Der **Querdenker**

Themen aus der Kanzlei **reichert & reichert**

Fokus **Datenschutz**

Die Datenschutzgrundverordnung

Matthias Herkert, Leiter Consulting

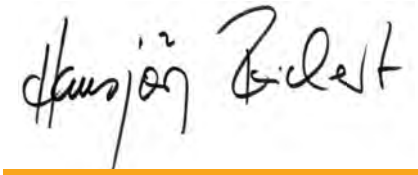
Am 25. Mai 2018 wird die europäische Datenschutz-Grundverordnung (EU-DSGVO) das Bundesdatenschutzgesetz (BDSG) ablösen. Ziel der neuen Regelungen ist ein unionsweit einheitlicher und wirksamer Schutz personenbezogener Daten, der insbesondere den Anforderungen an eine digitalisierte Welt Rechnung tragen soll. Die Regeln sollen in diesem Kontext durch eine möglichst einheitliche Rechtsanwendung in der Europäischen Union auch für die Wirtschaft mehr Rechtssicherheit und einen faireren Wettbewerb schaffen. Obwohl keine Vorgabe des BDSG völlig unverändert in der EU-DSGVO zu finden sein wird, wird die EU-DSGVO in Deutschland wohl für eine große Zahl von Unternehmen zu keinem grundlegenden Anpassungsbedarf der bisherigen Datenschutzorganisation führen. So haben zum einen die aus dem BDSG bekannten Mindeststandards weiterhin Gültigkeit, zum anderen werden die Grundprinzipien des Datenschutzes auch in der EU-DSGVO weitgehend fortbestehen. Damit ist die anfängliche Befürchtung nicht mehr begründet, durch die EU-DSGVO würde das Datenschutzniveau in Deutschland zukünftig unterlaufen oder abgesenkt.

Wichtige und zum Teil umfangreichere Änderungen kommen ab 2018 unter anderem durch das Marktortprinzip, geänderte Informationspflichten, die teilweise Verlagerung von Verantwortungen bei der Datenverarbeitung im Auftrag, dem sogenannten „One-Stop-Shop-Mechanismus" und den geänderten Möglichkeiten zur Verarbeitung personenbezogener Daten im Konzern zukünftig wohl insbesondere auf datengetriebene Unternehmen und Konzerne zu. Neu sind in jedem Fall die deutlich höheren Sanktionen bei Verstößen, die bis zu 4 % des weltweiten Umsatzes des vorangegangenen Geschäftsjahrs bzw. 20 Mio. Euro reichen können.

Handlungsbedarf: Datenschutzrelevante Prozesse auf Anpassungsbedarf prüfen und bei der Neugestaltung die Interaktion mit der DSGVO bereits berücksichtigen.

Unternehmen jeder Größe sind mit dem Thema Datenschutz konfrontiert und können mit dem professionellen Schutz von Kunden- und Mitarbeiterdaten ein wichtiges Qualitätsmerkmal setzen, das Vertrauen schafft. In der gelebten Praxis brauchen Unternehmen für den sicheren Umgang mit personenbezogenen Daten klare Zielsetzungen und eine gute Organisation. Mit unserem aktuellen Querdenker bieten wir Ihnen einen Einblick in das komplexe, spannende Thema. Unser Expertenteam steht Ihnen für die datenschutzrechtliche Beratung und als externer Datenschutzauftragter gerne zur Seite.

Herzlichst, Ihr Dr. Hansjörg Reichert



unsere Themen

RECHT

Meldepflicht bei **„Datenpannen“**

Anforderungen an die unternehmensinterne Erfassung und Strukturierung von Daten als Voraussetzung für eine datenschutzrechtliche „Selbstanzeige“ gemäß § 42 a BDSG bei Datenpannen.

Felix Strache, Rechtsanwalt

Elektronische Datenverarbeitung erleichtert die Verwaltung und Pflege umfangreicher Datenbestände, insbesondere Daten von Mitarbeitern, Kunden, Lieferanten und sonstigen Vertragspartnern. Diese Daten sind für Unternehmen von großer wirtschaftlicher Bedeutung. Mit der Speicherung, Nutzung und Verarbeitung dieser Daten geht aber auch eine große Verantwortung einher, diese Daten gegen unbefugte Zugriffe Dritter umfassend zu schützen. Trotz aller Schutzmaßnahmen mittels moderner IT-Sicherheitstechnik kommt es immer wieder zu „Datenpannen“ in Form eines sorgfaltswidrigen Umgangs der Unternehmen mit den Daten oder durch Datendiebstahl, z.B. externe Angriffe von Computer-Hackern. Die Folgen solcher Datenpannen für die betroffenen Personen sowie die Unternehmen können schwerwiegend sein, denkt man z.B. an einen unberechtigten Zugriff auf Personal- oder Bankdaten. Auch geht mit solchen Datenpannen ein erheblicher Vertrauensverlust einher, der vor allem bei bekannten Unternehmen durch öffentliche Berichterstattung verstärkt wird.

Wann besteht eine Meldepflicht?

Ob eine Meldepflicht nach § 42 a BDSG besteht, ist anhand der folgenden 4 Fragen zu klären:

1. Wer ist meldepflichtig?

Nichtöffentliche Stellen (natürliche und juristische Personen jeglicher Rechtsform) und zum Teil öffentliche Stellen (öffentlich-rechtliche Wettbewerbsunternehmen des Bundes).

2. Welche personenbezogenen Daten sind betroffen?

- besondere Daten (Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse, philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben),
- die einem Berufsgeheimnis unterliegen,
- die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen,
- Daten zu Bank- und Kreditkartenkonten.

3. Was ist mit den Daten geschehen?

Daten wurden unrechtmäßig an Dritte übermittelt oder sind auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt.

4. Welche Folgen müssen den Betroffenen drohen?

Schwerwiegende Beeinträchtigung der Rechte oder schutzwürdigen Interessen (insbesondere auch Vermögensinteressen) der Betroffenen. Darauf, dass eine solche Beeinträchtigung bereits eingetreten ist, kommt es nicht an. Vielmehr ist die verantwortliche Stelle verpflichtet eine Gefahrenprognose zu treffen, bei der folgender Grundsatz gilt:
Je größer die mögliche Beeinträchtigung der Rechte oder Interessen der Betroffenen ist, desto geringere Anforderungen sind an die Eintrittswahrscheinlichkeit zu stellen.

(Simitis, BDSG,§ 42a Rn. 9,beck-online)

Die Feststellung des Vorliegens der vier Voraussetzungen ist in der Praxis oftmals sehr schwierig. Vor allem fehlt in den meisten Unternehmen bereits eine Übersicht darüber, was für Daten in welcher Form im Unternehmen überhaupt gespeichert sind. Viel Zeit, dies festzustellen, haben die zuständigen Stellen nicht, da die Meldung unverzüglich, also ohne schuldhaftes Zögern erfolgen muss. Unternehmen sind daher gut beraten, durch einen betrieblichen Datenschutzbeauftragten laufend den Überblick darüber zu behalten, welche personenbezogenen Daten zu welchem Zweck gespeichert

werden und den Grundsatz der Datensparsamkeit ernst zu nehmen. Durch das unnötige Speichern von personenbezogenen Daten erhöht sich auch die Gefahr, dass diese Daten bei Datenpannen in die Hände unbefugter Dritter gelangen und eine Meldepflicht nach dem BDSG ausgelöst wird. Bei Unterlassung der Meldung drohen den zuständigen Stellen neben Schadensersatzansprüchen die Verhängung eines Bußgeldes bis zu einem Betrag von 300.000 €.

Ausblick: Rechtslage nach der EU-Datenschutz-Grundverordnung

Auch unter der ab Mai 2018 geltenden EU-Datenschutz-Grundverordnung (EU-DSVGO) wird die Meldepflicht bei Datenpannen bestehen bleiben. Die Schwellen für eine Meldepflicht werden im Vergleich zur aktuellen Rechtslage sogar noch weiter abgesenkt. Es wird zukünftig auch unterschiedliche Voraussetzungen für eine Meldung gegenüber den Behörden und den Betroffenen geben, wobei eine Meldepflicht gegenüber den Behörden der Regelfall sein wird. Eine Meldung gegenüber den Betroffenen wird hingegen nur dann erfolgen müssen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht, wobei es allerdings nicht mehr darauf ankommt, dass bestimmte Datenkategorien betroffen sind.

Des Weiteren wird es für die Meldung zukünftig eine verbindliche Meldefrist von 72 Stunden geben, sodass es zukünftig keinen zeitlichen Spielraum mehr geben wird, um sich einen ausreichenden Überblick über die betroffenen Daten zu verschaffen, das voraussichtliche Missbrauchsrisiko abzuschätzen und über einen bestehenden Meldepflicht zu entscheiden.

Auch im Hinblick auf die zukünftig deutlich höheren Bußgelder nach der EU-DSGVO sollten die Meldepflichten gegenüber den Behörden und Betroffenen deutlich ernster genommen werden, als dies bislang vielfach der Fall sein dürfte.

Unternehmen, die hier die erforderlichen Vorkehrungen treffen und ggf. Anpassungen ihrer Datenverwaltung vornehmen, brauchen auch die neu geregelten Meldepflichten nach der EU-DSGVO nicht zu fürchten. Und auch im Hinblick auf das bereits in 2015 in Kraft getretene IT-Sicherheitsgesetz, welches für Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung u.a. spezifische Meldepflichten bei erheblichen IT-Störungen vorsieht, ist neben dem Einsatz von IT-Sicherheitstechnik gemäß dem neusten Stand der Technik auch eine strukturierte und gesicherte Datenverwaltung von überragender Bedeutung. ■

Lassen Sie sich beraten

- Wie verschaffe ich mir einen Überblick über die im Unternehmen gespeicherten Daten?
- Wie stelle ich den Umgang mit personenbezogenen Daten im Unternehmen organisatorisch sicher?
- Was kann ich sonst noch präventiv gegen eine Datenpanne tun und wie gehe ich bei Eintritt einer Datenpanne / IT-Störung vor?

RECHT

Betriebliche **IT-Weisungen**

Arbeitgeber, die hierzu nichts regeln, gehen erhebliche Risiken ein

Felix Strache, Rechtsanwalt

Kaum ein Arbeitsplatz kommt heute noch ohne informationstechnische (IT-) Unterstützung aus. EDV-gestützte Datenverarbeitung ist heutzutage Standard in jedem Unternehmen. Die Bedeutung der IT am Arbeitsplatz wird zukünftig auch noch weiter zunehmen und die Arbeitswelt damit nachhaltig verändern. Mitarbeiter, die vorwiegend mit dem Computer arbeiten, sind nicht mehr zwingend an einen bestimmten Arbeitsplatz gebunden und können auf ihre Arbeitsmaterialien aufgrund von Serverlösungen von fast jedem beliebigem Ort mittels Internetzugang zugreifen. Trotz dieser erheblichen Veränderungen der Arbeitswelt finden sich in zahlreichen Unternehmen / Betrieben kaum oder gar keine betrieblichen Regelungen zur Nutzung und zum Umgang mit der vom Arbeitgeber bereitgestellten oder vom Mitarbeiter verwendeten eigenen IT. Hieraus resultieren erhebliche Risiken für Betriebs- und Geschäftsgeheimnisse und vor allem auch für die durch datenschutzrechtliche Bestimmungen geschützten personenbezogenen Daten von Kunden, Mitarbeitern und Geschäftspartnern.

Erhebliche Risikofaktoren für eine unbefugte Kenntniserlangung bzw. Verwendung dieser Daten zum Nachteil der Betroffenen sind eine unzureichende technische Datensicherheit und vor allem ein sorgfaltswidriger bzw. gedankenloser Umgang mit den Daten durch die Mitarbeiter. Ein in der Praxis häufig anzutreffender Fall ist zum Beispiel der Umgang mit vertraulichen Daten von Vertragspartnern, mit denen eine Geheimhaltungsvereinbarung mit Vertragstrafenregelung bei Verstößen geschlossen wurde. Sofern es keine betrieblichen Regelungen zum Umgang mit solchen geheimhaltungsbedürftigen Daten gibt, ist ein Verstoß gegen die Geheimhaltungsvereinbarung schnell geschehen und die meist empfindlich hohe Vertragsstrafe zur Zahlung fällig.

Fehlende Regelungen zur Privat-Nutzung der IT und des betrieblich zur Verfügung gestellten Internetzugangs, insbesondere auch des betrieblichen E-Mail-Accounts schaffen weitere rechtliche Risiken und Unklarheiten für den Arbeitgeber. So


© Jakub Jirsák - Fotolia.com

kann eine exzessive private Nutzung die Produktivität und Qualität der Arbeitsleistung der Mitarbeiter erheblich verschlechtern, vor allem aber im Hinblick auf den Schutz der personenbezogenen Daten aus der Privatnutzung ergeben sich Probleme für den Arbeitgeber. Bei z.B. ausdrücklicher Erlaubnis der Privatnutzung des betrieblichen E-Mail-Accounts durch die Mitarbeiter oder zumindest einer entsprechende betrieblichen Übung, ergeben sich dann gesetzliche Schranken im Hinblick auf den Zugriff auf die betrieblichen E-Mail-Accounts der Mitarbeiter. Ein Verstoß gegen die einschlägigen gesetzlichen Normen kann zu Unterlassungs- und ggf. Schadensersatzansprüchen des Mitarbeiters führen oder zu Maßnahmen nach dem Bundesdatenschutzgesetz (BDSG), insbesondere Bußgeldzahlungen. Im schlimmsten Fall können Verstöße sogar strafrechtliche Folgen für die Vertretungsorgane des Unternehmens nach sich ziehen. Strafrechtliche Sanktionen können sich z.B. aus Verstößen gegen Bestimmungen des Strafgesetzbuches (insb. § 206 StGB) und auch strafrechtliche Bestimmungen des BDSG (§ 44 BDSG) ergeben. Der richtige Umgang mit der betrieblichen und der von den Mitarbeitern selbst zur Verfügung gestellten IT sowie der zulässige Rahmen einer privaten Nutzung sollten zur Vermeidung unnötiger rechtlicher Risiken und Unklarheiten zusammenfassend in einer IT-Weisung oder IT-Richtlinie geregelt werden, die entweder einzelvertraglich zum Bestandteil der Arbeitsverträge gemacht werden sollte oder bei Vorhandensein eines Betriebsrats auch in Form einer IT-Dienstvereinbarung / Personalvereinbarung verabschiedet werden kann. ■

Lassen Sie sich beraten

- Habe ich eine private Nutzung der betrieblichen IT / des Internetzugangs / des Mail-Accounts durch Duldung / der Schaffung einer betrieblichen Übung bereits gestattet?
- Wie kann ich eine bereits gestattete private Nutzung der betrieblichen IT wieder aufheben?
- Wie kann ich in meinem Unternehmen / Betrieb eine einheitliche Regelung zum Umgang und zur Nutzung der IT umsetzen?
- Welche Mindestregelungen sollten in einer IT-Weisung / Richtlinie / Dienstvereinbarung enthalten sein?

Private Hardware im Unternehmen - **BYOD und Datenschutz**

Die Verbreitung von Smartphones und Tablet-Computern wie auch die von vielen Anwendern objektiv oder subjektiv empfundene höhere Gebrauchstauglichkeit (Usability) der meist vorrangig für den privaten Gebrauch konzipierten Geräte haben in den vergangenen Jahren einen Wandel in der Abgrenzung bei der Verwendung betrieblicher und privater Hardware am Arbeitsplatz ausgelöst.

Matthias Herkert, Leiter Consulting


© blackzheep - Fotolia.com

Moderne Consumer-Endgeräte unterscheiden sich heute im Leistungsumfang häufig kaum noch von traditioneller betrieblicher Hardware. Zunehmend verdrängen etwa die vorrangig für den Verbrauchermarkt entwickelten Betriebssysteme von Apple (iOS), Google (Android) und Microsoft (Windows Phone) die im betrieblichen Bereich bislang etablierten Lösungen wie RIM (BlackBerry). Der Wunsch, private Geräte auch für dienstliche Zwecke zu nutzen, dürfte daher auch in den kommenden Jahren weiter steigen. So erlaubten nach einer Studie des BITKOM-Verbandes 2013 bereits 43 Prozent der ITK-Unternehmen (Informations- und Telekommunikationstechnik) unter dem Schlagwort »Bring Your Own Device« (BYOD) ihren Mitarbeitern, private Endgeräte mit dem Unternehmensnetzwerk zu verbinden. Hierbei rückt neben arbeits-, steuer- und lizenzrechtlichen Fragen sowie den technischen Herausforderungen auch der Datenschutz bei der Gestaltung innerbetrieblicher Programme in den Fokus.

BYOD zw. Datenschutzrecht und betrieblicher Informationstechnologie

Während viele Betriebe beim Entwurf praxistauglicher BYOD-Regelungen noch immer vorrangig nach technischen Strategien suchen, werden Datenschutzthemen mitunter vollständig ausgeblendet. Da jedoch die erfolgreiche Umsetzung der IT-Lösungen, wie etwa der Einsatz eines Mobile Device Managements, regelmäßig auch Aspekte des Datenschutzes berühren, laufen BYOD-Lösungen ohne Begleitung durch den Datenschutz regelmäßig Gefahr zu kurz zu greifen.

Trennung von Unternehmensdaten und privaten Daten

So erfordert die im Datenschutz geforderte Herrschaft über die erhobenen, verarbeiteten und genutzten Daten häufig einen unmittelbaren Zugriff auf den Datenbestand oder ein einzelnes Datum. Greifbar wird diese Notwendigkeit etwa mit Blick auf das Betroffenenrecht auf der wirksamen und endgültigen Datenlöschung, das ohne den direkten Zugriff des Unternehmens auf das Speichermedium meist bereits an den mangelnden IT-Kenntnissen des Device-Eigentümers scheitern wird. Da dieser Zugriff auf den privaten Device ohne wirksame Regelungen in vielen Fällen rechtlich nicht zulässig sein wird, besteht hier in allen BYOD-Gestaltungen ein wichtiges Handlungs- und Gestaltungsfeld.

Technische und organisatorische Datenschutzmaßnahmen im Kontext von BYOD

Im Weiteren entsteht über die ohnehin notwendigen Maßnahmen zur Datensicherheit hinaus unter anderem durch den mobilen Charakter der BYO-Geräte zusätzlicher Handlungsbedarf bei der Gestaltung angemessener Sicherheitsmaßnahmen. Erfahrungsgemäß kommt hierbei erschwerend hinzu, dass viele Benutzer datenschutz- und sicherheitsbedingte Einschränkungen in der Nutzung Ihres privaten Gerätes kaum zulassen und Zugriffe durch den Arbeitgeber in vielen Fällen nicht akzeptiert werden.

Auf technischer Ebene scheinen sich daher Virtualisierungslösungen mit Thin-Clients und die zentrale Administration über Mobile-Device-Management-Systeme zumindest derzeit durchzusetzen.

Fazit

Die berufliche Nutzung privater Devices stellt gerade in kleinen und mittelständischen Unternehmen neue Herausforderungen an die Informationssicherheit und den Datenschutz. Dabei wird wohl nur in Ausnahmefällen der im privaten Umfeld gewohnte „freie Umgang" mit den BYO-Devices auch im geschäftlichen Bereich möglich sein. Während technische Maßnahmen alleine in keinem Fall ausreichen, können die bestehenden Risiken in der Kombination mit organisatorischen Vorgaben und verbindlichen Regelungen in der Praxis jedoch Größtenteils beherrscht werden. Im Ergebnis wird der Erfolg von BYOD-Lösungen von einem ausgewogenen Verhältnis zwischen dem begründeten Vertrauen in das Verantwortungsbewusstsein der Mitarbeiter auf der einen Seite sowie transparenten und an die Struktur des Unternehmens angepassten Regelungen auf der anderen Seite abhängen. ■

CONSULTING

Das Recht am eigenen Bild

Das Recht am eigenen Bild im Arbeitsverhältnis - der Prozess zur Einwilligung zum Umgang mit Mitarbeiterfotografien ist für viele Unternehmen ein wichtiger Bestandteil der Datenschutzorganisation.

Matthias Herkert, Leiter Consulting

Fotografien von Mitarbeitern auf der Homepage, in Image- oder Produktflyern, in Newslettern, im Intranet oder in Sozialen Medien – die Kommunikationswege, über die Unternehmen Fotografien Ihrer Mitarbeiter veröffentlichen wollen, werden - nicht zuletzt wegen der zunehmenden Digitalisierung der Kommunikation - immer vielfältiger. Das Problem bleibt indes das Alte: welche Datenschutzaspekte sind zu beachten, um die Veröffentlichung von Mitarbeiterfotografien „auf sichere Beine zu stellen"?

Im Grunde scheint die Lösung einfach: Die Verarbeitung von Bildnissen von Mitarbeiter, egal ob gedruckt oder digital, setzt die Einwilligung des Betroffenen voraus.

In der Praxis empfiehlt es sich, im Umgang mit Fotografien, auf denen Beschäftigte zu sehen sind und erkannt werden können (Bildnisse), weitgehend standardisierte Datenschutzprozesse zu entwickeln und zu etablieren. Je mehr Transparenz im Einwilligungsprozess herrscht und je weniger „Einzelfälle" gelöst und kommuniziert werden müssen, desto höher ist meist die Akzeptanz. Dabei sind die „Hürden" bis zu einer wirksamen Einwilligung des Betroffenen meist gar nicht so hoch.

Anlass und Bestimmtheit

Der Betroffene muss über Zweck, Art und Umfang der geplanten Veröffentlichung aufgeklärt werden. Als Faustregel gilt, dass, je weitgehender die Privatsphäre des Betroffenen berührt wird, auch der Umfang der Aufklärung zunehmen muss.

Freiwilligkeit

Die Einwilligung muss freiwillig und selbstbestimmt sowie ohne jeden Zwang und informiert erfolgen. Dem Betroffenen muss deutlich werden, dass er die Einwilligung verweigern kann, ohne dass ihm hieraus Nachteile entstehen. Soweit im Einzelfall keine konkreten Gründe dagegen sprechen, ist eine entsprechende Einwilligung wohl auch im Beschäftigungsverhältnis möglich.

Schriftform

Die Einwilligung der Beschäftigten bedarf der Schriftform. Die Schriftform soll nochmals aufzeigen, dass die Einwilligung freiwillig erfolgt und dem Beschäftigten aus einer Verweigerung der Einwilligung keine negativen Folgen erwachsen.

Sensitive Daten

Soweit sich die Einwilligung auch auf „besondere Arten personenbezogener Daten" i.S.d. Datenschutzes beziehen soll, müssen diese ausdrücklich genannt werden. Sehen Sie einen entsprechenden Hinweis im Einwilligungsformular vor, da „alltägliche" Gesundheitsdaten (z.B. Brille auf dem Foto sichtbar) oder Daten zur ethnischen Herkunft (Hautfarbe auf dem Foto erkennbar) sonst leicht übersehen werden.

Widerruf

Unabhängig von den Möglichkeiten und Grenzen des Widerrufs muss der Beschäftigte vor seiner Einwilligung über die Möglichkeiten eines Widerrufs aufgeklärt werden. „Großzügige Widerrufsmöglichkeiten" verbessern in der Praxis meist die Zustimmungsquote der Mitarbeiter.

Betriebsrat

Aus den allgemeinen Mitwirkungs- und Mitbestimmungstatbeständen des Betriebsverfassungsgesetzes können Mitbestimmungsrechte des Betriebsrates bestehen, die zu beachten sind. ■

DATENSCHUTZ ORGANISIEREN

- Prüfen Sie im ersten Schritt, ob die Datenverwendung nicht bereits auf gesetzlicher Grundlage erlaubt ist (z.B. Mitarbeiterfotografie auf dem Firmenausweis).
- Entwerfen Sie einen standardisierten Prozess für die Einwilligung und eine einheitliche Vorlage der Einwilligungserklärung.
- Klären Sie die innerbetrieblichen Rollen im Einwilligungsprozess.
- Passen Sie die Vorlage vor jeder Verwendung an den konkreten Sachverhalt an.
- Unkonkrete „Pauschaleinwilligungen" reichen nicht aus, es ist aber möglich zum Beispiel für bestimmte Kommunikationsmedien grundsätzliche Einwilligungen im Vorgriff auf spätere (zeitnahe) Verwendungen zu erklären.
- Ärgern Sie sich nicht über den Bürokratismus sondern lösen Sie das Problem pragmatisch und transparent.

Sicherheit beim Telefonieren mit Voice-Over-IP

Bis 2018 will die Telekom den Wechsel in das „Netz der Zukunft" abschließen. Sowohl Privathaushalte als auch Unternehmen telefonieren dann zukünftig digital über das Internet mit Voice-Over-IP (VoIP). Darauf müssen Sie in Zukunft achten:

Stefan Tröndle, Business Process Architect, EDV:Systemhaus Tröndle e.K.

In der Welt der bisherigen Telefonie wurde eine Leitung durch einen Anbieter zu den Anschlüssen durchgeschaltet. Diese Leitung unterlag der Kontrolle des Anbieters und die darüber geführten Telefongespräche wurden in der Regel eindeutig einem Anschluss geografisch zugeordnet. Bis 2018 will die Telekom auf das Telefonieren mit Voice-Over-IP (VoIP) umstellen. Dann gibt es diese Verbindung nicht mehr. Telefongespräche mit VoIP können an jedem beliebigen Internetanschluss mit ausreichender Bandbreite geführt werden. Dies bringt neben einer besseren Sprachqualität (insofern beide Gesprächspartner über VoIP telefonieren) auch eine höhere Mobilität und Flexibilität mit sich. Letzteres ist jedoch Vor- und Nachteil zugleich.

Was sind mögliche Gefahren des Voice-Over-IP?

Eine Gefahr besteht beim Verlust oder dem unachtsamen Bekanntgeben der Zugangsdaten gegenüber Fremden, denn Dritte könnten so auf Kosten des Anschlussinhabers Gespräche führen.

Neben dem Telefonieren auf Kosten anderer ist somit auch eine Umleitung auf andere Nummern und so eine erhebliche Schädigung Ihres Geschäfts möglich.

Zudem ermöglicht es die Funktion „Clip-no-screening", die bei vielen Anbietern sehr einfach freigeschaltet werden kann, nahezu jedem, seinem Gegenüber eine beliebige Rufnummer zu präsentieren. In der Folge gibt die Rufnummernanzeige keine verlässliche Auskunft mehr über die Identität des Anrufers.

Dies stellt auch vor allem beim Notruf ein Problem dar. Angenommen, eine Person aus Konstanz, die mit ihrem geschäftlichen Notebook mit installiertem Software-Telefon in München ist, muss die Feuerwehr rufen. Der Anruf erfolgt mit der örtlichen Nummer (Konstanz) und wird deshalb automatisch mit der örtlichen Rettungsleitstelle (Konstanz) verbunden.

Unsere Empfehlung: Halten Sie Ihre Zugangsdaten geheim und ändern Sie die vom Anbieter vergebenen Kennwörter direkt nach dem Erhalt.

Und wie sieht es mit der Sicherheit aus? Ist das Netz abhörsicher?

Im Vergleich zum analogen und ISDN-Netz steht es beim Telefonieren über das Internet ähnlich um die Abhörsicherheit bzw. –unsicherheit. Gespräche über das Internet hinterlassen Metadaten, die Angreifern (oder auch Behörden) Aufschluss über Gespräche geben könnten. Verbindungen zwischen der Telefonanlage oder dem Software-Telefon zum Provider kann man kontrollieren und in der Regel auch verschlüsseln. Spätestens dann aber hängt es davon ab, wie Ihr Gesprächspartner mit seinem Provider verbunden und ob das Gespräch Ende-zu-Ende verschlüsselt ist. Erst nach der vollständigen Umstellung aller Netze hin zu Voice-Over-IP (vorauss. im Jahr 2020) kann man davon ausgehen, dass Gespräche in der Regel verschlüsselt aufgebaut werden.

Unsere Empfehlung: Integrieren Sie verschiedene Maßnahmen zur Sicherheit beim Telefonieren mit VoIP in Ihr Datenschutzkonzept:

- Software/Firmware der Telefonanlage/Router/Firewall immer auf dem aktuellen Stand halten.
- In der Firewall sollten lediglich die IP-Adressen des Providers freigegeben werden
- Änderung der vom Provider zugewiesenen Kennwörter und anschließende Dokumentation und Sicherung. ■

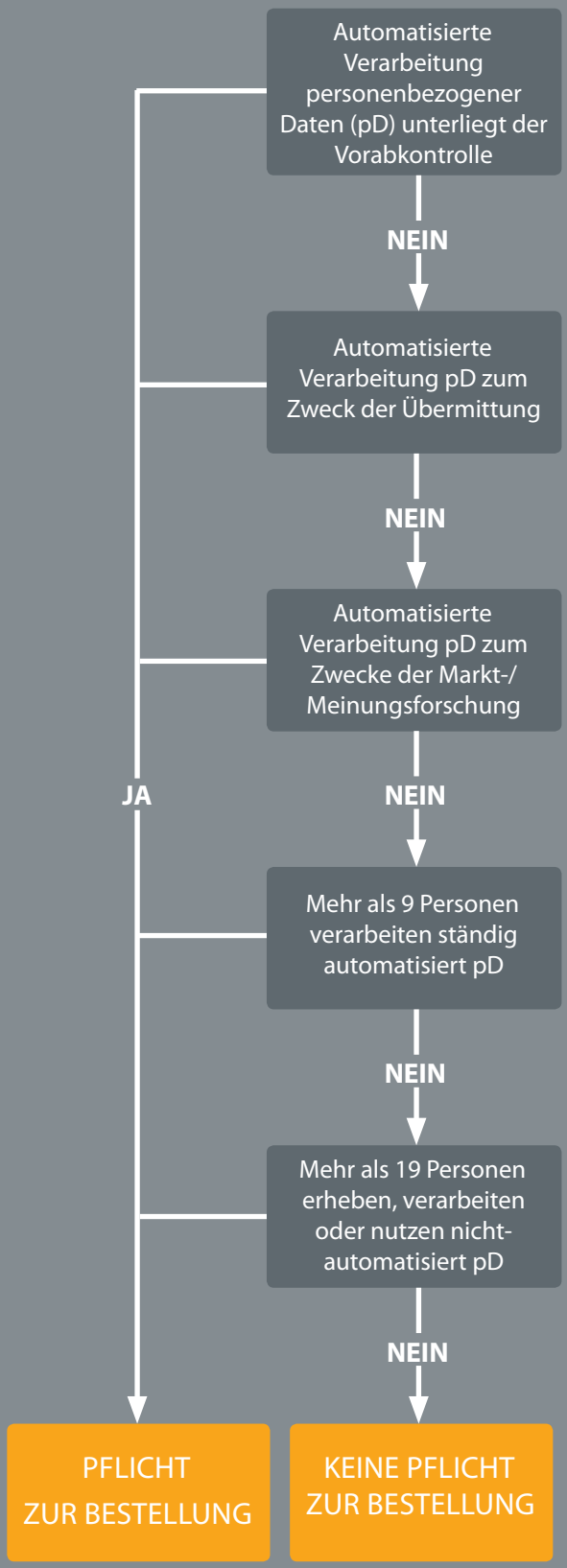
Stefan Tröndle leitet ein Systemhaus in Singen mit 11 Mitarbeitern, die sich mit allen Aspekten von Kommunikation und Sicherheit beschäftigen.

Die Faszination für Telekommunikation hat er von seinem Großvater, einem Fernmeldebetriebsinspektor, geerbt.

TRÖNDLE
systemhaus providing solutions

KURZ**CHECK**

Brauche ich einen Datenschutz-beauftragten in meinem Unternehmen?*



**Kurzcheck gilt für nicht-öffentliche Stellen*

Wir unterstützen Sie!


Dr. Hansjörg Reichert


Matthias Herkert


Felix Strache

Unsere Kanzlei berät zu Datenschutz- und IT-Projekten seit vielen Jahren. Hierbei bieten wir unseren Mandanten datenschutzrechtliche Beratung und die Bestellung als externer Datenschutzbeauftragter. Unser Ziel ist es, für die individuellen Fragestellungen unserer Mandanten datenschutzrechtlich passgenaue Lösungen zu entwickeln und durch die praxisnahe Gestaltung datenschutzkonformer Prozesse, die Umsetzung gesetzlicher Vorgaben effizient in bestehende betriebliche Abläufe zu integrieren.

Gemeinsam mit unseren Mandanten entwickelt unser hochqualifiziertes und projekterfahrenes Team aus Anwälten und Wirtschaftsberatern moderne und individuelle Datenschutzorganisationen, die sich ohne unnötigen Zusatzaufwand in die bestehenden betrieblichen Abläufe integrieren.

Schauen Sie auf unserer Website www.reichert-reichert.de vorbei oder sprechen Sie uns an.

IMPRESSUM

Herausgeber
reichert & reichert
steuerberater & rechtsanwaltskanzlei

Zeppelinstraße 7 - 78224 Singen
+49 (0) 7731.9587-0

Reichenaustraße 19a - 78467 Konstanz
+49 (0) 7531.81987-0

kanzlei@reichert-reichert.de

Redaktion
Dr. Hansjörg Reichert, Matthias Herkert, Felix Strache

Gastautor
Stefan Tröndle, Systemhaus Tröndle GmbH

Layout
Anita Steinbrück

erschienen im November 2016

reichert reichert
steuern . recht . consulting