Messenger im Unternehmen

Dr. Niels Lepperhoff/Mareike Papendorf, Düsseldorf*

1. Einleitung

Jedes Unternehmen ist auf Kommunikation zwischen seinen Beschäftigten angewiesen. Neben den klassischen Formen schriftlich („Hausmitteilung") und mündlich, d.h. face-2-face, haben verschiedene elektronische Formen Einzug gehalten. Zu den bekannten elektronischen Formen für die unmittelbare Kommunikation zählen das Telefon, E-Mails, Kurznachrichten (SMS usw.), Video-Chat, Sprach-Chat und Text-Chat. Technisch gemeinsam ist diesen Formen, dass alle an der Kommunikation beteiligten Personen im Regelfall die gleiche Software nutzen müssen. Häufig bieten diese Programme verschiedene Kommunikationsformen gleichzeitig an. Meist können mehrere Teilnehmer gleichzeitig miteinander kommunizieren. Beispiele für moderne Kommunikationsmittel sind Skype, Skype for Business (ehem. Lync), Google Hangouts, Teamspeak, Whatsapp und SimsME. Für die folgende Betrachtung werden diese und verwandte Programme unter der Bezeichnung „Instant Messenger" zusammengefasst.

Eine Nutzung im Unternehmen berührt verschiedene Datenschutzfragen von dem Schutz vor unbefugtem Lesen oder Verändern bis hin zu Zulässigkeit der Verwendung. Dieser Beitrag beschäftigt sich mit ausgewählten Aspekten der Zulässigkeit und konzentriert sich auf eine ausschließliche dienstliche Nutzung.

2. Generelle Funktionen

Wenn man verschiedene Instant Messenger betrachtet, lassen sich vier Funktionsgruppen unterscheiden:

- Kommunikation mittels Text, Sprache oder Bild,
- Verwaltung und Übertragung von Statusinformationen („anwesend, „abwesend" usw.),
- Verwaltung von Empfängern sowie Empfängergruppen und
- Aufzeichnung von Kommunikationsinhalten.

In der Ausgestaltung dieser Funktionsgruppen unterscheiden sich die verschiedenen Produkte. Die folgende Betrachtung zielt auf grundsätzliche Überlegungen ab, so dass sie sich auf eine generalisierte Betrachtung der Funktionsgruppen beschränken kann.

Die Kommunikation kann synchron erfolgen, d.h. die Kommunikationspartner agieren gleichzeitig miteinander (z.B. Chat per Text, Sprache oder Video). Der bekannteste Vertreter der asynchronen Kommunikation ist die E-Mail. Schreiben und Lesen fallen zeitlich auseinander.

3. Rechtliche Einordnung

Instant Messenger kommunizieren technisch durch das Übertragen von Signalen über Telekommunikationsnetze. Damit ist für den eigentlichen Kommunikationsvorgang prinzipiell der Anwendungsbereich des Telekommunikationsgesetzes eröffnet (§§ 3 Nr. 6 und Nr. 24 TKG). Ob ein Arbeitgeber bei erlaubter Privatnutzung als Diensteanbieter gemäß § 3 Nr. 6 TKG zu betrachten sei, ist umstritten[1, 2, 3]. Bei dienstlicher Nutzung nutzt der Mitarbeiter die Instant Messenger auf Anweisung hin, so dass eine Anwendung des TKG ausscheidet[4, 5]. Anders sieht es für Unternehmen aus, die Kommunikation über Instant Messenger für Dritte – wozu auch Konzerngesellschaften zählen – anbieten. Diese Anbieter unterfallen dem TKG[6]. An dieser Stelle wird auf eine ausführliche Darstellung verzichtet, da sich Instant Messenger nicht von anderen Telekommunikationsdiensten unterscheiden und mit Blick auf die Problemstellung des Artikels keine neue Fragestellung aufwerfen.

Der Kommunikationsvorgang findet mit dem Zustellen der Nachricht in dem Verfügungsbereich des Empfängers sein Ende[7]. Das Verwalten von erhaltenen Nachrichten oder auch Gesprächsmittschnitten findet nach Abschluss des Kommunikationsvorganges statt. Da diese Verwaltung den Abschluss der Signalübertragung voraussetzt, eröffnet § 1 Abs. 1 TMG die Anwendbarkeit des TMG.

Die zwei Funktionsgruppen „Verwaltung und Übertragung von Statusinformationen" und „Verwaltung von Empfängern und Empfängergruppen" stellen Telemediendienste i.S.v. § 1 Abs. 1 TMG dar. Daher ist für die Nutzung des Instant Messenger an sich das TMG einschlägig, während für die Inhalte das BDSG zur Anwendung kommt[8].

Um den Rahmen des Artikels nicht zu sprengen, konzentrieren sich die folgenden Ausführungen auf die Inhalte der Nutzung, d.h. auf eine Zulässigkeit im Rahmen des BDSG. Die Anwendung des TMG insbesondere bei der Frage der

* Niels Lepperhoff ist Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD und der GDD). Er verfügt über langjährige Berufserfahrung als externer Datenschutzbeauftragter und berät sowohl deutsche als auch internationale Unternehmen. Daneben ist er Inhaber eines Lehrauftrages des Masterstudienganges „Medienrecht und Medienwirtschaft" an der Technischen Hochschule Köln.

Mareike Papendorf hat Wirtschaftsrecht an den Hochschulen Köln und Trier studiert. Sie ist bei der Xamit Bewertungsgesellschaft mbH als Beraterin beschäftigt. Ihr Tätigkeitsschwerpunkt liegt auf dem Datenschutzrecht.

1 Eigenschaft als Diensteanbieter im Rahmen der Wahrung des Fernmeldegeheimnisses wird angenommen von Taeger/Gabel – Munz (2010), § 88 TKG Rn. 20.

2 Umstrittene Meinung wird angenommen von Gola (2014): Datenschutz am Arbeitsplatz, Rn. 227.

3 Herrschende Meinung über Eigenschaft als Diensteanbieter wird angenommen von Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), Rn. 221 f. Thüsing selber vertritt die gegenteilige Meinung, ebenda Rn. 246.

4 Thüsing, Arbeitnehmerdatenschutz und Compliance (2010), Rn. 210 f.

5 Gola, Datenschutz am Arbeitsplatz (2014), Rn. 226.

6 Gola, Datenschutz am Arbeitsplatz (2014), Rn. 220.

7 Urteile des Bundesverfassungsgerichts vom 2. März 2006 – 2 BvR 2099/04 sowie vom 27. Februar 2008 – 1 BvR 370/07.

8 Taeger/Gabel – Moos, Einführung TMG (2010), Rn. 20.

Aufzeichnung (Abschnitte 4.1.3 und 5.1.3) wird deshalb nicht verneint, sondern bleibt einer gesonderten Analyse vorbehalten. Gleiches gilt für das TKG, das für die Übertragung von Signalen einschlägig ist.

4. Zulässigkeit der betrieblichen Nutzung

Es stellt sich nun die Frage, ob und ggf. unter welchen Voraussetzungen eine betriebliche Nutzung von Instant Messengern aus Sicht des Datenschutzes zulässig ist. Hierbei muss zwischen Arbeitnehmern und sonstigen Personen differenziert werden, da unterschiedliche Rechtsgrundlagen zum Tragen kommen. Auch zwischen der Kommunikation an sich, der Verwaltung und Übertragung von Statusmeldungen sowie der Aufzeichnung von Kommunikationsinhalten wird differenziert, da sie in der Praxis unterschiedlichen Anforderungen gerecht werden müssen.

4.1 Arbeitnehmer

Die meisten Arbeitnehmer nutzen in ihrem Berufsalltag verschiedene Kommunikationsmittel. Neben klassischen Varianten, wie Post und Telefon, sind auch elektronische Mittel wie E-Mails und Instant Messenger immer beliebter geworden. Die Wahl des Kommunikationsmittels trifft in der Regel der Arbeitgeber im Rahmen seines Direktionsrechtes. Für den Arbeitnehmer ist es insbesondere bei Instant Messengern oft nicht transparent und nachvollziehbar, welche Daten dort über ihn erhoben, verarbeitet und evtl. sogar übermittelt werden. Für jeden dieser Schritte muss für jedes einzelne Datum eine Rechtsgrundlage vorhanden sein. Ob und ggf. unter welchen Voraussetzungen solche Rechtsgrundlagen vorhanden sind, wird im Folgenden überprüft.

4.1.1 Kommunikation mittels Text, Sprache oder Bild und Verwaltung von Empfänger

Bei der betrieblichen Verwendung eines Instant Messengers werden regelmäßig personenbezogene Daten der Mitarbeiter erhoben, verarbeitet und genutzt. Im Regelfall erhält jeder Nutzer ein persönliches Profil unter seinem Namen, so dass seine Aktivitäten mit ihm als Person verbunden werden. Regelmäßig baut die betriebliche Arbeitsorganisation auf den Personenbezug der Mitarbeiter auf.

Grundsätzlich stellt eine Einwilligung nach §§ 4 Abs. 1 i.V.m. 4a BDSG eine Nutzungserlaubnis dar. Gegen die Einholung einer Einwilligung spricht nicht nur, dass sie im Rahmen des Arbeitsverhältnisses regelmäßig mangels Freiwilligkeit unwirksam sein wird, sondern auch dass sie verweigert oder widerrufen werden kann. Die praktische Konsequenz wäre, dass der Instant Messenger nicht von jedem Mitarbeiter verwendet werden müsste. Oder dass über Kunden, die keine Einwilligung zur Verwendung ihrer personenbezogenen Daten erteilt haben, nicht gesprochen werden dürfte. Diese Ausnahmen müssten natürlich verwaltet und technisch wie auch organisatorisch umgesetzt werden. Zudem müssten Alternativen vorhanden sein, damit Besprechungen auch ohne die Nutzung des Instant Messengers durchführbar sind. Telefonate und E-Mails stellen in den Fällen, wo Blickkontakt gewünscht ist, keine Alternative dar.

Sofern die Nutzung des Instant Messengers für die Durchführung des Arbeitsverhältnis erforderlich ist, z.B. als einziges Kommunikationsmittel, bemisst sich die datenschutzrechtliche Zulässigkeit grundsätzlich nach § 32 Abs. 1 S. 1 BDSG.

Im Rahmen der Durchführung des Arbeitsverhältnisses mag die Nutzung von Instant Messengern eher anzutreffen sein als bei der Begründung, bspw. beim Führen von Bewerbungsgesprächen, oder der Beendigung. Die Nutzung der vom Arbeitgeber bereit gestellten Arbeitsmittel dürfte regelmäßig für die Erfüllung der arbeitsvertraglichen Pflichten erforderlich sein. Insofern wird die in § 32 Abs. 1 S. 1 BDSG geforderte Erforderlichkeit gegeben sein.

In der Praxis bleibt zu beachten, dass § 32 Abs. 1 S. 1 BDSG keine schrankenlose Erlaubnisnorm darstellt. Die Erforderlichkeit für die Durchführung des Arbeitsverhältnisses ist für jedes zu erhebende, zu verarbeitende und zu nutzende Datum festzustellen (siehe auch Abschnitt 4.1.2). Dabei ist der Kreis der Zugriffsberechtigten mit zu berücksichtigen. Wenn jeder von bspw. 5.000 Mitarbeitern Zugriff hat, muss der Zugriff auf das Datum für jeden der 5.000 Mitarbeiter im Rahmen seiner Arbeit erforderlich sein. Für die Praxis bieten sich deshalb abgestufte Zugriffsberechtigungen auf Personen- und Datenartebene an. Oder anders formuliert, je größer der Kreis der Nutzer, desto höher der Konfigurationsaufwand. Produkte, die nicht die notwendigen Instrumente zur Rechteverwaltung mitbringen, können folglich nicht ohne Datenschutzverstoß verwendet werden.

Eine freiwillige Nutzung, d.h. eine Nutzung, die nicht erforderlich ist, überzeugt nicht, da der Instant Messenger dann eher nicht als Arbeitsmittel anzusehen wäre. Damit stünde die Annahme, dass die Nutzung ausschließlich dienstlich erfolgt, in Frage. § 28 Abs. 1 Nr. 2 BDSG erscheint deshalb höchstens in besonders gelagerten Einzelfällen als Rechtsgrundlage in Betracht zu kommen.

§ 28 Abs. 6 BDSG – insbesondere Nr. 3 – beinhaltet eine Erlaubnisnorm für die Erhebung, Verarbeitung und Nutzung von besonderen personenbezogenen Daten i.S.v. von § 3 Abs. 9 BDSG, z.B. bei Krankmeldungen von Mitarbeitern per Chat, wenn diese zur Geltendmachung, Ausübung oder Verteidigung von rechtlichen Ansprüchen erforderlich sind. Die Rechte und Pflichten aus dem Arbeitsvertrag sind solche rechtlichen Ansprüche. Gleichwohl verlangt § 28 Abs. 6 Nr. 3 BDSG zusätzlich, dass die berechtigten Interessen der Betroffenen nicht überwiegen. Dies dürfte, insbesondere wenn zahlreiche Nutzer Zugriff auf diese personenbezogenen Daten haben, regelmäßig der Fall sein.

Es sei darauf hingewiesen, dass bei der Verwendung von Fotos der Mitarbeiter die Vorschriften des KunstUrhG und des UrhG zu beachten sind.

4.1.2 Verwaltung und Übertragung von Statusinformationen

Statusinformationen wie z.B. „anwesend“, „abwesend“, „in Besprechung“ helfen den „Blick ins Büro“ zu ersetzen. Bereits vor der Kontaktaufnahme ist erkennbar – sofern der Status korrekt gesetzt ist –, ob der gewünschte Gesprächsteilnehmer erreichbar ist. Gerade bei Chats hilft der Status

einzuschätzen, ob der gewünschte Gesprächspartner antworten könnte oder nicht. Insofern spricht einiges dafür, dass, wie in Abschnitt 4.1.1 hergeleitet, im Regelfall § 32 Abs. 1 S. 1 BDSG die Rechtsgrundlage der Wahl sein könnte.

Wer die Statusinformationen einer Person im Zeitverlauf beobachtet, erfährt etwas über deren Verhalten und je nach Tätigkeit auch etwas über ihre Leistung (z.B. Anzahl und Dauer der Kundentermine im Außendienst). Eine Verhaltens- und Leistungsbeurteilung auf Basis des Arbeitsvertrags steht grundsätzlich nur dem Arbeitgeber bzw. den durch den Arbeitgeber ermächtigten Mitarbeitern zu. Auch wenn einiges dafür spricht, sei an dieser Stelle offen gelassen, ob ein Mitarbeiter, der die Statusinformationen seiner Kollegen für eine Verhaltens- oder Leistungsbeobachtung ohne Ermächtigung durch den Arbeitsgeber nutzt, gegen § 5 BDSG verstößt. Wird der Status automatisch durch den Instant Messenger gesetzt, bspw. auf „abwesend", wenn die Tastatur eine Zeitlang nicht genutzt wurde, nimmt die Eingriffstiefe weiter zu.

Wer an dieser Stelle überlegt, ob § 28 Abs. 1 Nr. 2 BDSG eine bessere Rechtsgrundlage wäre, sei daran erinnert, dass die Interessensabwägung auf jeden Fall zu Gunsten des Betroffenen ausginge[9].

Mögliche Lösungen sind

- die Statusinformation zu deaktivieren oder
- den Zugriff soweit einzuschränken, dass der Zugriff für die Durchführung des Arbeitsverhältnisses erforderlich wird und die Verhaltens- und Leistungsbeurteilung ausschließlich von Berechtigten durchgeführt werden kann.

Eine Einschränkung des Zugriffs wäre z.B. gegeben, wenn die Statusinformationen ausschließlich für die Kollegen sichtbar sind, mit denen täglich kommuniziert werden muss. Weiterhin sollte der Mitarbeiter den Kreis der Zugriffsberechtigten kennen sowie den Status und die Sichtbarkeit selber beeinflussen können.

Status, die Rückschlüsse auf besondere personenbezogene Daten ermöglichen, wie z.B. „krank" oder „im Gebet", sind grundsätzlich unzulässig. Die Interessensabwägung nach § 28 Abs. 6 Nr. 3 BDSG geht regelmäßig zu Gunsten des Betroffenen aus. Die übrigen Erlaubnistatbestände des § 28 Abs. 6 BDSG kommen aller Erfahrung nach in eher ungewöhnlichen Fallkonstellationen zum Tragen.

4.1.3 Aufzeichnung von Kommunikationsinhalten

Die Aufzeichnung von Chat-Kommunikation – als Text, Sprache oder Video – geschieht teilweise automatisch durch den Instant Messenger. Für die Aufzeichnung, die mindestens die personenbezogenen Daten der Teilnehmer („Name") enthält, bedarf es eines konkreten Zwecks, wie z.B. Protokollierung von Verkaufsaufträgen. Bei einer automatischen Protokollierung genereller Kommunikation fehlt es bereits häufig an einem Zweck. Gleichwohl verstehen – wie einige Banken schmerzhaft erfahren haben – Aufsichtsbehörden und Strafverfolgungsbehörden auch diese Aufzeichnungen zu nutzen.

Aus der Zulässigkeit der Chat-Kommunikation (Abschnitt 4.1.1) folgt deshalb nicht zwangsläufig die Zulässigkeit ihrer Aufzeichnung. Neben einem Nutzungszweck bedarf es einer eigenständigen Rechtsgrundlage, die auch die Speicherung legitimiert.

Bei der Aufzeichnung des gesprochenen Wortes im Rahmen von Sprach-Chats oder Video-Chats sei an die strafrechtlichen Vorschriften insbesondere § 201 StGB erinnert. Diese Vorschrift betrifft alle Instant Messenger, wie z.B. Teamspeak, die die Aufnahme des gesprochenen Wortes ermöglichen. Im Regelfall wird eine Einwilligung aller betroffenen Personen erforderlich sein.

4.2 Andere Personengruppen

Je nach Zweck der Nutzung können auch personenbezogene Daten von anderen Personengruppen, wie z.B. Kunden, Lieferanten oder auch Bewerbern, verarbeitet oder genutzt werden. Selbst wenn diese Personengruppen nicht selber als Nutzer teilnehmen, können ihre Daten im Rahmen von Konversationen verwendet werden. Denkbare Rechtsgrundlagen wären § 28 Abs. 1 Nr. 1 oder Nr. 2 BDSG für Kunden und Lieferanten, sowie § 32 Abs. 1 S. 1 BDSG für Bewerber. Sofern besondere personenbezogene Daten verwendet werden, z.B. von Patienten, käme § 28 Abs. 6 BDSG in Frage. Die Zulässigkeit lässt sich folglich erst am konkreten Zweck entscheiden. Spezialgesetzliche Verarbeitungsverbote sollten dabei beachtet und im Rahmen der Nutzung umgesetzt werden.

5. Unternehmensübergreifende Nutzung

In der Praxis werden Instant Messenger nicht nur innerhalb eines Unternehmens eingesetzt. Gerade in Konzernen oder Unternehmensgruppen werden Instant Messenger gerne konzern- bzw. gruppenweit genutzt, um eine Zusammenarbeit – auch über große räumliche Distanzen hinweg – zu ermöglichen oder zu vereinfachen. Häufig wird aufgrund einer gemeinsamen Corporate Identity oder starker Einbindungen in Konzernstrukturen nicht bedacht, dass es sich bei den beteiligten Einheiten um rechtlich selbständige Unternehmen handeln kann.

Andererseits kann die Nutzung von Instant Messengern eine Methode sein, um mit Lieferanten, Kunden oder sonstigen Geschäftspartner zu kommunizieren. Hier sind sich die Beteiligten der unternehmensübergreifenden Kommunikation bewusst, und in der Regel bestehen vertragliche Beziehungen zwischen den Unternehmen.

5.1 Arbeitnehmer

Arbeitnehmer haben ein schützenswertes Interesse daran, dass ihre Daten nicht grundlos an Dritte weitergegeben werden. Demgegenüber stehen die Pflichten aus dem Arbeitsvertrag, die in einigen Fällen die Übermittlung von Daten erforderlich machen. Für die Übermittelung jedes einzelnen personenbezogenen Datums muss eine Rechtsgrundlage vorhanden sein. Bei einer unternehmensübergreifenden Nutzung von Instant Messengern muss beachtet

9 Vgl. für den ähnlich gelagerten Fall der Empfangsbestätigung bei E-Mail: Landesdatenschutzbeauftragte für Datenschutz Bremen, 34. Tätigkeitsbericht (2012), S. 55.

werden, dass es im Datenschutz kein Konzernprivileg gibt und daher ein Konzernbezug im Arbeitsvertrag vorhanden sein muss, wenn personenbezogene Daten innerhalb des Konzerns übermittelt werden sollen[10].

5.1.1 Kommunikation mittels Text, Sprache oder Bild und Verwaltung von Empfängern

Der Nutzen von Instant Messengern nimmt bekanntermaßen mit der Anzahl der Nutzer zu. Deshalb ist es für Konzerne, Unternehmensgruppen oder Unternehmen, die über die Gesellschafterstruktur zusammenwirken, attraktiv denselben Instant Messenger zu nutzen. Jeder Mitarbeiter kann mit jedem ohne Rücksicht auf die Unternehmenszugehörigkeit kommunizieren. Chattet Max Mustermann von Unternehmen A mit Eve Doe von Unternehmen B, werden technisch gesehen personenbezogene Daten von Max an Eve übertragen. Aus Sicht des Datenschutzrechtes liegt eine Übermittlung durch A an B vor. Zu der Zulässigkeitsfrage aus Kapitel 4 gesellt sich die Frage nach der Übermittlungserlaubnis.

Der routinierte Griff zur Auftragsdatenverarbeitung nach § 11 BDSG ist naheliegend. Eine Auftragsdatenverarbeitung bringt neben zahlreichen anderen Verpflichtungen auch das Trennungsgebot für den Auftragnehmer zur Anwendung. Im obigen Beispiel müsste das Unternehmen B zwei Instant Messenger vorhalten, da gerade diese Daten zusammenführen und nicht trennen wollen. Einen für die Kommunikation innerhalb von B und einen für die Kommunikation mit A. B dürfte die erhaltenen Daten nicht für eigene Zwecke verwenden. In der Praxis wird oft davon ausgegangen, dass alle Beziehungen zwischen Partnerunternehmen als Auftragsdatenverarbeitung ausgestaltet sind und daher beliebige Daten übermittelt werden dürfen. Diese Annahme ist jedoch nicht immer zutreffend. Nehmen wir beispielsweise an, B erhält von A für eigene Controllingzwecke aggregierte Rechnungsdaten ohne Personenbezug. Für diese Daten wäre das BDSG nicht anwendbar, und daher könnte auch kein Vertrag zur Auftragsdatenverarbeitung geschlossen werden. Max sendet per Chat eine Erläuterung zu diesen Daten. Eve dürfte die Tatsache, dass Max der Autor der Erläuterungen ist, nicht im Rahmen der eigenen Controllingzwecke verwenden und nicht an andere Personen – auch nicht an andere Mitarbeiter von B – weitergeben. Da eine Auftragsdatenverarbeitung absurde Konsequenzen hätte, bleibt nur der Weg über eine gesetzliche Erlaubnis.

Der Rückgriff auf § 32 Abs. 1 S. 1 BDSG bei Mitarbeitern ist so naheliegend wie problematisch. Die Messlatte ist neben der Erforderlichkeit, die in Abschnitt 4 diskutiert wurde, auch das Arbeitsverhältnis. Um eine Übermittlung zu rechtfertigen, müsste das Arbeitsverhältnis alle beteiligten Unternehmen umfassen[11]. Die Beziehung von Tochter- zum Mutterunternehmen kann durchaus in Arbeitsverträgen explizit berücksichtigt werden oder sich aus der Tätigkeitsbeschreibung ergeben. Bereits die Beziehungen zwischen Schwester- oder gar Enkelunternehmen finden sich eher selten im Arbeitsvertrag wieder. Ein Konzernbezug des Arbeitsverhältnisses lässt sich erfahrungsgemäß umso schwerer herstellen, je tiefer der Mitarbeiter in der Hierarchie angesiedelt ist. § 32 Abs. 1 S. 1 BDSG mag deshalb in bestimmten Konstellationen tragen, allerdings nicht als generelle Erlaubnisnorm.

Die Effektivität eines Instant Messengers steigt mit der Anzahl an Nutzern. Erst wenn alle Mitarbeiter über den Instant Messenger erreichbar sind, kann er andere Dienste wie E-Mail oder Telefon ersetzen. Auf Seiten der Unternehmen besteht ein berechtigtes wirtschaftliches Interesse an einer hohen Effizienz und Effektivität der Investition. Die beruflichen Kontaktdaten gehören regelmäßig nicht zur Privatsphäre einer Person, sondern betreffen lediglich die berufliche Tätigkeit. Überwiegende berechtigte Interessen der Mitarbeiter an einer Unterlassung der Übermittlung sind nicht erkennbar[12]. Die Übermittlung lässt sich folglich durch § 28 Abs. 1 Nr. 2 BDSG begründen.

Die Übermittlung – auch als Chat-Inhalt – besonderer personenbezogener Daten von Mitarbeitern ist nach § 28 Abs. 6 Nr. 3 BDSG für die „Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche“ grundsätzlich erlaubt. In Bezug auf den Arbeitsvertrag gilt das Vorgenannte. Selbst wenn die Erforderlichkeit bejaht wird, dürfte die zusätzlich erforderliche Interessenabwägung angesichts der Eingriffstiefe regelmäßig zu Gunsten der Betroffenen ausgehen. Die übrigen Erlaubnistatbestände des § 28 Abs. 6 BDSG kommen aller Erfahrung nach in eher ungewöhnlichen Fallkonstellationen zum Tragen.

5.1.2 Übermittlung von Statusinformationen

Wie in Abschnitt 5.1.1 ausgeführt, trägt § 32 Abs. 1 S. 1 BDSG eher nicht als generelle Erlaubnisnorm. Deshalb bleibt nur der Rückgriff auf § 28 Abs. 1 Nr. 2 BDSG. Durch die Möglichkeit zur Leistungs- und Verhaltenskontrolle besteht eine höhere Eingriffsintensität in das Persönlichkeitsrecht der Betroffenen. Kann sich der Arbeitgeber noch auf sein eigenes Kontrollrecht berufen (siehe Abschnitt 4.1.2), bleibt dieses dem empfangenden Unternehmen regelmäßig verwehrt, da es keine arbeitsvertragliche Beziehung zum Betroffenen unterhält. Dadurch entfällt zudem das Argument der betrieblichen Arbeitsorganisation, so dass regelmäßig die berechtigten Interessen der Betroffenen an Unterlassung der Übermittlung überwiegen dürften. Eine Übermittlung des Status ist folglich grundsätzlich unzulässig.

5.1.3 Aufzeichnung von übermittelten Kommunikationsinhalten

Grundsätzlich gilt das in Abschnitt 4.1.3 Erläuterte auch bei der Aufzeichnung übermittelter Kommunikationsinhalte. Sofern eine Einwilligung auf den Arbeitsvertrag gestützt worden ist, sei daran erinnert, dass eine arbeitsvertragliche Beziehung regelmäßig nicht mit allen an der Kommunikation beteiligten Unternehmen besteht.

10 Gola/Schomerus, BDSG Kommentar (2010), § 32 Rn. 20.

11 Gola/Wronka, Handbuch Arbeitnehmerdatenschutz (2013), Rn. 810 ff.

12 GDD, Mitarbeiterdaten im Unternehmensverbund – Praxishilfe V (2014), S. 17.

5.2 Andere Personengruppen

Werden personenbezogene Daten von Nicht-Mitarbeitern bspw. in einem Chatgespräch übertragen, gelten die üblichen Regeln – insbesondere § 28 BDSG – für die Übermittlung personenbezogener Daten. Es empfiehlt sich deshalb, verbindlich zu regeln, welche Inhalte durch den Instant Messenger erhoben, verarbeitet oder genutzt werden dürfen. Als Faustregel mag gelten, dass alles, was „offiziell" zwischen allen beteiligten Unternehmen mit Zugriff auf die Kommunikationsinhalte übermittelt werden darf, d.h. außerhalb einer Auftragsdatenverarbeitung, auch im Chat gestattet ist. Je mehr Unternehmen Zugriff auf einen Chat-Kanal haben, desto höher werden die Hürden in der Praxis werden.

6. Fazit

Die Nutzung von Instant Messengern im Berufsleben bietet zahlreiche Vorteile. Dabei darf jedoch nicht vergessen werden, dass sie vor ihrem Einsatz auf ihre Rechtmäßigkeit hin überprüft werden müssen. Für die Frage der Rechtmäßigkeit sind insbesondere die Möglichkeiten der Rechteverwaltung und die Zugriffsmöglichkeiten zu betrachten. Die Übermittlung von Statusmeldungen ist kritisch zu sehen, da sie nur in wenigen Fällen erforderlich sein wird. Aufzeichnungen von Kommunikationsinhalten bedürfen besonderer Prüfung, da hier sogar strafrechtliche Konsequenzen drohen können. Letztendlich ist es eine Frage des Einzelfalls ob und ggf. mit welchen Einschränkungen ein Instant Messenger betrieblich genutzt werden kann.

Rechtsprechung

Safe Harbour bietet kein angemessenes Datenschutzniveau

(**Europäischer Gerichtshof**, Urteil vom 6. Oktober 2015 – C-362/14 –)

1. **Art. 25 Abs. 6 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verabeitung personenbezogner Daten und zum freien Datenverkehr in der durch die Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003 geänderten Fassung ist im Licht der Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass eine aufgrund dieser Bestimmung ergangene Entscheidung wie die Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, in der die Europäische Kommission feststellt, dass ein Drittland ein angemessenes Schutzniveau gewährleistet, eine Kontrollstelle eines Mitgliedstaats im Sinne von Art. 28 der Richtlinie in geänderter Fassung nicht daran hindert, die Eingabe einer Person zu prüfen, die sich auf den Schutz ihrer Rechte und Freiheiten bei der Verarbeitung sie betreffender personenbezogener Daten, die aus einem Mitgliedstaat in dieses Drittland übermittelt wurden, bezieht, wenn diese Person geltend macht, dass das Recht und die Praxis dieses Landes kein angemessenes Schutzniveau gewährleistet.**
2. **Die Entscheidung 2000/520 ist ungültig.**

Aus den Gründen:

Ausgangsverfahren und Vorlagefragen

Herr Schrems, ein in Österreich wohnhafter österreichischer Staatsangehöriger, nutzt seit 2008 das soziale Netzwerk Facebook (im Folgenden: Facebook).

Alle im Unionsgebiet wohnhaften Personen, die Facebook nutzen wollen, müssen bei ihrer Anmeldung einen Vertrag mit Facebook Ireland abschließen, einer Tochtergesellschaft der in den Vereinigten Staaten ansässigen Facebook Inc. Die personenbezogenen Daten der im Unionsgebiet wohnhaften Nutzer von Facebook werden ganz oder teilweise an Server der Facebook Inc., die sich in den Vereinigten Staaten befinden, übermittelt und dort verarbeitet.

Am 25. Juni 2013 legte Herr Schrems beim Commissioner eine Beschwerde ein, mit der er ihn im Wesentlichen aufforderte, in Ausübung der ihm übertragenen Befugnisse Facebook Ireland die Übermittlung seiner personenbezogenen Daten in die Vereinigten Staaten zu untersagen. Er machte geltend, das Recht und die Praxis der Vereinigten Staaten gewährleisteten keinen ausreichenden Schutz der in diesem Land gespeicherten personenbezogenen Daten vor den Überwachungstätigkeiten der dortigen Behörden. Dabei verwies er auf die von Herrn Edward Snowden enthüllten Tätigkeiten der Nachrichtendienste der Vereinigten Staaten, insbesondere der National Security Agency (im Folgenden: NSA).

Da sich der Commissioner nicht für verpflichtet hielt, die von Herrn Schrems in seiner Beschwerde gerügten Tatsachen zu untersuchen, wies er die Beschwerde als unbegründet zurück. Er war nämlich der Ansicht, dass es keine Beweise für einen Zugriff der NSA auf die personenbezogenen Daten von Herrn Schrems gebe. Er fügte hinzu, die von Herrn Schrems in seiner Beschwerde erhobenen Rügen könnten nicht mit Erfolg geltend gemacht werden, da alle die Angemessenheit des Schutzes personenbezogener Daten in den Vereinigten Staaten betreffenden Fragen im Einklang mit der Entscheidung 2000/520 zu klären