondere das Merkmal „ohne Zwang". Mit der Begründung, dass ein klares Verhandlungsungleichgewicht zwischen Arbeitnehmer und Arbeitgeber besteht, schließt etwa die EU-Kommission in Art. 7 Abs. 4 ihres Vorschlags einer Datenschutz-Grundverordnung die Möglichkeit einer Einwilligung im Arbeitsverhältnis grundsätzlich aus.[10] Auch der Bewerber ist zumeist in einer dem Arbeitnehmer vergleichbaren, strukturell schwachen Position: Von der Einstellung hängt oft nicht nur seine berufliche Zukunft, sondern auch seine finanzielle Existenz ab. Auch wenn er eigentlich nicht einverstanden ist, wird er häufig einwilligen, um keinen schlechten Eindruck zu erwecken.[11] Damit ist der Bewerber einem – der Situation des Arbeitnehmers durchaus vergleichbaren – faktischen Zwang ausgesetzt.[12] Daraus wird vielfach eine (widerlegbare) Vermutung für die Unfreiwilligkeit einer Einwilligung hergeleitet,[13] mit der Folge, dass eine Einwilligung nur in Ausnahmefällen – etwa bei besonders geringer Schutzbedürftigkeit der Daten – möglich wäre.[14]

Trotz aller Schutzwürdigkeit des Bewerbers darf aber nicht übersehen werden, dass ein so weitgehendes Einwilligungsverbot Arbeitnehmern das Recht nähme, eigenverantwortlich darüber zu entscheiden, welche personenbezogenen Daten sie preisgeben wollen.[15] Diese Dispositionsbefugnis ist jedoch grundrechtlich geschützt:[16] Sie gehört zum Kernbereich des Rechts auf informationelle Selbstbestimmung.[17] Eine Vermutung für die Unfreiwilligkeit spricht Bewerbern ihre Mündigkeit ab.[18] Selbstbestimmt und eigenverantwortlich entscheiden zu können, gehört aber häufig sogar zu den Einstellungskriterien. Eine pauschale Lösung ist deswegen nicht angemessen. Richtig ist vielmehr, die Freiwilligkeit im Einzelfall zu überprüfen.[19] Damit wird nicht in die Entscheidungsfreiheit der Betroffenen eingegriffen, während der Grundrechtsschutz gewährleistet bleibt, was einen interessengerechten Ausgleich ermöglicht. Insbesondere bei hoch qualifizierten Bewerbern, die sich nicht zwangsläufig in einer schwächeren Position als der Arbeitgeber befinden, erscheint eine Gesamtabwägung im Einzelfall sachgerecht.

Allerdings kann der Bewerber nicht in jede Datenerhebung und -verwendung einwilligen. Insbesondere ausdrückliche Erhebungsverbote können nicht durch eine Einwilligung beseitigt werden (§ 134 BGB),[20] da dem Bewerber insoweit die Dispositionsbefugnis fehlt. Absolute Erhebungsverbote ergeben sich etwa aus den Grundsätzen zum Fragerecht des Arbeitgebers, die von der Rechtsprechung entwickelt wurden.[21] Denn sie gestehen dem Arbeitgeber nur dann ein Fragerecht zu, wenn er an der Antwort ein „berechtigtes, billigenswertes und schutzwürdiges Interesse" hat.[22] Die Grenzen des Fragerechts sind auf die Datenerhebung bei Dritten zu übertragen, da es im Ergebnis keinen Unterschied macht, ob der Arbeitgeber nach einer Information fragt oder sie nach einer Einwilligung selbst erhebt.[23] Wonach der Arbeitgeber nicht fragen darf, dafür darf er also auch keine Einwilligung verlangen.

Handelt es sich um besondere personenbezogenen Daten (i.S.v. § 3 Abs. 9 BDSG) ist gem. § 4a Abs. 3 BDSG zusätzlich notwendig, dass sich die Einwilligungserklärung ausdrücklich auf die besonders geschützten Daten bezieht.

Weiterhin muss der Bewerber wissen, wozu genau er sich einverstanden erklärt. Dies verlangt auch die unionsrechtskonforme Auslegung des § 4a BDSG, die angezeigt ist, weil die Norm der Umsetzung von Art. 2 lit. h EG-Datenschutzrichtlinie (EG-DS) dient.[24] Dieser setzt voraus, dass die Einwilligung „für den konkreten Fall und in Kenntnis der Sachlage" erfolgt. Nach einer Ansicht muss diese Kenntnis bereits bei Einstellung der Daten in das Netzwerk vorliegen, da die Einwilligung gem. § 183 BGB gerade eine vorherige Einverständniserklärung sei.[25] Weil aber die meisten Bewerber ihr Profil in Netzwerken bereits vor der Bewerbung eingerichtet haben, käme damit kaum jemals eine Einwilligung in Betracht. Da aber nicht in die Einstellung, sondern in die

10 Vorschlag der Kommission abrufbar unter http://ec.europa.eu/justice/data-protection/dochument/review2012/com 2012 11 de.pdf, Begründung in Ziffer 34 der vorstehenden Gründe; näher bei *Straube/Klagges*, ArbRAktuell 2012, 81 (81).

11 *Rolf/Rötting*, RDV 2009, 263 (267).

12 *Schaar*, MMR 2001, 644 (644).

13 *Däubler*, in: Däubler/Wedde/Weichert (Hrsg.), BDSG Kompaktkommentar, 3. Aufl. 2010, § 4a Rdn. 23.

14 *Hilbrans*, in: Däubler/Hjort/Schubert/Wolmerath (Hrsg.), Arbeitsrecht, Individualarbeitsrecht mit kollektivrechtlichen Bezügen, Handkommentar, 2. Aufl. 2010, § 4a BDSG Rdn. 3.

15 *Gola/Schomerus* (Fn. 9), § 4a Rdn. 9.

16 *Thüsing*, NZA 2011, 16 (18), der allerdings nur bei bereits erfolgter Einstellungszusage von einer freien Entscheidung ausgeht.

17 BVerfGE 65, 1, 1. Leitsatz.

18 *Thüsing*, RDV 2010, 147 (149).

19 Ebenso *Zscherpe*, MMR 2004, 723 (727).

20 *Taeger*, in: Taeger/Gabel, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2010, § 4a Rdn. 17.

21 Überblick bei *Däubler* (Fn. 13), § 4a Rdn. 29.

22 BAG, Urt. vom 7.6.1984 – 2 AZR 270/83 – AP BGB § 123 Nr. 26; BAG, Urt. vom 5.10.1995 – 2 AZR 923/94 – AP BGB § 123 Nr. 40.

23 *Gola/Schomerus* (Fn. 9), § 4a Rdn. 7; *Wohlgemuth*, BB 1996, 690 (692).

24 *Däubler* (Fn. 13), § 4a Rdn. 19.

25 *Forst*, NZA 2010, 427 (431).

Erhebung der Daten eingewilligt werden soll, kann es richtigerweise nur darauf ankommen, dass die Einverständniserklärung zeitlich vor der Datenerhebung liegt. Der Zeitpunkt der Einstellung der Daten in das soziale Netzwerk dagegen ist insofern irrelevant.

b) Einwilligungserklärung

Die Einwilligungserklärung bedarf grundsätzlich der Schriftform. Andere Formen sind nur zugelassen, wenn besondere Umstände sie angemessen machen, § 4a Abs. 1 S. 3 BDSG. Da die Schriftform zum Schutz der Betroffenen als Regelfall normiert ist, ist die Norm restriktiv auszulegen.[26] Eine andere Form ist aber dann zulässig, wenn der Betroffene selbst ein Medium wählt, bei dem die Datenerfassung eine übliche Begleiterscheinung ist.[27] Bei einer Online-Bewerbung nach Hinweis genügt deswegen auch eine formlose Einwilligung etwa per E-Mail.[28] Auch in einem Kontaktschluss mit dem Arbeitgeber in einem sozialen Netzwerk ist daher eine Einwilligung zu sehen. Teilweise wird dafür verlangt, dass der Arbeitgeber bei der Kontaktanfrage auf die beabsichtigte Erhebung hinweist.[29] Dagegen spricht, dass er in einem berufsorientierten Netzwerk (wie XING, LinkedIn) nichts anderes bezwecken kann, als Daten zu erheben. Durch die individuelle Kontaktaufnahme wird dem Bewerber bewusst, dass und wem er Einblick in seine Daten gewähren soll. Klickt er auf „ja", erklärt er sich einverstanden. Die Kontaktanfrage des Arbeitgebers genügt deswegen als konkludenter Hinweis auf die Datenerhebung. In einem privatorientierten Netzwerk (wie Facebook, StudiVZ) dagegen darf schon nach den AGB der Betreiber[30] nur privat gehandelt werden. Hier braucht der Bewerber also nicht damit zu rechnen, dass Informationen im Bewerbungsprozess verwertet werden. Denn sonst müsste er davon ausgehen, dass sein zukünftiger Arbeitgeber gesetzeswidrig handelt. Es wäre aber widersinnig, wenn die Rechtsordnung dies von ihm verlangen würde. Daraus folgt, dass ein Freundschaftsschluss in einem privaten Netzwerk nicht als Einwilligung in berufsrelevante Datenerhebung zu verstehen ist, sodass der Arbeitgeber auch nach Kontaktschluss nach dem BDSG keine Daten aus privatorientierten Netzwerken sammeln darf, wenn er nicht spezifisch darauf hingewiesen hat.

Verlangt der Arbeitgeber schriftliche Einverständniserklärungen, ziehen nach der Erfahrung einer Detektei ca. 15 % ihre Bewerbung zurück.[31]

Auch eine konkludente Einwilligung ist, wenn sie eindeutig ist, einer ausdrücklichen Einwilligung gleichwertig.[32] Bewirbt sich jemand trotz arbeitgeberseitigen Hinweises, bedeutet dies, dass er mit dem Datenumgang einverstanden ist. Eine konkludente Einwilligung liegt dann schon in der Bewerbung selbst.[33] Der Bewerber kann dies verhindern, indem er im Anschreiben vermerkt, dass er keine Online-Recherche wünscht.

Für den Beispielsfall ergibt sich damit folgende Lösung: In den Varianten 1 und 2 hat B durch seine Bewerbung, in Variante 3 durch den Kontaktschluss konkludent in den Datenumgang eingewilligt. Seine Teamfähigkeit unterliegt keinem absoluten Erhebungsverbot, so dass P sie erheben und verwenden darf. Dies gilt jedoch nicht für die sexuelle Orientierung, weil der Arbeitgeber nicht nach dieser differenzieren und damit auch nicht danach fragen darf. Zudem bezog sich Bs Einwilligung nicht ausdrücklich auf dieses Datum.

In Variante 4 hat B den C nicht ausdrücklich genannt. Seine Einwilligung umfasst deswegen nicht das, was C auf seinem Profil veröffentlicht. P darf das Datum der Alkoholgeneigtheit des B nicht erheben.

c) Die Einwilligung im BDSGE

Im Zusammenhang mit dem eingangs erwähnten Gesetzesentwurf zur Änderung des BDSG (BDSGE) wurde die Einwilligung stark diskutiert. Der Entwurf sieht in § 32l Abs. 1 BDSGE zwar weiterhin eine Einwilligung vor, verbietet diese jedoch für alle Fälle, die nicht ausdrücklich in den §§ 32 bis 32l BDSGE vorgesehen sind. Eine solche Erlaubnisnorm ist § 32 Abs. 6 S. 4 BDSGE. Diese erlaubt die Datenerhebung bei sonstigen Dritten (also nicht allgemein zugänglichen Quellen),[34] wenn der Bewerber eingewilligt hat und eine Interessenabwägung durchgeführt worden ist, die zu Gunsten des Arbeitgebers ausfiel. Diese Regelung ist allerdings europarechtswidrig, da sie gegen Art. 7 lit. a EG-DS verstößt. Dort ist normiert, dass „die Verarbeitung [...] erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist: a) die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben". Unter Verarbeitung ist gem. Art. 2 lit. b EG-DS auch das Erheben von Daten zu verstehen. Die Einwilligung ist damit ausnahmslos möglich.[35] Bei der Richtlinie handelt es sich um eine Vollharmonisierungsvorgabe, da Ziel der Regelung gem. Erwägungsgrund 8 EG-DS[36] („Zur Beseitigung der Hemmnisse für den Verkehr personenbezogener Daten ist ein gleichwertiges Schutzniveau [...] unerlässlich. [...] Deshalb ist eine Maßnahme zur Angleichung der Rechtsvorschriften erforderlich.") die Herstellung der Gleichwertigkeit der einzelstaatlichen Datenschutzbestimmungen war.[37] Der deutsche Gesetzgeber darf

26 *Simitis*, in: Simitis (Hrsg.), BDSG Kommentar, 6. Aufl. 2006, § 4 Rdn. 33 ff.

27 *Däubler* (Fn. 13), § 4a Rdn. 15.

28 *Forst*, NZA 2010, 427 (431).

29 *Forst*, NZA 2010, 427 (432).

30 *Rolf/Rötting*, RDV 2009, 263 (266); Facebook AGB 4. Nr. 4, www.facebook.de, abgerufen am 20.7.2012; § 2 Nr. 6 Nutzungsbedingungen von pafnet.de, abrufbar unter www.pafnet.de, abgerufen am 20.7.2012. Anders die AGB berufsorientierter Netzwerke, vgl. AGB von XING, www.xing.de, abgerufen am 20.7.2012.

31 So *Lotze*, Geschäftsführer des Detektiv-Instituts Kocks, in: *Schleufe*, ZEIT Online vom 11.11.2010, www.zeit.de/karriere/bewerbung/2010-10/schummeln-bewerbungen, abgerufen am 20.7.2012.

32 *Däubler* (Fn. 13), § 4a Rdn. 16.

33 A.A. *Simitis* (Fn. 26) § 4a Rdn. 44.

34 BR-Drs. 535/10, S. 12.

35 *Forst*, NZA 2010, 1043 (1044).

36 Erwägungsgründe können zur Auslegung herangezogen werden, *GA Mazák*, in: Schlussanträge v. 15.2.2007, Rs. C-411/05, Slg. 2007, I-8531 Rdn. 51 – *Palacios*.

37 EuGH vom 20.5.2003, Rs. C-564/00, Slg. 2003, I-4989 Rdn. 39 – *Österreichischer Rundfunk*; *Brühann*, EuZW 2009, 639 (641).

daher keine strengeren Voraussetzungen als die durch die Richtlinie vorgegebenen an die Rechtfertigung der Datenerhebung knüpfen.[38] § 32l Abs. 1 BDSGE ist somit unionsrechtswidrig[39] und wäre wegen des Anwendungsvorrangs[40] von den Gerichten nicht anzuwenden.

d) Zwischenergebnis

Beachtet der Arbeitgeber die Voraussetzungen der Einwilligung, ist sie – entgegen bisheriger überwiegender Meinung im Schrifttum[41] – in der Praxis ein interessengerechtes und geeignetes Instrument für den Umgang mit Bewerberdaten, da sie einerseits dem Bewerber die volle Kontrolle über seine Daten belässt, andererseits aber dem Arbeitgeber eine unkomplizierte Möglichkeit der Datenerhebung eröffnet. Statt der m.E. europarechtswidrigen Fassung im BDSGE wäre es zu begrüßen, wenn der Gesetzgeber durch eine deutliche Stellungnahme in § 4a BDSG, wann eine andere Form als die Schriftform ausreichend ist, Rechtssicherheit schaffen würde.

3. Zulässigkeit gem. § 32 Abs. 1 S. 1 BDSG

Auch § 32 S. 1 BDSG ist eine Erlaubnisnorm für den Datenumgang i.S.v. § 4 Abs. 1 BDSG. Sie setzt voraus, dass Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben werden und dies für die Entscheidung über die Begründung eines solchen erforderlich ist. Gem. § 3 Abs. 11 BDSG gelten Bewerber als Beschäftigte, so dass § 32 S. 1 BDSG auf einfache personenbezogene Daten anwendbar ist. Auf besondere personenbezogene Daten ist § 32 S. 1 BDSG jedoch nicht anwendbar, sondern wird von § 28 Abs. 6 BDSG verdrängt. Dafür spricht eine unionsrechtskonforme Auslegung.[42] Denn Art. 8 Abs. 2 EG-DS verpflichtet den Gesetzgeber, besondere Arten personenbezogener Daten stärker zu schützen.[43] § 28 Abs. 6 BDSG tut dies, indem er verlangt, dass der Bewerber die Daten offenkundig selbst öffentlich gemacht hat.[44]

a) Direkterhebungsgrundsatz

Die Datenerhebung nach § 32 BDSG ist nach dem Direkterhebungsgrundsatz (§ 4 Abs. 2 S. 2, siehe oben II.1.) nur zulässig, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt oder die Indirekterhebung erforderlich ist und keine Anhaltspunkte für eine Beeinträchtigung überwiegender Interessen des Betroffenen bestehen. § 32 BDSG spricht zwar nicht von einer Datenerhebung bei Dritten. Zweck einer Erhebung von Bewerberdaten in sozialen Netzwerken ist es aber, zu überprüfen, ob der Bewerber richtige Angaben gemacht hat, und sich ein Bild von dessen Persönlichkeit zu machen. Diese Überprüfung verliert ihren Sinn, wenn sie unter Mitwirkung des Bewerbers geschieht. Damit ist die Indirekterhebung für den zu erfüllenden Zweck erforderlich i.S.v. § 4 Abs. 2 S. 2 Nr. 2 a) BDSG.

b) Interessenabwägung

Auch in § 32 S. 1 BDSG wird die Erforderlichkeit der Datenerhebung verlangt. Ob damit lediglich gemeint ist, dass die Datenerhebung notwendig sein muss,[45] oder eine Verhältnismäßigkeitsprüfung stattfinden soll, wird aus dem Wortlaut nicht deutlich. Laut Gesetzesbegründung ist erforderlich, was nach BAG und BVerfG vor Einführung des § 32 BDSG zulässig war,[46] also was dem Grundsatz der Verhältnismäßigkeit entspricht.[47] Eine Verhältnismäßigkeitsprüfung fand demnach stets statt.[48] Nähme man nun eine bloße Notwendigkeit an, wäre der Schutz des Betroffenen im Gegensatz zur „alten" Gesetzeslage verkürzt.[49] Gerade das war aber nicht Intention des Gesetzgebers.[50]

Die Datenerhebung muss damit auch verhältnismäßig sein, also einem legitimen Zweck dienen und geeignet, erforderlich und angemessen sein, um diesen Zweck zu erreichen. Dies hat der Arbeitgeber im Einzelfall zu prüfen. Legitimer Zweck ist gem. § 32 S. 1 BDSG, die Entscheidung über die Begründung eines Beschäftigungsverhältnisses zu ermöglichen. Geeignet ist, was zu dieser Entscheidung beitragen kann. Dies sind nur Daten, nach denen der Arbeitgeber bei der Einstellung auch differenzieren darf. Darf er Daten etwa nach § 8 Abs. 1 AGG von vornherein nicht berücksichtigen, sind sie deswegen schon nicht geeignet.

Erforderlich ist, für was es kein milderes und gleich effektives Mittel gibt. Als milderes Mittel kommt die Datenerhebung beim Bewerber selbst in Betracht.[51] Dabei besteht aber die Gefahr, dass der Arbeitgeber Falschinformationen bekommt.[52] Zudem erfährt der Arbeitgeber nur über die Online-Recherche, wie sich der Bewerber im Internet selbst präsentiert; auch diese Art der Selbstdarstellung sagt etwas über die Persönlichkeit des Anwärters aus. Die Erhebung bei Dritten ist daher erforderlich.

Bei der nun durchzuführenden Interessenabwägung müssen die Grundrechte beider Seiten beachtet werden, da diese nach der Theorie der mittelbaren Drittwirkung auch in das Privatrecht ausstrahlen.[53] Auf Seiten des Arbeitgebers sind besonders sein Informationsinteresse, aber auch wirtschaftliche Interessen, das Recht am eingerichteten und

38 *Brühann*, EuZW 2009, 639 (640 ff.); *Forst*, RDV 2010, 150 (152).
39 A. A. *Tinnefeld/Petri/Brink*, MMR 2010, 727 (729).
40 *Haltern*, Europarecht, Dogmatik im Kontext, 2. Aufl. 2007, Rdn. 934, 940.
41 *Rolf/Rötting*, RDV 2009, 263 (267).
42 *Forst*, NZA 2010, 427 (430).
43 Richtlinie 95/46/EG, ABlEG Nr. L-281 v. 23.11.1995, S. 31.
44 *Wank*, in: Müller-Glöge/Preis/Schmidt (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 11. Aufl. 2011, § 28 BDSG Rdn. 2.
45 *Vogel/Glas*, DB 2009, 1747 (1751); *Deutsch/Diller*, DB 2009, 1462 (1463).
46 BT-Drs. 16/13657, S. 21: „Die Regelung entspricht auch insoweit den bisher von der Rechtsprechung erarbeiteten Grundsätzen des Datenschutzes im Beschäftigungsverhältnis".
47 BAG, Urt. vom 7.9.1995 – 8 AZR 828/93, NZA 1996, 637; BAG, Urt. vom 22.10.1986 – 5 AZR 660/85, NZA 1987, 415.
48 *Rolf/Rötting*, RDV 2009, 263 (264).
49 *Schmidt*, RDV 2009, 193 (198).
50 BT-Drs. 16/13657, S. 20 f.
51 *Wybitul*, BB 2010, 1085 (1086).
52 *Lelley*, Personal 4/2009, 52 (52) schätzt den Anteil der Falschangaben auf bis zu 30 %.
53 BVerfG, Urt. vom 15.01.958 – 1 BVR 400/51, E 7, 198.

ausgeübten Gewerbebetrieb[54] sowie Art. 14 GG zu berücksichtigen. Diesen stehen das Recht des Bewerbers auf informationelle Selbstbestimmung[55], Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, und seine Berufsfreiheit gem. Art. 12 GG entgegen.

Im Folgenden werden einige Kategorien entwickelt, an denen sich der Arbeitgeber bei der Durchführung der Interessenabwägung orientieren kann: Art des Netzwerks, Schutzgrad, Aktualität, Urheberschaft und Sensibilität des Datums.

aa) Art des Netzwerks

Zugunsten des Arbeitgebers ist zu berücksichtigen, dass in berufsorientierten Netzwerken Daten gerade deswegen preisgegeben werden, um sich beruflichen Kontakten zu präsentieren. Dagegen spricht in privatorientierten Netzwerken für den Bewerber, dass diese laut ihren AGB gar nicht für geschäftliche Zwecke genutzt werden dürfen und er nicht damit rechnen muss, dass der Arbeitgeber mit ihrer Nutzung gegen die Vertragsbedingungen der Netzwerkbetreiber verstößt.[56]

bb) Schutzgrad

Je freizügiger ein Bewerber mit seinen Daten umgeht, desto weniger wird er sich auf sein informationelles Selbstbestimmungsrecht berufen können. Der Nutzer eines sozialen Netzwerks kann seine Informationen mit nachfolgenden Schutzgraden mit absteigender Schutzintensität versehen: Allgemein zugängliche Daten, nur Netzwerkmitgliedern zugängliche Daten, nur Kontakten von Kontakten zugängliche Daten, nur Kontakten zugängliche Daten. Welchen Schutzgrad der Bewerber für die jeweilige Information eingestellt hat, fließt maßgeblich in die Abwägung ein, da er die Daten in unterschiedlicher Intensität aus seiner Privatsphäre entlässt.

Allgemein zugängliche Daten sind solche, die einem individuell nicht bestimmbaren Personenkreis offen stehen.[57] Darunter fallen etwa Informationen, die per Suchmaschine auffindbar sind.[58] Bei diesen wird das Arbeitgeberinteresse zumeist überwiegen.[59] Denn wer seine Daten freiwillig der Allgemeinheit bekannt gibt, hat sein Recht auf informationelle Selbstbestimmung bereits ausgeübt. Er bedarf des Datenschutzes nicht mehr.[60] Das gilt aber nur, wenn der Bewerber die Daten selbst allgemein zugänglich gemacht hat.[61]

Einer Ansicht nach befinden sich auch Daten, die nur für Mitglieder eines sozialen Netzwerkes einsehbar sind, auf der niedrigsten Schutzstufe.[62] Argumentiert wird, dass sich nach einem einfachen Registrierungsprozess faktisch jeder binnen Minuten Zugriff beschaffen kann und die Daten insofern allgemein zugänglich seien.[63] Dabei wird jedoch verkannt, dass der Personenkreis jederzeit individuell bestimmbar ist und sich jeder Nutzer bei Registrierung den jeweiligen AGB unterwirft, die etwa in privatorientierten Netzwerken die Verwendung der Daten zu anderen Zwecken untersagen. Wer seine Daten bewusst nur für Mitglieder freigibt, will gerade nicht, dass sie für alle zugänglich sind. Derart zugriffsbeschränkte Daten sind daher richtigerweise schutzbedürftiger als allgemein zugängliche Daten.

Facebook erlaubt es, ein Profil für „Freunde von Freunden" freizuschalten; bei XING ist eine Stufung sogar bis zur Freigabe für „Mitglieder bis zum 4. Bekanntheitsgrad" möglich. Eine solche Stufung beeinflusst den Schutzgrad der Daten aber nur geringfügig. Möglicherweise können diese Daten zwar von einer geringeren Anzahl an Personen abgerufen werden als solche, die allen Mitgliedern des Netzwerkes zugänglich sind. Aber der Bewerber kann nicht kontrollieren, wer sein Kontakt zweiten oder höheren Grades wird, und gibt damit seine Daten der Verfügungsgewalt seiner bereits bestehenden Kontakte preis: Seine Daten kann etwa einsehen, wer sein Profil mit einem Kontakt seiner Kontakte verbindet. Der Schutzgrad ist deswegen nur geringfügig höher als bei nur Mitgliedern des Netzwerks zugänglichen Daten.

Den höchsten Schutzgrad besitzen Daten, die nur Kontakten zugänglich sind. Diese können nur von Profilinhabern abgerufen werden, die mit dem Profil des Bewerbers direkt verbunden sind. Verbinden kann man sich nur durch einen Kontaktschluss. Bei solchen Daten überwiegt grundsätzlich das Bewerberinteresse. Etwas anderes gilt, wenn der Bewerber dem Arbeitgeber durch den Kontaktschluss bewusst seine Daten freigegeben hat; dann ist er weniger schutzwürdig.[64]

cc) Aktualität

Auch die Aktualität der Daten muss in die Abwägung einfließen. „Längst vergangene Jugendsünden" sollen bei der Einstellung des Bewerbers keine Rolle spielen.[65] Je länger die Einstellung des Datums zurückliegt, desto weniger berechtigt ist das Interesse des Arbeitgebers an seiner Erhebung. Teilweise wird dafür eine Fünfjahresgrenze gefordert.[66] Eine solche pauschale Grenze widerspricht aber dem Sinn der Verhältnismäßigkeitsprüfung, gegenläufige Interessen gerade im Einzelfall in Einklang zu bringen, und ist daher abzulehnen.

dd) Urheberschaft

Auch wenn der Bewerber offensichtlich keinen Einfluss

54 *Kratz/Gubbels*, NZA 2009, 652 (653 f.).
55 BVerfG, Beschluss vom 24.5.1988 – 4 B 93/88, NJW 1988, 3031.
56 *Rolf/Rötting,* RDV 2009, 263 (266); Facebook AGB, pafnet.de Nutzungsbedingungen (Fn. 30).
57 BVerfG, Beschluss vom 3.10.1969 – 1 BvR 46/65, E 27, 73.
58 *Gola/Schomerus* (Fn. 9), § 28 Rdn. 33 a.
59 *Rolf/Rötting*, RDV 2009, 263 (266).
60 *Forst*, NZA 2010, 427 (430).
61 *Däubler* (Fn. 13), § 28 Rdn. 58 zählt Daten, die von Dritten allgemein zugänglich gemacht worden sind, nicht zu den allgemein zugänglichen Daten. Diese rein vom Ergebnis her gedachte Definition geht m.E. zu weit.
62 *Oberwetter,* BB 2008, 1562 (1564).
63 *Oberwetter*, BB 2008, 1562 (1564).
64 *Forst*, NZA 2010, 427 (432).
65 *Oberwetter*, BB 2008, 1562 (1564).
66 *Wellhöner/Byers*, BB 2009, 2310 (2315).

darauf hatte, dass Daten veröffentlicht wurden, erhöht das sein Interesse an der Nichterhebung.[67] Dies ist etwa der Fall, wenn es sich um ein Datum handelt, das von einem Dritten auf die Facebook-Pinnwand oder in das Gästebuch des Bewerbers eingestellt wurde.

ee) Sensibilität

Letztes Kriterium ist die Sensibilität des zu erhebenden Datums. Besondere personenbezogene Daten unterfallen von vornherein nicht § 32 BDSG und dürfen nicht erhoben werden. Des Weiteren sind die Grundsätze zum Fragerecht des Arbeitgebers vollständig zu übertragen. Die Interessen des Bewerbers überwiegen also immer dann, wenn kein Fragerecht besteht, d.h. der Bewerber ein Recht zur Lüge hat.[68]

Ob der Arbeitgeber ein konkretes Datum auf der Grundlage des § 32 BDSG erheben darf, lässt sich daher nicht pauschal beantworten, sondern erfordert stets eine genaue Interessenabwägung anhand der oben entwickelten Kriterien.

Am Beispielsfall ergibt sich nach alldem folgende Lösung:

In der Variante 1 – allgemein zugängliches Datum – ist das Datum der Teamfähigkeit von B für P wichtig, da er einen Teamleiter sucht. P hat daher ein hohes Interesse an der Erhebung. Dagegen fällt das Interesse des B geringer aus: Er hat das Datum allgemein zugänglich gemacht und insofern auf seinen Grundrechtsschutz verzichtet. P darf es also erheben.

Ist – wie in Variante 2 – das Datum nur Mitgliedern des Netzwerks zugänglich, kommt es darauf an, ob das Datum sich bei Facebook oder XING befindet. Im ersten Fall überwiegt das Interesse des B, so dass P das Datum nur aus XING erheben darf.

War das Mannschaftsfoto nur für Kontakte sichtbar, so ist B durch den Kontaktschluss bei XING weniger schutzbedürftig, so dass P das Datum dort erheben darf (aber nicht aus Facebook, vgl. II. 1. b.).

Da B in Variante 4 nicht beeinflussen kann, was über ihn auf Cs Profil steht, überwiegt sein Interesse. P darf die Alkoholgeneigtheit des B nicht erheben.

Da die sexuelle Orientierung ein besonderes personenbezogenes Datum ist, kommt § 32 Abs. 1 S. 1 BDSG nicht als Rechtsgrundlage für seine Erhebung in Betracht.

c) Tatsächliche Probleme der Interessenabwägung

Das Erfordernis einer solch umfassenden Interessenabwägung führt zu einem Paradoxon: Einerseits wird von dem Arbeitgeber verlangt, dass er eine Interessenabwägung anstellt, um herauszufinden, ob er das Datum überhaupt erheben darf. Um dies tun zu können, muss er aber das Datum bereits kennen, da er es sonst nicht in die Abwägung einstellen kann. Das Datum muss also erst erhoben werden, bevor geprüft werden kann, ob man es erheben darf. Stellt der Arbeitgeber nach Erhebung fest, dass er das Datum nicht hätte erheben dürfen, so darf er es anschließend nicht verwenden. Es ist aber realitätsfern, von einem Personaler zu verlangen, bei der Entscheidung etwas zu vergessen, was er bereits weiß; wenn er es nicht bewusst tut, so ist zumindest zu befürchten, dass er die Information bei seiner Entscheidung im Hinterkopf hat.

Dieses Problem lässt sich durch folgende Gestaltung lösen: Der Arbeitgeber weist nicht die Person, die die Personalentscheidung trifft, zur Durchführung der Recherche an, sondern überträgt diese Aufgabe einer dritten Person. Als „Datenfilter" trennt diese zur Erhebung zulässige und unzulässige Daten und leitet nur die zulässigen Daten an den Personaler weiter. Da der Personaler dann nur die Daten kennt, die er auch erheben hätte dürfen, kann er auch nur diese zur Einstellungsentscheidung heranziehen. Damit ist sichergestellt, dass die Einstellungsentscheidung datenschutzrechtlich einwandfrei gefällt wird. Dieses Einschalten einer dritten Person als „Datenfilter" würde auch die Beweisführung im Rahmen des § 22 AGG erleichtern, dass er Daten nur erhoben, bei der Personalentscheidung aber nicht verwendet hat (dazu sogleich, III.)

d) Verschärfung im BDSGE

Der Entwurf zur Neuregelung des Beschäftigtendatenschutzes sieht in § 32 Abs. 6 S. 2 BDSGE eine Verschärfung des Direkterhebungsverbotes in dem Sinne vor, dass eine Indirekterhebung nur noch möglich ist, wenn es sich um allgemein zugängliche Daten handelt, bei denen das schutzwürdige Interesse des Bewerbers nicht überwiegt. Die Abwägung nach dem Schutzgrad der Daten fällt damit weg. Für die dann durchzuführende Interessenabwägung finden sich im BDSGE zwei Fiktionen. Die Grunddaten Name, Anschrift, Telefonnummer und Emailadresse dürfen nach § 32 Abs. 1 S. 1 BDSGE stets erfragt werden. Nach gesetzgeberischer Wertung sind diese Daten für die Durchführung eines Bewerbungsverfahrens stets notwendig.[69] Daten, die „insbesondere" erhoben werden dürfen, sind gem. S. 3 fachliche und persönliche Fähigkeiten, Kenntnisse und Erfahrungen sowie Ausbildung und beruflicher Werdegang. Der Begriff „Fähigkeiten" umfasst dabei auch „soft skills" wie Teamfähigkeit oder Zuverlässigkeit.[70] § 32 Abs. 6 S. 3 BDSGE als ein „lex Facebook" normiert eine unwiderlegliche Vermutung dafür, dass bei Daten aus privatorientierten Netzwerken das Interesse des Bewerbers stets überwiegt.[71] Die Erhebung allgemein zugänglicher Daten aus Facebook oder StudiVZ ist deswegen in keinem Fall zulässig.

Zusätzliche Voraussetzungen für besondere personenbezogene Daten regelt der BDSGE in § 32 Abs. 2 S. 1. Besonders geschützt sind demnach rassische und ethnische Herkunft, Religion, Weltanschauung, Behinderung, sexuelle Identität, Gesundheit, Vermögensverhältnisse, Vorstrafen

67 *Forst*, NZA 2010, 427 (432).

68 *Zöll* (Fn. 20), § 32 Rdn. 19.

69 BR-Drs. 535/10, S. 9.

70 *Beckschulze/Natzel*, BB 2010, 2368 (2369).

71 § 32 Abs. 6 S. 3 BDSGE: „Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind."

und laufende Ermittlungsverfahren. Für die Schwerbehinderteneigenschaft normiert § 32 Abs. 3 BDSGE sogar ein Erhebungsverbot. Die übrigen sensitiven Daten dürfen gem. § 32 Abs. 2 S. 1 BDSGE nur unter den Voraussetzungen erhoben werden, unter denen nach § 8 Abs. 1 AGG eine unterschiedliche Behandlung zulässig ist.[72] Nach diesem muss es sich bei dem Datum aus Sicht eines verständigen Dritten um eine wesentliche berufliche Anforderung handeln[73]. Weiterhin muss der Zweck der Unterscheidung rechtmäßig, also nicht unvernünftig oder willkürlich, sein.[74] Außerdem ist eine Verhältnismäßigkeitsprüfung notwendig.[75]

e) Zwischenergebnis

Nach § 32 BDSG lassen sich einfache personenbezogene Daten damit zwar auch ohne Einwilligung erheben. Der Prozess ist aber sowohl für den Arbeitgeber als auch für den Bewerber unbefriedigend. Wegen der erforderlichen Interessenabwägung herrscht Ungewissheit auf beiden Seiten, welche Daten erhoben und verwendet werden dürfen. Im Interesse der Rechtssicherheit ist der BDSGE in Hinsicht auf diese Norm daher zu begrüßen; die dortige Beschränkung auf nur allgemein zugängliche, einfache personenbezogene Daten aus berufsorientierten Netzwerken wäre weit praxistauglicher als die jetzige Regelung.

4. Zulässigkeit gem. § 28 Abs. 1 S. 1 Nr. 3 BDSG

Eine weitere Erlaubnisnorm ist § 28 Abs. 1 S. 1 Nr. 3 BDSG. Diese erlaubt die Erhebung und Verwendung von allgemein zugänglichen Daten, wenn das schutzwürdige Interesse des Betroffenen nicht offensichtlich überwiegt.

a) Anwendbarkeit

Die Norm müsste neben § 32 BDSG anwendbar sein. Teilweise wird § 32 BDSG als das speziellere Gesetz angesehen.[76] Dagegen wird angeführt, dass § 28 Abs. 1 S. 1 Nr. 3 BDSG im Gegensatz zu § 32 BDSG gerade kein Vertragsverhältnis voraussetzt.[77] Aus der insoweit widersprüchlichen Gesetzesbegründung[78] kann kein Argument entnommen werden.[79] Ein Vorrang des strengeren § 32 BDSG würde dazu führen, dass der Arbeitgeber alle allgemein zugänglichen Informationen, die nicht erforderlich sind, nicht erheben darf.[80] Diese Folge ist im Lichte des Grundrechts auf Informationsfreiheit (Art. 5 Abs. 1 S. 1 GG) bedenklich. Denn damit dürfte nur der Arbeitgeber nicht, was alle anderen öffentlichen und nicht-öffentlichen Stellen nach den Maßstäben des § 28 Abs. 1 Nr. 3 BDSG dürfen. Gerade für den Arbeitgeber verbinden sich mit der Einstellungsentscheidung aber wirtschaftliche Risiken, so dass er zumindest wissen dürfen sollte, was jeder andere wissen darf.[81] § 28 Abs. 1 Nr. 3 BDSG ist daher neben § 32 BDSG anwendbar.

b) Voraussetzungen

Es muss sich um allgemein zugängliche Daten – die also etwa über Google, Yahoo oder andere Suchdienste gefunden werden können – handeln. Im Gegensatz zu § 32 BDSG muss der Arbeitgeber hier keine intensive Einzelfallprüfung vornehmen.[82] Nur wenn auf der Hand liegt, dass ein schutzwürdiges Interesse des Bewerbers überwiegt, darf das Datum nicht erhoben oder verwendet werden.[83] Zu überlegen ist, ob das Einstellen eines Datums in ein privatorientiertes Netzwerk ein solches offensichtliches Überwiegen des Schutzinteresses des Bewerbers begründet. Dafür könnten die AGB dieser Netzwerke sprechen, die ausschließlich eine private Nutzung vorsehen. Da jeder Nutzer diesen AGB zugestimmt hat, lassen sich aus ihnen Rückschlüsse auf seine Verwendungsabsicht ziehen.

Indem der Bewerber das Datum aber für den Zugriff über allgemeine Suchmaschinen freigibt, entzieht er es dem Schutz dieser AGB. Um das offensichtliche Überwiegen des Bewerberinteresses auszulösen, müssen daher noch weitere Umstände (etwa eine besondere Sensibilität des Datums) dazu treten. Dabei ist § 28 Abs. 1 S. 2 BDSG zu beachten, nach dem die Zwecke für die Nutzung bereits bei der Erhebung konkret festgelegt werden müssen. Unter diesen wenig strengen Voraussetzungen kann der Arbeitgeber allgemein zugängliche Daten gemäß § 28 Abs. 1 S. 1 Nr. 3 BDSG somit stets erheben, gleichgültig, ob sie aus privatorientierten oder berufsorientierten Netzwerken stammen. Nach dem BDSGE wäre dies nicht mehr möglich, sondern auch hier eine Interessenabwägung vorzunehmen (s.o. II. 2. c).

Am Fall liegt in den Varianten 1, 2 und 3 bei der Teamfähigkeit kein offensichtlich überwiegendes Interesse des B vor. P darf das Datum erheben. In Variante 4 ist für P allerdings offensichtlich, dass B auf die Veröffentlichung auf dem Profil des C keinen Einfluss hatte, so dass er das dort befindliche Datum der Alkoholgeneigtheit nicht erheben darf.

c) Besondere personenbezogene Daten

Besondere personenbezogene Daten können nur unter der zusätzlichen Voraussetzung des § 28 Abs. 6 BDSG erhoben werden. Dieser verlangt, dass der Bewerber die Daten offenkundig selbst öffentlich gemacht hat. Dies trifft nur zu, wenn die Daten vom Bewerber selbst oder aufgrund seiner

72 Einzelfallgruppen in *Bauer/Göpfert/Krieger*, AGG, 2. Aufl. 2008, § 8 Rdn. 42.
73 *Boemke/Danko*, AGG im Arbeitsrecht, 2006, § 6 Rdn. 6.
74 BAG, Urt. vom 7.7.2005 – 2 AZR 399/04, NZA 2006, 266.
75 *Bauer/Göpfert/Krieger*, AGG, § 8 Rdn. 20.
76 KK-BDSG/*Däubler*, § 32 Rdn. 8.
77 *Forst*, NZA 2010, 427 (430).
78 BT-Dr. 16/13657, S. 20, sagt einerseits, dass außer § 28 Abs. 1 S. 1 Nr. 1 und S. 2 keine Datenschutzvorschriften, die eine Datenerhebung erlauben, verdrängt werden; andererseits aber: „Werden personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, findet § 28 Abs. 1 keine Anwendung mehr."
79 *Gola/Jaspers*, RDV 2009, 212 (214).
80 *Rolf/Rötting*, RDV 2009, 263 (264).
81 *von Steinau-Steinrück/Mosch*, NJW-Spezial 2009, 450 (451).
82 *Gola/Schomerus* (Fn. 9), BDSG, § 28 Rdn. 31.
83 *Bergmann/Möhrle/Herb*, Datenschutzrecht Loseblatt-Kommentar, Stand August 2009, § 28 Rdn. 251.

Veranlassung freiwillig[84] veröffentlicht worden sind.[85]

Im Beispielsfall müsste B die Information über seine sexuelle Orientierung offenkundig selbst öffentlich gemacht haben. Auch wenn man dieses Merkmal eng auslegt,[86] ist eine Gruppenzugehörigkeit in einem sozialen Netzwerk, die der Nutzer für Suchmaschinen freigeschalten hat, erkennbar durch den Bewerber selbst öffentlich gemacht. P darf das Datum damit (nur) in Variante 1 erheben.

5. Zulässigkeit gem. § 28 Abs. 6 Nr. 3 BDSG

Für besondere personenbezogene Daten kommt weiterhin eine Rechtfertigung nach § 28 Abs. 6 Nr. 3 BDSG in Betracht. Die Norm verlangt, dass der Datenumgang zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Bewerbers überwiegt.

Zu denken ist zunächst an das Anfechtungsrecht des Arbeitgebers wegen Falschauskunft des Bewerbers und an Rechte aus dem vorvertraglichen Schuldverhältnis, §§ 311 Abs. 2, 241 Abs. 2 BGB. Diese sind aber formal gesehen keine Ansprüche,[87] sodass § 28 Abs. 6 Nr. 3 BDSG nicht auf sie gestützt werden kann.

Allerdings könnte es möglich sein, die Datenerhebung mit einem Anspruch aus positiver Vertragsverletzung zu begründen. Dies ist nur der Fall, wenn § 28 Abs. 6 Nr. 3 BDSG auch potenzielle zukünftige Ansprüche ausreichen lässt. Dafür spricht, dass die Datenerhebung als Informationsbeschaffung es häufig erst ermöglicht zu prüfen, ob ein Anspruch besteht. In diesen Fällen würde § 28 Abs. 6 Nr. 3 BDSG leer laufen,[88] wenn man noch nicht bestehende Ansprüche nicht zur Begründung des Datenerhebungsrechts zulässt. Da dies eine Hauptanwendungsgruppe der Norm sein dürfte, ist davon auszugehen, dass zukünftige Ansprüche umfasst werden.

Der Arbeitgeber kann auf der Grundlage des § 28 Abs. 6 Nr. 3 BDSG besondere personenbezogene Daten erheben und verwenden, wenn er sie für zukünftige Ansprüche aus dem Arbeitsvertrag benötigt.

Es darf jedoch kein Grund zur Annahme bestehen, dass Interessen des Bewerbers überwiegen. Bei der vorgenommenen Ausdehnung des Wortlauts muss die Interessenabwägung restriktiv bewertet werden.[89] „Kein Grund zur Annahme" liegt deswegen erst vor, wenn die erhebende Stelle sich sicher ist, dass keine Belange des Betroffenen überwiegen.[90]

Im Beispielsfall fällt die Interessenabwägung zuungunsten des P aus. Denn die Diskriminierung Homosexueller ist gesetzlich gem. Art. 3 Abs. 3 S. 2 GG und § 1 AGG verboten. P darf deswegen seine Einstellungsentscheidung nicht von der sexuellen Orientierung abhängig machen. Daher kann ihm das Datum auch nicht bei der Entscheidung nützen. Es fehlt somit schon an der Geeignetheit. Er darf das Datum daher nicht erheben.

III. Rechtliche und tatsächliche Folgen einer unzulässigen Erhebung oder Verwendung aus sozialen Netzwerken

Einen „zahnlosen Tiger" nennt *Oberwetter*[91] das Datenschutzrecht, weil es kaum Konsequenzen habe, dagegen zu verstoßen. Tatsächlich nützt einem Bewerber das schönste Gesetz wenig, wenn der Arbeitgeber sich nicht daran gebunden fühlt. Zu untersuchen ist daher noch, mit welchen Rechtsfolgen ein Arbeitgeber bei unzulässigem Datenumgang tatsächlich rechnen muss.

1. Zivilrechtliche Folgen

Zunächst kommen Ansprüche der Netzwerkbetreiber gegen den Arbeitgeber in Betracht, wenn dieser widerrechtlich Daten nutzt. Sind Daten nicht über Suchmaschinen abrufbar, muss der Arbeitgeber sich registrieren und dabei die AGB des Netzwerks akzeptieren. Privatorientierte Netzwerke schließen darin die kommerzielle Nutzung aus.[92] Da die Bewerberauswahl der Personalplanung dient,[93] ist dadurch der Umgang mit Bewerberdaten schon vertraglich verboten. Um ihr aus Datenschutzgründen bereits angeschlagenes Image nicht noch mehr zu gefährden, werden Netzwerkbetreiber mit allen Mitteln gegen Datenschutzverstöße vorgehen.[94] Gegen Arbeitgeber bestünde ein Unterlassungsanspruch aus § 1004 BGB analog i.V.m. Nutzungsvertrag und Schadensersatzansprüche aus §§ 280 Abs. 1, 241 Abs. 2 BGB i.V.m. Nutzungsvertrag.[95]

Entsteht dem Bewerber durch den unzulässigen Datenumgang ein Schaden, kann er Schadensersatzansprüche aus §§ 280 Abs. 1, 311 BGB; § 15 AGG; § 7 BDSG; § 823 Abs. 1 oder Abs. 2 BGB i.V.m. BDSG geltend machen. Diese sind aber nur schwer durchsetzbar. Denn der Bewerber muss beweisen, dass ihm ein Schaden entstanden ist und er eingestellt worden wäre, wenn der Arbeitgeber die Daten nicht unzulässiger Weise erhoben und verwendet hätte.[96] Dies wird nur selten gelingen. Schon zu zeigen, dass der Arbeitgeber überhaupt Daten aus sozialen Netzwerken erhoben hat, ist denkbar schwierig. Geradezu unmöglich ist es, zu beweisen, dass der Arbeitgeber diese Daten für seine Einstellungsentscheidung auch verwendet hat. Die Praxisrele-

84 *Wedde* (Fn. 13), § 28 Rdn. 172.
85 *Simitis* (Fn. 26), § 28 Rdn. 330.
86 Wie gefordert bei *Wedde* (Fn. 13), § 28 Rdn. 173.
87 *Sutschet*, in: Bamberger/Roth, Beck'scher Online-Kommentar zum BGB, Edition 18, Stand: 1.8.2010, § 241 BGB Rdn. 43.
88 *Thüsing*, Arbeitnehmerdatenschutz und Compliance, 2010, Rdn. 385.
89 *Wedde* (Fn. 13), § 28 Rdn. 174.
90 *Simitis* (Fn. 26), § 28 Rdn. 334.
91 *Oberwetter*, BB 2008, 1562 (1565).
92 *Rolf/Rötting*, RDV 2009, 263 (266); Facebook AGB 4. Nr. 4, abruf-bar unter www.facebook.de, zuletzt abgerufen am 01.11.2010; § 2 Nr. 6 Nutzungsbedingungen von pafnet.de, abrufbar unter www.pafnet.de, zuletzt abgerufen am 01.11.2010. Anders die AGB berufsorientierter Netzwerke, vgl. AGB von XING, abrufbar unter www.xing.de, zuletzt abgerufen am 01.11.2010.
93 *Forst*, NZA 2010, 427 (429).
94 *Forst*, NZA 2010, 427 (432).
95 *Forst*, NZA 2010, 427 (432).
96 *Forst*, NZA 2010, 427 (433).

vanz der Schadensersatzansprüche ist daher gering.[97] Etwas anderes gilt für nach § 1 AGG geschützte Daten, denn für den Schadensersatzanspruch nach § 15 AGG gilt die Beweislastumkehr des § 22 AGG.[98] Der Bewerber muss nur Indizien für eine Benachteiligung beweisen, während der Arbeitgeber darzulegen hat, dass er im Einklang mit dem AGG gehandelt hat. Sein Risiko ist deswegen signifikant höher. Der Schadensersatz beträgt bis zu drei Monatsgehälter (§ 15 Abs. 2 S. 2 AGG).

2. Haftende Personen

Grundsätzlich haftet der Arbeitgeber selbst. Einer juristische Person wird das Verhalten ihrer Organe analog § 31 BGB zugerechnet.[99] Bei §§ 280, 311 BGB haftet er gem. § 278 BGB auch für das Verhalten von Erfüllungsgehilfen, also etwa auf Weisung handelnder Arbeitnehmer.[100] Bei deliktischen Ansprüchen (§§ 7 f. BDSG, 823 ff. BGB) wird gem. § 831 Abs. 1 S. 1 BGB zugerechnet, sodass der Arbeitgeber die Exkulpationsmöglichkeit des § 831 Abs. 1 S. 2 BGB hat. Auch die Hilfsperson, z.B. der Personalmanager,[101] oder der oben vorgeschlagene „Datenfilter" kann aus deliktischen Ansprüchen haftbar sein.[102] Allerdings kann ein haftender Arbeitnehmer analog §§ 670, 257 BGB vom Arbeitgeber verlangen, von den Ansprüchen freigestellt zu werden.[103] Dann zahlt dieser, wenn er nicht eigene Schadensersatzansprüche gegen den Arbeitnehmer (§§ 280 Abs. 1, 241 Abs. 2 BGB i.V.m. Arbeitsvertrag) und seinen Freistellungsanspruch aufrechnen kann. Zwar ist der inkorrekte Datenumgang eine Pflichtverletzung;[104] jedoch haftet der Arbeitnehmer gemäß den Grundsätzen zur beschränkten Arbeitnehmerhaftung nur bei grober Fahrlässigkeit voll.[105]

3. Ordnungswidrigkeits- und strafrechtliche Folgen

In Bayern kontrolliert das Landesamt für Datenschutz gem. § 38 S. 1 BDSG die Einhaltung des BDSG. Es kann Bußgeldverfahren gegen den Leiter des Unternehmens gem. § 43 BDSG einleiten[106] und den unzulässigen Umgang mit zugangsbeschränkten Daten mit bis zu 300.000 Euro belangen (§ 43 Abs. 2 Nr. 1 i.V.m. Abs. 3 S. 1 BDSG). Bei Bereicherungs- oder Schädigungsabsicht liegt gem. § 44 Abs. 1 BDSG eine Straftat vor, die mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft werden kann.[107] Dies ist aber schwer nachzuweisen und deswegen wenig praxisrelevant.[108] Statistisch muss ein Unternehmen nur alle 39.400 Jahre mit einer Datenschutzüberprüfung rechnen.[109]

IV. Fazit

1. Für die Erhebung und Verwendung einfacher personenbezogener Daten ist die **Einwilligung** das sicherste Instrument. Sie ist nach BDSG konkludent und formlos möglich. Nach hier vertretener Auffassung kann der Arbeitgeber auch bei Geltung des BDSGE aufgrund einer Einwilligung Daten erheben und verwenden, ohne mit rechtlichen Konsequenzen rechnen zu müssen.

2. Sind Profildaten **allgemein zugänglich**, muss nach BDSG nur eine kursorische Interessenabwägung durchgeführt werden. Im BDSGE kommen eine Hinweispflicht, die Beschränkung auf berufsorientierte Netzwerke und eine genaue Verhältnismäßigkeitsprüfung hinzu.

3. Auf **Netzwerkmitglieder zugangsbeschränkte Daten** darf der Arbeitgeber nach BDSG nur aus berufsorientierten Netzwerken nach Verhältnismäßigkeitsprüfung, nach BDSGE gar nicht erheben oder verwenden.

4. Nur **Kontakten zugängliche Daten** darf der Arbeitgeber nur in berufsorientierten Netzwerken erheben oder verwenden; laut BDSGE muss dabei der Bewerber selbst den Kontaktschluss initiiert haben.

5. Die **Grundsätze zum Fragerecht** des Arbeitgebers im Einstellungsgespräch sind vollständig zu übertragen und bilden die Grenze der Erhebung und Verwendung von Bewerberdaten.

6. Mit rechtlichen oder tatsächlichen **Konsequenzen** bei Verstößen braucht der Arbeitgeber allerdings nur sehr eingeschränkt zu rechnen, so dass Bewerber trotz vieler Erhebungsverbote davon ausgehen müssen, dass häufig dennoch Daten aus sozialen Netzwerken in ihre Beurteilung einfließen.

97 *Oberwetter*, BB 2010, 1562 (1565); *Schaub*, Arbeitsrechtshandbuch, 12. Aufl. 2007, § 26 Rdn. 12.
98 Dazu *Grobys*, NZA 2006, 898 ff.
99 BGH, Urt. vom 9.5.2005 – II ZR 287/02, NJW 2005, 2450 (AG); vom 13.1.1987 – VI ZR 303/85, BGHZ 99, 298 (GmbH); RG, Urt. vom 13.2.1911 – VI 652/09, RGZ 76, 35, 48; BGH, Urt. vom 8.2.1952 - I ZR 92/51, NJW 1952, 537 (OHG und KG); vom 24.2.2003 – II ZR 385/99, BGHZ 154, 88 (GbR).
100 *Kieninger*, in: Säcker/Rixecker (Hrsg.), Münchner Kommentar zum BGB, 5. Aufl. 2007, § 309 Rdn. 7.
101 *Thüsing* (Fn. 88), Rdn. 520.
102 *Däubler* (Fn. 13), § 7 Rdn. 38.
103 BAG, Urt. vom 23.6.1988 – 8 AZR 300/85, E 59, 89.
104 *Wind*, RDV 1991, 16 (21).
105 BAG, GrS vom 27.9.1994 – GS 1/89 (A), E 78, 56.
106 *Ehmann*, in: Praxiskommentar Bundesdatenschutzgesetz, 5. Aufl. 2009, § 43 S. 603.
107 Dazu eingehend in diesem Heft *Riemer*, Seite 22.
108 *Ehmann* (Fn. 106), § 43 S. 606.
109 *Tomik*, FAZ v. 24.9.2010, S. 3.