Fokus **DATENSCHUTZ** | 1

Der **Querdenker**

Themen aus der Kanzlei **reichert & reichert**

reichert reichert
steuern . recht . consulting

DER NEUE QUERDENKER
zum Thema Datenschutz

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 Datenschutzbeauftragter gerne zur Seite.

Herzlichst, Ihr Dr. Hansjörg Reichert

Die **DATENSCHUTZ-GRUNDVERORDNUNG**
löst das Bundesdatenschutzgesetz ab

Am 25. Mai 2018 hat die europäische Datenschutz-Grundverordnung (DSGVO) das seit 1977 in mehreren Fassungen angepasste, rein nationale Bundesdatenschutzgesetz (BDSG-alt) abgelöst. Ziel der neuen Regelungen war ein unionsweit einheitlicher und wirksamer Schutz personenbezogener Daten, der nun insbesondere auch den Anforderungen an eine digitalisierte, grenzüberschreitende Welt Rechnung tragen soll.

Obwohl hierbei keine Vorgabe des BDSG-alt völlig unverändert in der DSGVO zu finden ist, führte die Umstellung für eine große Zahl von Unternehmen zu keinem grundlegenden Anpassungsbedarf der bisherigen Datenschutzorganisation. So haben die früher bereits aus dem BDSG-alt bekannten Datenschutz-Mindeststandards auch unter der Datenschutz-Grundverordnung weiterhin Gültigkeit und auch die Grundprinzipien des Datenschutzes bestehen weitgehend fort. Die zum Teil geäußerten Befürchtungen, durch europaweit harmonisierte Datenschutzregeln könnte das bis dahin in Deutschland erreichte Datenschutzniveau unterlaufen oder abgesenkt werden, waren damit völlig unbegründet.

Wichtige Ergänzungen und Anpassungsbedarfe kamen indes unter anderem durch das Marktortprinzip, neue Informationspflichten gegenüber den von geplanten Datenverarbeitungen betroffenen Personen, die teilweise Verlagerung von Verantwortungen bei der Datenverarbeitung im Auftrag, dem sogenannten „One-Stop-Shop-Mechanismus“ und den geänderten Möglichkeit zur Verarbeitung personenbezogener Daten im Konzern insbesondere auf datenverarbeitungsintensive und datengetriebene Unternehmen zu.

Neu und gerade in den Medien viel beachtet, waren in jedem Fall die deutlich höheren Sanktionen bei Verstößen, die nun bis zu vier Prozent des gesamten weltweiten Jahresumsatzes beziehungsweise bis zu 20 Mio. Euro reichen können. Eine Androhung, die zu einer bislang im Datenschutz weitgehend unbekannten Sorge und einem nicht immer gut begründeten Aktionismus geführt hat.

Denn unverändert bleibt auch nach dem 25. Mai 2018 die Tatsache, dass Datenschutz kein Zustand sondern ein fortlaufender Prozess ist. Unternehmen, die Ihre Datenschutzorganisation stetig weiterentwickeln und fortlaufend in einem Dialog mit ihrem internen oder externen Datenschutzbeauftragten blieben, hatten bereits unter dem BDSG (alt) kaum Gründe zu Sorge – und können auch unter dem neuen Recht auf diesem Fundament sehr gut weiterarbeiten und gestalten.

IHR ANSPRECHPARTNER:

MATTHIAS HERKERT,
LEITER CONSULTING

Betriebliche **IT-Weisungen**

Arbeitgeber die hierzu nichts regeln, gehen erhebliche Risiken ein!

ARBEITGEBER DIE HIERZU NICHTS REGELN, GEHEN ERHEBLICHE RISIKEN EIN!

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 weiter zunehmen und die Arbeitswelt nochmals nachhaltig verändern. Mitarbeiter, die vorwiegend mit dem Computer arbeiten, sind bereits heute in vielen Fällen nicht mehr an einen bestimmten Arbeitsplatz gebunden und können auf ihre Arbeitsmaterialien über Serverlösungen von fast jedem beliebigem Ort zugreifen. Trotz dieser erheblichen Veränderungen der Arbeitswelt finden sich in zahlreichen Unternehmen wenige 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 wie auch für die durch datenschutzrechtliche Bestimmungen geschützten personenbezogenen Daten von Kunden, Mitarbeitern und Geschäftspartnern.

RISIKOFAKTOREN BESTEHEN AUF TECHNISCHER UND MENSCHLICHER SEITE

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

DIE DULDUNG PRIVATER INTERNET- UND E-MAIL-NUTZUNG KANN ZU STRAFRECHTLICHEN SANKTIONEN FÜHREN

Fehlende Regelungen zur Privat-Nutzung der IT, des betrieblich zur Verfügung gestellten Internetzugangs und insbesondere auch des betrieblichen E-Mail-Accounts schaffen weitere rechtliche Risiken und Unklarheiten für den Arbeitgeber. So kann eine exzessive private Nutzung die Produktivität und Qualität der Arbeitsleistung der Mitarbeiter erheblich verschlechtern. Aber auch aus der Privatnutzung betrieblicher Systeme ergeben sich erhebliche Probleme für den Arbeitgeber. Bei zum Beispiel ausdrücklicher Erlaubnis der Privatnutzung des betrieblichen E-Mail-Accounts durch die Mitarbeiter oder bereits bei einer entsprechende betrieblichen Übung (~ wissentliche Duldung), ergeben sich dann gesetzliche Schranken im Hinblick auf den Zugriff des Arbeitgebers auf die betrieblichen E-Mail-Accounts der Mitarbeiter. Ein Verstoß gegen die einschlägigen gesetzlichen Normen kann zu Unterlassungs- und ggf. Schadensersatzansprüchen des Beschäftigten führen oder zu Maßnahmen nach der Datenschutz-Grundverordnung, insbesondere zu Zahlungen von Geldbußen. 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, über die Öffnungsklausel des Artikel 84 Abs. 1 DSGVO, auch strafrechtliche Bestimmungen des BDSG (§ 42 BDSG) ergeben.

MIT IT-WEISUNG UND IT-RICHTLINIE KANN DEN RISIKEN WIRKSAM BEGEGNET WERDEN

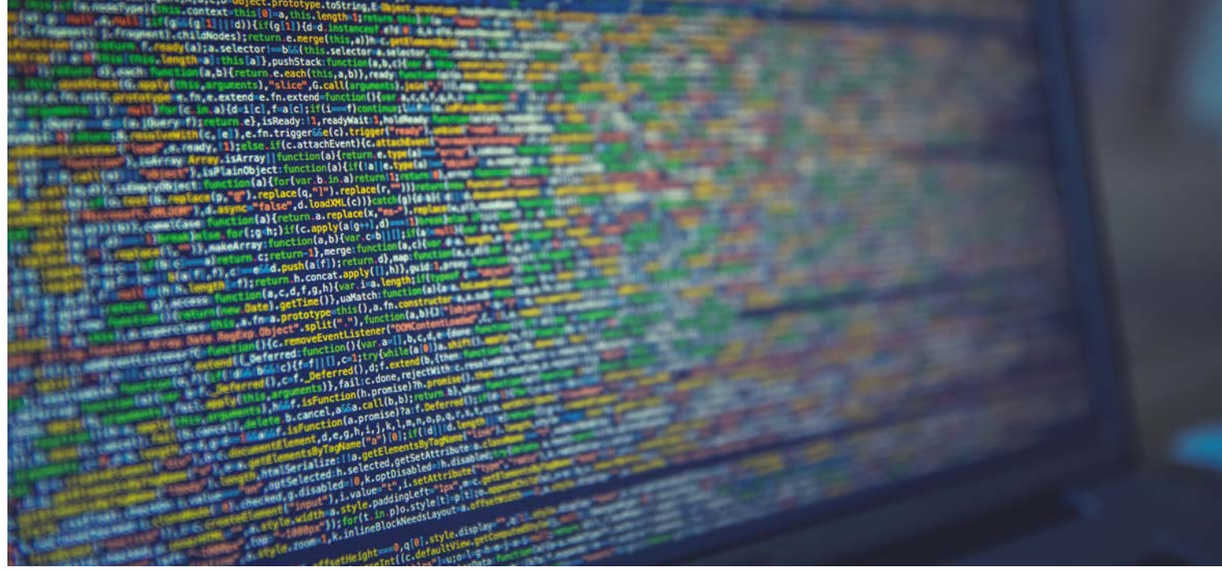
Der richtige Umgang mit der betrieblichen und der von den Mitarbeitern selbst zur Verfügung gestellten IT sowie der zulässige Rahmen einer privaten Nutzung sollten zur Vermeidung unnötiger rechtlicher Risiken und Unklarheiten zusammenfassend in einer IT-Weisung oder IT-Richtlinie geregelt werden, die entweder einzelvertraglich zum Bestandteil der Arbeitsverträge gemacht werden sollte oder bei Vorhandensein eines Betriebsrats oder einer Mitarbeitervertretung auch in Form einer IT-Dienstvereinbarung / Personalvereinbarung verabschiedet werden kann. Soweit durch eine entsprechende Duldung bzw. Schaffung einer betrieblichen Übung die private IT-Nutzung bereits (ungewollt) gestattet wurde, sollte diese wieder aufgehoben werden.

IHR ANSPRECHPARTNER:

MATTHIAS HERKERT,
LEITER CONSULTING

DATENPANNE

Die Beurteilung und Meldung der Verletzung des Schutzes personenbezogener Daten stellt hohe Anforderungen an Unternehmen



NICHT JEDE DATENPANNE IST VERMEIDBAR UND NICHT JEDER FEHLER KANN VERHINDERT WERDEN. KOMMT ES ZU EINER DATENPANNE IST EIN RASCHES HANDELN UND EINE GUT ORGANISIERTE PROJEKT-ORGANISATION NOTWENDIG, UM EMPFINDLICHE GELDBUSSEN ZU VERMEIDEN.

Die Vorschriften zur Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 33 DSGVO) dient, gemeinsam mit den Regelungen zur Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 34 DSGVO), dem Schutz der Rechte der von der Datenverarbeitung betroffenen natürlichen Personen bei Datenschutzverletzungen. Die Pflicht zur Meldung einer Verletzungshandlung soll die Aufsichtsbehörde über eine solche Gefahr in Kenntnis setzen und gibt ihr so eine Grundlage für die Entscheidung über den Einsatz ihrer gesetzlichen Befugnisse. Die Meldepflicht dient also zum einen der Minimierung der negativen Auswirkungen von Datenschutzverletzungen durch Publizität, gleichzeitig gewährt die Vorschrift vorbeugenden Schutz des Betroffenen, indem sie Anreize zur Vermeidung von (zukünftigen) Verletzungen beim Verantwortlichen setzt.

DATENPANNEN KÖNNEN JEDES UNTERNEHMEN TREFFEN

Eine Verletzung des Schutzes personenbezogener Daten (sog. Datenpanne) liegt immer dann vor, wenn der datenverarbeitenden Stelle bekannt wird, dass personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten zur Kenntnis gelangt sind oder gelangt sein könnten. Eine unrechtmäßige Kenntnisnahme kann zum Beispiel der Verlust eines mobilen Devices (z.B. Notebook, Tablet oder Smartphone) oder eines Speichermediums (z.B. USB-Stick, CD-ROM), der Diebstahl eines solchen Gerätes, der Versand einer E-Mail an einen oder mehrere falsche Adressaten oder jeder Angriff aus einem Netzwerk, insbesondere aus dem Internet, auf ein Computersystem (z.B. auf einen Webserver oder Applikationsserver) sein.

DIE MELDEPFLICHTEN WURDEN UNTER DER DSGVO ERWEITERT

Im Gegensatz zu den Regelungen des früheren BDSG-alt, das eine Meldepflicht nur für eine Verletzung von bestimmten Datenkategorien vorsah, erstreckt sich die Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten unter der DSGVO nun auf alle personenbezogenen Daten. Gemeldet werden muss in diesem Kontext nun also jede Verletzungshandlung, es sei denn, dass die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Der Verantwortliche muss in einer Risikobewertung die Eintrittswahrscheinlichkeit eines drohenden Schadensereignisses prognostizieren und diese Prognose für eine mögliche spätere Überprüfung durch Aufsichtsbehörden oder Gerichte ausführlich dokumentieren. Eine Meldepflicht besteht hierbei bereits bei Bestehen eines grundsätzlichen, über Geringfügigkeit hinausgehenden Risikos und ist nicht erst im Falle eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen erforderlich.

UNVERZÜGLICHE MELDUNG

Hierbei ist Eile geboten. Die Meldung an die Aufsichtsbehörde hat gemäß Art. 33 Abs.1 S. 1 DSGVO unverzüglich, spätestens jedoch 72 Stunden nach Bekanntwerden zu erfolgen. Soweit zum Zeitpunkt der ersten Meldung, was in der Praxis sehr wahrscheinlich ist, noch nicht der gesamte Umfang der Verletzungshandlung abschließend beurteilt werden kann, sind Teilkenntnisse schrittweise der Aufsichtsbehörde zu melden (Art. 33 Abs. 4 DSGVO).

PRÜF- UND MELDEPROZESSE MÜSSEN IM UNTERNEHMEN EINGEFÜHRT UND GESCHULT WERDEN

Um den gesetzlichen Pflichten nachkommen zu können, muss der Prozess vom Bekanntwerden einer (möglichen) Datenschutzverletzung über deren Beurteilung bis hin zur Entscheidung über eine Meldung an die Aufsichtsbehörden in die Prozessorganisation aufgenommen und innerbetrieblich geschult werden. Anders als in den Meldeprozessen unter dem BDSG-alt, rückt die Bedeutung des Datenschutzbeauftragten dabei zum Zeitpunkt des tatsächlichen Eintretens einer Verletzungshandlung regelmäßig in den Hintergrund. Prozessseitig ist entscheidend, dass die verantwortlichen Vertreter des Unternehmens und der betroffenen Fachabteilungen sowie ein verantwortlicher (interner oder externer) IT-Mitarbeiter oder Informationssicherheitsbeauftragter informiert werden, um in einem ersten Schritt Sofortmaßnahmen zur Verhinderung weiterer Schadensereignisse einzuleiten und im Anschluss den Umfang, die Reichweite, die Intensität sowie mögliche Folgen der Verletzungshandlung möglichst exakt zu beurteilen. Insbesondere bei Angriffen auf Datenverarbeitungsanlagen in globalen Netzwerken können hierfür umfangreiche IT-forensische Analysen notwendig sein, die in vielen Fällen von den Beschäftigten des Unternehmens selber nicht erbracht werden können. Erst auf Grundlage der Informationen aus diesen Analysen kann der Datenschutzbeauftragte das Vorliegen einer Meldepflicht beurteilen und eine entsprechende Empfehlung an das Management oder die Geschäftsleitung geben.

MELDUNGEN KÖNNEN ELEKTRONISCH VORGENOMMEN WERDEN

Ergibt sich aus den Analysen und Beurteilungen das Vorliegen einer Meldepflicht, können die nächsten Schritte zwischenzeitlich in allen Bundesländern digital über die Homepages der jeweils zuständigen Aufsichtsbehörden erfolgen. Die Meldung selber sollte hierbei durch den Datenschutzbeauftragten erfolgen oder mit diesem eng abgestimmt werden, da dieser gemäß Art. 39 Abs. 1 lit. e DSGVO erste Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen ist, und bei den nach der Meldung zu erwartenden Rückfragen meist direkt angesprochen wird.

QUICK WIN

Um im Fall einer Verletzung des Schutzes personenbezogener Daten in der gesetzlich gebotenen Schnelligkeit reagieren zu können und das sichere Zusammenspiel aller benötigten Personen, unter anderem aus der Geschäftsführung, der IT-Abteilung, der von der Datenschutzverletzung betroffenen Fachabteilung und dem Datenschutz zu gewährleisten, sollten die notwendigen Abläufe und Prozesse frühzeitig entworfen und bekannt gemacht werden. Vergleichbar mit Erste-Hilfe- und Brandschutzübungen sollten die Abläufe geübt werden, damit im „Ernstfall" jeder weiß, „wo er hingreifen muss".

IHR ANSPRECHPARTNER:

MARKUS SPÖHR,
WIRTSCHAFTSJURIST

TIPP!

Diesen und viele weitere Artikel finden Sie auch Online auf unserem Blog: www.datenschutz-am-bodensee.com
www.datenschutz-am-bodensee.com/meldung-datenpanne/

WEITERE BEITRÄGE ZUM THEMA "DATENPANNE":

THEMA 1: Erste Geldbuße nach Datenpanne
www.datenschutz-am-bodensee.com/bussgeld-datenpanne/
THEMA 2: Datenpanne bei Facebook
www.datenschutz-am-bodensee.com/facebook-datenpanne/
THEMA 3: Orientierungshilfe des BayLfD zur Meldepflicht bei Datenpannen
www.datenschutz-am-bodensee.com/orientierungshilfe-datenpanne/

Ein Bild sagt mehr als tausend Worte

Das Recht am eigenen Bild

IHRE ANSPRECHPARTNERIN:

LISA-SABRINA LAIS,
BACHELOR OF ARTS

Fotografien auf der Homepage, im Intranet, in Sozialen Medien oder in Image- oder Produktflyern – die visuellen Kommunikationswege werden sind immer vielfältiger. Das Problem bleibt indes das Alte: welche Datenschutzaspekte sind zu beachten, um Fotografien „auf sichere Beine zu stellen"?
Auch unter der Datenschutzgrundverordnung wird der Umgang mit Fotografien in den meisten Fällen wohl auf die Einwilligung des Betroffenen als Rechtsgrund zu stützen sein (Art. 6 Abs. 1 S. 1 lit. a DSGVO). Hierbei empfiehlt es sich, im Umgang mit Fotografien (Bildnisse) standardisierte Datenschutzprozesse zu entwickeln und zu etablieren. Die hierbei wesentlichsten Inhalte zeigen wir Ihnen in diesem Artikel als Überblick auf.

FREIWILLIGKEIT

Der Betroffene muss bei der Abgabe seiner Einwilligung eine echte und freie Wahl haben, sodass er die Einwilligung verweigern kann ohne Nachteile zu erleiden. In Fällen, in denen zwischen dem Anfragenden und dem Einwilligenden ein klares Ungleichgewicht besteht, muss davon ausgegangen werden, dass Einwilligungen nicht freiwillig gegeben werden und daher nicht gültig sind.

BESTIMMTHEIT, INFORMIERTHEIT UND ZWECKBINDUNG

Der Betroffene muss über den konkreten Zweck, Art und Umfang der geplanten Verwendung aufgeklärt werden. Als Faustregel gilt, je tiefer der Eingriff in die Privatsphäre ausfällt, desto höher sind die Anforderungen an die Bestimmtheit der Informationen. Allgemeine oder pauschale Formulierungen, genauso wie Blanko-Einwilligungen, führen dazu, dass keine wirksame Einwilligung vorliegt.

UNMISSVERSTÄNDLICHKEIT

Die Einwilligung des Betroffenen muss in »Kenntnis der Sachlage« erfolgen. Bei der Formulierung der Einwilligungserklärung ist daher zum Beispiel auf ein nicht zwingend erforderliches technisches und fremdsprachiges Fachvokabular genauso zu verzichten wie auf lange juristisch entbehrliche Texte und »Werbefloskeln«.

FORMERFORDERNIS

Einwilligungen müssen in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung gegeben werden. Ein Schriftformerfordernis gibt es unter der DSGVO nicht mehr, vielmehr sind auch elektronische Formate und mündlichen Erklärungen zulässig. Fast unnötig in diesem Kontext zu erwähnen, dass Stillschweigen oder Untätigkeit des Betroffenen keinesfalls eine eindeutig bestätigende Handlung darstellt.

ZEITPUNKT DER EINHOLUNG DER EINWILLIGUNG

Soweit die Einwilligung die Rechtmäßigkeit der Verarbeitung begründen soll, muss die Erklärung der Einwilligung notwendigerweise zeitlich vor der Verarbeitung erfolgen. Eine zu einem späteren Zeitpunkt (nachträglich) erklärte Einwilligung entfaltet ihre Wirkung ausschließlich für die Zukunft und kann, allenfalls »im Hinblick auf mögliche Schadensersatzansprüche der Betroffenen eine Rolle« spielen.

WIDERRUFLICHKEIT

Der Betroffene ist vor Abgabe der Einwilligung ausdrücklich von seinem Recht, die Einwilligung zu einem späteren Zeitpunkt jederzeit zu widerrufen, in Kenntnis zu setzen.

NACHWEISPFLICHT

Über Artikel 7 Abs. 1 DSGVO besteht eine Beweislastregel für das Vorliegen der Einwilligung zu Lasten des Verantwortlichen. Diese Regelung konkretisiert die Rechenschaftspflicht des Artikel 5 Abs. 2 DSGVO, wonach der Verantwortliche die Rechtmäßigkeit der Verarbeitung nachweisen können muss. Da in der Verordnung die Art des zu führenden Nachweises nicht bestimmt ist, kommen neben der Verwahrung schriftlicher Einwilligungen und der Speicherung von in elektronischer Form wohl auch systematische Protokollierungen, Hinweise und Vermerke in Betracht.

BESONDERE KATEGORIEN PERSONENBEZOGENER DATEN

Soweit sich eine Einwilligung auch auf die Verarbeitung besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO beziehen soll, muss dies Einwilligung durch den Betroffenen ausdrücklich auch hierauf bezogen 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.

DAS ENDE DES FAMILIENFOTOALBUMS…!?

Auch wenn es in manchen Publikationen so klingen mag – die DSGVO steht dem Familienfotoalbum nicht im weg! Wenn die Verarbeitung personenbezogener Daten durch eine natürliche Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird, fällt die Verarbeitung gemäß Art. 2 Abs. 2 lit. c DSGVO unter das sog. »Haushaltsprivileg« und die Datenschutzgrundverordnung ist nicht anwendbar. Fotos aus dem Urlaub oder von Familienfeiern dürfen also auch zukünftig in das Fotoalbum geklebt werden – zur Freude oder zum Bedauern Ihrer darauf abgebildeten Kinder ;-)

PRIVATE HARDWARE IM UNTERNEHMEN - BYOD und Datenschutz

Die hohe Verbreitung von privaten Smartphones und Tablet-Computern in Unternehmen wie auch die von vielen Anwendern empfundene höhere Gebrauchstauglichkeit (Usability) der privaten Geräte haben in den vergangenen Jahren dazu geführt, dass die datenschutzrechtliche Abgrenzung der Daten bei der Verwendung privater Hardware am Arbeitsplatz stärker in den Fokus rutschte.

Der Wunsch, private Geräte auch für dienstliche Zwecke zu nutzen, dürfte auch in den kommenden Jahren weiter steigen. So erlaubten nach einer Studie des BITKOM-Verbandes bereits 2013 43 Prozent der ITK-Unternehmen ihren Mitarbeitern, private Endgeräte mit dem Unternehmensnetzwerk zu verbinden.

Anders als zu Beginn des Trends, als die vollständige Nutzung der privaten Endgeräte anstelle der betrieblichen Hardware im Fokus stand, stehen inzwischen, insbesondere durch die hohe Verbreitung von Messenger-Diensten wie WhatsApp als Teil der betrieblichen Kommunikationsstrategie, selektive Nutzungen privater Geräte immer mehr im Vordergrund.

BYOD ZWISCHEN DATENSCHUTZRECHT UND BETRIEBLICHER INFORMATIONSTECHNOLOGIE

Während viele Unternehmen beim Entwurf ihrer BYOD-Programme vorrangig nach technischen Strategien suchen, werden Datenschutzthemen, genauso wie arbeits-, steuer- und lizenzrechtliche Fragen mitunter ausgeblendet oder fließen erst zu einem späten Zeitpunkt in die Planungen mit ein.

Da jedoch die erfolgreiche Umsetzung der IT-Lösungen gerade auch Aspekte des Datenschutzes berühren, laufen BYOD-Lösungen ohne Begleitung durch den Datenschutz regelmäßig Gefahr gegen rechtliche Regelungen zu verstoßen.

TRENNUNG VON UNTERNEHMENSDATEN UND PRIVATEN DATEN

So erfordert die im Datenschutz geforderte Herrschaft über die verarbeiteten Daten einen unmittelbaren Zugriff auf den Datenbestand oder ein einzelnes Datum. Greifbar wird diese Notwendigkeit etwa mit Blick auf das Betroffenenrecht der wirksamen und endgültigen Datenlöschung aus Art. 17 DSGVO, das ohne den direkten Zugriff auf das Speichermedium, selbst bei vorhandener Bereitschaft des Device-Eigentümers, meist spätestens an dessen mangelnden IT-Kenntnissen scheitern wird.

Da dieser Zugriff auf die privaten Devices zudem ohne entsprechende Regelungen in den meisten Fällen rechtlich kaum zulässig sein wird, besteht hier in allen BYOD-Gestaltungen ein wichtiges Handlungs- und Gestaltungsfeld.

DATENTRANSFER UND ÜBERMITTLUNGEN IN DRITTSTAATEN

Als zusätzliches Risiko sind mögliche Datenübermittlungen privater Applikationen in Länder außerhalb der EU / des EWR (sog. »Drittsaaten«) im Rahmen der BYOD-Analysen zu berücksichtigen. Soweit diese Verarbeitungen als Auftragsverarbeitung durch den Anbieter der App erfolgen, treffen den Arbeitgeber als „Verantwortlichen" alle Pflichten aus Art. 28 DSGVO. Die in diesem Rahmen notwendigen vertraglichen Gestaltungen werden in der Praxis kaum umsetzbar sein und können in der Folge bei Nichtbeachtung zu Geldbußen von bis zu 10.000.000 EUR führen. Entsprechende Vorgaben für die Nutzung und Auswahl „zulässiger" Applikationen sollten damit in jeder BYOD-Strategie verankert werden.

TECHNISCHE UND ORGANISATORISCHE DATENSCHUTZMASSNAHMEN IM KONTEXT VON BYOD

Im Weiteren entsteht über die notwendigen Maßnahmen zur Datensicherheit hinaus, unter anderem durch den mobilen Charakter der BYO-Geräte, Handlungsbedarf bei der Gestaltung angemessener Maßnahmen zur Sicherheit der Verarbeitung. 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. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung lassen sich daher auf privaten Geräten meist nur begrenzt umsetzen und durchsetzen.

Auf technischer Ebene scheinen sich daher Virtualisierungslösungen mit Thin-Clients und die zentrale Administration über Mobile-Device-Management-Systeme derzeit noch anzubieten. Diesen Systemen stehen jedoch ein hoher Administrationsaufwand und die zum Teil erheblichen Lizenzkosten gegenüber.

FAZIT

Die berufliche Nutzung privater Devices stellt hohe 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 Risiken in der Kombination mit organisatorischen Vorgaben und verbindlichen Regelungen in der Praxis größtenteils beherrscht werden.

Im Ergebnis wird der Erfolg von BYOD-Lösungen von einem ausgewogenen Verhältnis zwischen dem 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.

IHRE ANSPRECHPARTNERIN:

EILEEN BINDER,
WIRTSCHAFTSJURISTIN

Mailverschlüsselung

Eine Gratwanderung zwischen Komfort und Sicherheit

Seit Inkrafttreten der DSGVO mehren sich die Anfragen zum Thema "verschlüsselte Kommunikation", denn die Sicherheit einer unverschlüsselten Mail kann mit einer Postkarte verglichen werden. Dieser gängige Vergleich ist für die meisten Mails, die innerhalb der Industriestaaten getauscht werden, allerdings falsch; um dies zu verdeutlichen, wollen wir den Weg einer Mail kurz betrachten.

Eine Mail wird vom Computer des Absenders in der Regel einem Mailprovider übergeben (z.B. GMX, T-Online, Office 365, 1&1, etc.). Die deutschen Provider fordern für dieses erste Teilstück schon seit einigen Jahren die sog. Transportverschlüsselung, d.h. die Mail wird kryptografisch "eingepackt", dann transportiert und auf dem Server des Mailproviders wieder ausgepackt. Sofern der Empfänger den gleichen Mailprovider benutzt, wird die Mail dann einfach in das Zielpostfach gespeichert und der Weg endet.
Sollten unterschiedliche Provider involviert sein, wird dieser Transport ebenfalls in der Regel verschlüsselt. Die meisten deutschen Anbieter haben sich in der Initiative "E-Mail Made in Germany" (EMIG) zusammengeschlossen und für diesen ersten Transportweg noch weitere gemeinsame Schutzmaßnahmen definiert.

Es bleibt also prinzipiell in diesem Szenario „nur" die Unsicherheit, dass die Poststation mitlesen kann, der Briefträger ist, zumindest für den überwiegenden Teil der Mails erstmal außen vor und damit ist die Sicherheit schon deutlich höher anzusiedeln als bei einer Postkarte – und das völlig transparent für den Anwender und ohne weiteren Aufwand.

Wenn wir das Restrisiko ausschließen wollen, oder Mails außerhalb des europäischen Raums transportieren wollen bzw. es sich um sehr kritische Daten handelt, gibt es, neben der Transportverschlüsselung auch die Inhaltsverschlüsselung. Zur Nutzung der Inhaltsverschlüsselung benötigt jeder der Teilnehmer ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüsselteil. Dabei kann der öffentliche Teil wörtlich auch so verstanden sein, diesen können Sie z.B. auf der Webseite abbilden oder auf einer Plakatwand drucken.

Der öffentliche und der private Schlüsselteil sind dabei über ein mathematisches Verfahren miteinander verbunden, können aber nur mit sehr großem Aufwand (im Bereich von einigen Jahren Rechenleistung aktueller Höchstleistungscomputer) "geknackt" werden.
Wenn Sie dann also eine inhaltsverschlüsselte Mail an einen Empfänger senden wollen, benötigen Sie den öffentlichen Schlüsselteil des Empfängers. Die Nachricht wird dann mit diesem Schlüssel verkryptet und es ist so sichergestellt, dass nur ein Empfänger, der im Besitz des richtigen privaten Schlüssels ist, die Nachricht entschlüsseln kann.

Umgekehrt funktioniert die digitale Signatur, hier wird die Nachricht mit Ihrem privaten Schlüssel "unterschrieben" (ebenfalls ein mathematisches Verfahren, dass, verkürzt, die Anzahl, Reihenfolge der Buchstaben der Mail zu einer Prüfsumme umwandelt und diese dann UNTER der Nachricht abbildet). Jeder, der Ihren öffentlichen Schlüssel kennt, kann damit die Authentizität der Mail prüfen. Eine Kombination existiert natürlich auch, hier kann dann eine sichere Kommunikation mit gesicherten Identitäten abgebildet werden.

Allerdings haben Sie aber sicherlich schon erkannt, worin die Probleme dieses Systems liegen: Sie benötigen selbst ein Schlüsselpaar und müssen dieses jedem möglichen Korrespondenzpartner im Vorfeld einer möglichen Kommunikation übermitteln. Dazu kommt, dass die Schlüssel in der Regel ein Ablaufdatum haben, d.h. bei bestehender Aufbewahrungsfrist müssen Sie auch Ihre eigenen Schlüssel und die der Korrespondenzpartner für viele Jahre aufbewahren. Für diese Problemstellungen gibt es technische Lösungen, die die recht hohe Komplexität abmildern, aber trotzdem sind weit <1% der weltweiten Mails aktuell verschlüsselt.

Alternativ zur zertifikatsbasierten Mailverschlüsselung gibt es Hybridverfahren, wie z.B. das auch in der Kanzlei reichert&reichert eingesetzte Verfahren Cryptshare. Mit diesem Verfahren tauschen Sie auf einem sicheren Weg (z.B. persönlich oder telefonisch) ein Kennwort aus, mit dem künftige Korrespondenz verschlüsselt wird. Die Übertragung der Nachricht erfolgt dann SSL-verschlüsselt; das ist der Sicherheitsstandard, der auch beim Online-Banking verwendet wird - für die sporadische, sichere Korrespondenz ist dies ein probates Mittel.

Aus technischer Sicht ist darauf zu hoffen, dass die großen Mailprovider den zertifikatsbasierten, inhaltsverschlüsselten Mailaustausch fördern; für kleinere Benutzergruppen ist sonst ein flächendeckender Einsatz kaum möglich.

Stefan Tröndle leitet ein Systemhaus in Singen mit 15 Mitarbeitern, die sich mit allen Aspekten von Kommunikation und Sicherheit beschäftigen.

Die Begeisterung für Verschlüsselung ist auch seinem ehrenamtlichen Engagement im Katastrophenschutz und der damit verbundenen Kommunikationswege geschuldet.

TRÖNDLE
systemhaus providing solutions

STEFAN TRÖNDLE,
BUSINESS PROCESS ARCHITECT, SYSTEMHAUS TRÖNDLE GMBH

TIPP!

Sie möchten den Querdenker weiterempfehlen?
Jetzt online nachlesen:
www.reichert-reichert.de

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

erschienen im Juni 2019/
Wiederauflage von 2015
Redaktion
Dr. Hansjörg Reichert, Matthias Herkert, Markus Spöhr, Gastbeitrag Stefan Tröndle

Layout & Fotografie
FRANK.COMMUNICATION.
www.frank-com.de