Compliance-Pflichten im Homeoffice

Der Trend zum Arbeitsplatz in den eigenen vier Wänden verstärkt sich und wird die Corona-Pandemie wahrscheinlich überdauern. Das Arbeiten im Homeoffice erfordert jedoch ein Umdenken, arbeits- und sozialrechtlich, datenschutzrechtlich, organisatorisch sowie aufsichtsrechtlich. Denn auch im Homeoffice sind sämtliche Compliance-Pflichten, von IDD über MiFID II bis zur Geldwäsche-Prävention und Datenschutz, zu erfüllen.

von Andreas Dolezal, Unternehmensberater & Compliance Experte

Sämtliche Gesetzesgrundlagen sowie die darin enthaltenen Compliance- und Wohlverhaltensregeln stellen auf das Ausüben der jeweiligen (Vertriebs-)Tätigkeiten ab. Wenn die Versicherungsvertriebsrichtlinie IDD von der „Ausübung des Versicherungsvertriebs" spricht, oder MiFID II von der „Erbringung von Wertpapierdienstleistungen", dann gelten die Bestimmungen ortsunabhängig – also auch im Homeoffice.

Vertraulichkeit von Kundeninformationen wahren

Schon beim Einrichten eines häuslichen Arbeitsplatzes sollte auf das Erfüllen der Compliance-Pflichten Rücksicht genommen werden. Auch im Homeoffice muss unter anderem die Vertraulichkeit von geschäftlichen Daten und Informationen gewährleistet sein. Dabei geht es nicht nur um personenbezogene Daten, die im Fokus der Datenschutz-Grundverordnung DSGVO stehen, sondern beispielsweise gemäß MiFID II auch um alle Daten und Informationen, die Finanzberatern im Zuge ihrer Beratungstätigkeit über Kunden bekannt sind.

Hilfreich beim Wahren der Vertraulichkeit ist das klare Abgrenzen von (privatem) Wohnbereich und (beruflichen) Arbeitsbereich. Im Idealfall haben Sie für das Homeoffice einen eigenen, separaten sowie versperrbaren Raum zur Verfügung. Besonders ratsam ist dies, wenn fallweise Kundenbesuche empfangen werden. Ein separates Arbeitszimmer macht nicht nur einen professionelleren Eindruck auf Ihre Besucher, es kann auch vorkommen, dass Sie einer Aufsichtsbehörde (Gewerbeaufsicht, FMA) Zugang zu Ihrem Gewerbestandort beziehungsweise Homeoffice gewähren müssen.

Das Trennen von Arbeits- und Wohnbereich trägt auch dazu bei, dass Sie abends besser entspannen können ohne permanent ans Büro erinnert zu werden und die Gedanken laufend um die Arbeit kreisen zu lassen. Nur wenn Sie abschalten und sich regenerieren können, sind Sie bei der Arbeit produktiv und konzentriert. Es geht also nicht nur um das räumliche Abgrenzen von Arbeits- und Wohnbereich, sondern ebenso um das mentale.

Mit einem separaten, versperrbaren Arbeitszimmer können Sie viel einfacher für die gebotene Sicherheit und Vertraulichkeit von geschäftlichen Informationen (darunter womöglich auch „sensible"

wie Gesundheitsdaten), Dokumenten und IT-Geräten sorgen. Diese müssen vor dem Zugriff durch unbefugte Personen geschützt werden. Bedenken Sie, dass zum Kreis der unbefugten Personen auch Lebenspartner, Kinder und Freunde zählen sowie Besucher, Reinigungskräfte, Handwerker usw.!

Oftmals steht ein eigenes Arbeitszimmer allerdings nicht zur Verfügung. Dann bleibt Ihnen nichts anders übrig als einen Kompromiss zu finden. Beispielsweise indem Sie sich Ihren Heimarbeitsplatz in

einem Zimmer einrichten, der tagsüber beziehungsweise während der Arbeitszeit nicht oder kaum genutzt wird, wie etwa ein Esszimmer oder ein Wirtschaftsraum. Wenn Sie auch so einen Raum nicht haben, dann bleibt Ihnen nur, sich jene Ecke im Haus oder der Wohnung zu suchen, in der es tagsüber am ruhigsten ist. Ich weiß, dass ist gerade mit Kindern im Home-Schooling, oder wenn auch der Lebenspartner im Homeoffice arbeitet und zwei Arbeitsplätze gebraucht werden, einfacher gesagt als getan.

Sorgen Sie jedenfalls dafür, dass sämtliche geschäftlichen Dokumente sowie beruflich genutzte IT-Geräte am Ende des Arbeitstages sicher verwahrt werden, zum Beispiel gut verschlossen in einem (Akten-)Schrank. Bleiben Dokumente und IT-Geräte ungeschützt und unbeobachtet am Arbeitsplatz liegen, können Sie keinesfalls die gebotene Vertraulichkeit und Sicherheit gewährleisten. Ganz abgesehen davon, dass von außen durch das Fenster oder die Terrassentür sichtbare Laptops, Smartphones usw. Diebe und Einbrecher anlocken.

Clean Desk Policy einhalten

Ebenso wie im Büro sollte im Homeoffice eine Clean Desk Policy gelten. Der Arbeitsplatz sollte stets aufgeräumt hinterlassen werden, zum Beispiel wenn Sie zu einem Termin müssen oder Ihren Arbeitstag beenden. Dies sorgt dafür, dass unbefugte Personen – und dazu zählen auch Lebenspartner, Besucher, Freunde, Kinder – keinen Zugang zu IT-Geräten (zum Beispiel USB-Speichersticks, externe Festplatten) erhalten und vertrauliche Dokumente und Informationen nicht einsehen können.

Bei kurzen Abwesenheiten während der Arbeitszeit kann es ausreichend sein, den Büroraum zu verschließen und den Bildschirm zu sperren. Bei geplanten Abwesenheiten, zum Beispiel Dienstreisen, Urlaub oder Aus- und Weiterbildungsveranstaltungen, soll der Arbeitsplatz so aufgeräumt werden, dass keine schutzbedürftigen Datenträger oder Dokumente unverschlossen am Arbeitsplatz zurückgelassen werden.

Keine berufliche Nutzung privater IT-Geräte

IT-Geräte wie Laptops und Smartphones, die in Ihrem Privateigentum stehen, sollten nicht für berufliche Zwecke genutzt werden. Unternehmen generell, aber insbesondere Finanzdienstdienstleister, sollten aus vielerlei Hinsicht auf diese „Misch-Verwendung“ verzichten.

Aus datenschutzrechtlicher Sicht werden dabei beruflich genutzte (personenbezogene und womöglich „sensible“) sowie private Daten vermischt. Es ist beinahe unmöglich, bei solch einem Durcheinander von Daten die gesetzlichen Vorschriften zum Datenschutz zu wahren. Selbst klare Regeln für das Nutzen von privaten Geräten können dieses Problem nicht endgültig lösen.

Als Unternehmer sind Sie für den Datenschutz und das Verarbeiten personenbezogener Daten verantwortlich, und haben die Sicherheit, Integrität und Vertraulichkeit von Daten und Informationen zu gewährleisten. Erlauben Sie Ihren Mitarbeitern (oder sich selbst) das berufliche Nutzen privater Endgeräte, mit denen in der Freizeit gestreamt, gesurft, gespielt, geshoppt usw. wird, dann verlieren Sie als letztverantwortlicher Unternehmer weitgehend die Kontrolle über das Einhalten und Befolgen von Maßnahmen zum Datenschutz, der IT-Sicherheit und der Vertraulichkeit.

Aufsichtsrechtlich kann die Vertraulichkeit von Kundeninformationen auf privaten Geräten insbesondere dann kaum gewahrt werden, wenn diese von mehreren Personen (Lebenspartner, Kinder usw.) beruflich oder privat genutzt werden. Bedenken Sie, dass Arbeitgeber nicht einfach auf private Endgeräte von Mitarbeitern zugreifen können. Im Zusammenhang mit den umfangreichen Pflichten zur Dokumentation, beispielsweise von Kundengesprächen, oder den Pflichten zum Aufzeichnen von elektronischer Kommunikation, kann das zum Problem werden. Befinden sich Gesprächsprotokolle und E-Mail-Verkehr auf einem privaten Endgerät, werden Sie es schwer haben, den Aufsichtsbehörden das Erfüllen der gesetzlichen Pflichten nachzuweisen und den Behörden gegebenenfalls Einblick zu gewähren. Ganz abgesehen davon, dass Sie sich – mangels Kontrollmöglichkeit – nicht sicher sein können, ob im Homeoffice auf privaten Endgeräten die (aufsichtsrechtlichen) Aufbewahrungs- und (datenschutzrechtlichen) Löschfristen tatsächlich befolgt werden.

Vielleicht benötigen Sie ausgerechnet dann, wenn ein Mitarbeiter längere Zeit (etwa wegen Dienstreise oder Urlaub) oder unvorhergesehen (wie bei Krankheit oder Unfall) abwesend ist, dringend Zugriff auf jene Daten und Informationen, die auf seinem beruflich genutzten, aber dennoch privaten Laptop gespeichert sind. Auch in solchen Ausnahmefällen kann der Zugriff auf Endgeräte, die im Eigentum des Mitarbeiters stehen, ungerechtfertigt sein und arbeitsrechtliche Konsequenzen nach sich ziehen.

Streitigkeiten darüber, wer für im Falle von Beschädigung oder Verlust eines privaten Endgerätes haftet beziehungsweise Ersatz leistet, gehen Sie ebenfalls aus dem Weg, wenn das berufliche Nutzen von privaten Geräten generell untersagt ist. Stellen Sie Ihren Mitarbeitern im Homeoffice lieber die erforderliche und geeignete Hardware zur Verfügung. Mit dem kommenden „Homeoffice-Paket“ der Bundesregierung wird dies wahrscheinlich ohnehin verpflichtend.

Genauso wie berufliche und private Daten müssen auch (personenbezogene) Daten aus verschiedenen Geschäftstätigkeiten voneinander getrennt werden. Verfügen Sie über mehrere Gewerbeberechtigungen, wie zum Beispiel Versicherungsvermittlung, Immobilientreuhänder oder Vermögensberatung (oder eine gänzlich finanzdienstleistungsferne Gewerbeberechtigung), dann trennen Sie die jeweiligen Datenbestände voneinander. Zumindest durch physisch getrennte Speichermedien und separate E-Mail-Accounts.

Jeden Benutzer eindeutig identifizieren

Das so genannte Berechtigungsmanagement legt fest, welcher Benutzer wor-

auf zugreifen darf und kann. Zur Unterscheidung des jeweiligen Benutzers (zum Beispiel Rollentrennung zwischen Backoffice-Mitarbeiter, Vertrieb und Systemadministrator) dient die eindeutige Identifizierung beim Anmelden. Damit ist automatisch klar, dass jeder Mitarbeiter seine persönlichen Anmelde- und Login-Daten geheim halten müssen beziehungsweise niemandem weitergeben darf.

Über individuelle Anmeldedaten erkennen IT-Systeme darüber hinaus, ob nur das Lesen von Informationen gestattet ist, oder auch das Ändern und Löschen. Unautorisierten Benutzern (oder IT-Komponenten) wird der Zugriff nicht gewährt. Damit wird unter anderem die gesetzliche Pflicht zur Datenminimierung erfüllt, denn jeder Benutzer darf nur auf jene (personenbezogenen) Daten zugreifen, die er oder sie zur Aufgabenerfüllung benötigt.

Berufliche Logins & Passwörter nicht privat nutzen

Alle Anwendungen und IT-Geräte benötigen sichere und separate Passwörter beziehungsweise Login-Daten. Passwörter und Login-Daten dürfen nicht doppelt oder mehrfach verwendet werden. Schon überhaupt nicht dürfen beruflich genutzte Passwörter und Login-Daten, also zum Beispiel die Kombination aus Benutzername oder Passwort und geschäftliche E-Mail-Adresse, privat verwendet werden.

Stellen Sie sich vor, Sie shoppen online, nutzen dazu jene Login-Daten, die Ihnen auch den Zugriff auf den zentralen Datenspeicher im Unternehmen erlauben, und dann wird der Online-Shop Opfer eines Hacker-Angriffes und die Login-Daten der Nutzer werden gestohlen. Sowohl Mitarbeiter als auch Chefs als Verantwortliche im Sinne des Datenschutzes können in so einem Fall wirklich große Problem bekommen. Beruf und privat müssen auch in diesem Zusammenhang strikt getrennt werden.

IT-Geräte und Daten sicher transportieren

Sicherlich werden Sie ab und zu zwischen Homeoffice und Unternehmensstandort pendeln. Auch zu Kundenterminen oder Treffen mit Geschäftspartnern nehmen Sie Smartphone und gegebenenfalls Laptop, USB-Speichersticks, Dokumente und Verträge usw. mit. Seien Sie achtsam beim Transport, tagtäglich gehen hunderte USB-Speichersticks, Smartphones usw. verloren oder werden gestohlen.

Auf mobilen Speicherträgern dürfen beim Transport nur Kopien von Daten sein, niemals die Originaldateien. Daten auf mobilen Datenspeichern müssen verschlüsselt sein. Berücksichtigen Sie diese beiden Punkte, dann bleiben die unangenehmen Folgen eines gestohlenen USB-Speicherstick oder externen Festplatte im Regelfall überschaubar.

Denken Sie daran, dass es sich bei Papierdokumenten wie Verträgen oft um Unikate mit Originalunterschriften handelt. Solche Dokumente mit allen Unterschriften erneut zu organisieren, kann zeitintensiv sein (und Sie werden peinlicher Weise beichten müssen, warum Kunde oder Geschäftspartner erneut unterschreiben müssen).

Daten sicher übertragen

Daten, die über unsichere Datenverbindungen oder unverschlüsselt übertragen werden, sind für Kriminelle so einfach zu lesen wie die Rückseite eine Postkarte. Um das Abhören oder Manipulieren von Daten während der Übertragung zu verhindern und deren Vertraulichkeit zu wahren, sollte zumindest das Verschlüsselungsprotokoll SSL/TLS verwendet werden. Mit SSL/TLS werden übertragene Daten verschlüsselt und sind für Außenstehende nicht lesbar. Können Sie E-Mails via Tablet oder Smartphone empfangen und senden, dann denken Sie beim Aktivieren des SSL/TLS-Zertifikates auch an diese Geräte.

Für Internetseiten ist mittlerweile das HTTPS-Protokoll Stand der Technik. Internetseiten, die dieses Protokoll noch nicht verwenden, werden von vielen aktuellen Internet-Browsern bereits blockiert beziehungsweise warnt der Browser vor dem Aufrufen der Seite. Suchmaschinen ignorieren Internetseiten ohne HTTPS oder reihen Sie in den Suchergebnissen an die hintersten Plätze.

Virtual Private Network-Verbindungen, kurz VPN, sind eine weitere Möglichkeit, um Daten sicher zu übertragen. VPNs schützen übertragene Daten mithilfe kryptografischer Verfahren und können die Risiken öffentlicher WLAN-Hotspots reduzieren. VPN-Clients, VPN-Server und VPN-Verbindungen sollten ausschließlich von IT-Experten installiert und konfiguriert werden, also von den Kollegen aus der IT-Abteilung oder einem externen Dienstleister.

Sicherungskopien erstellen

Eine der wesentlichsten und wichtigsten Maßnahmen zum Schutz von Daten ist das regelmäßige Erstellen von Sicherungskopien. Gehen Daten verloren, zum Beispiel durch defekte Hardware oder Schadprogramme, können gravierende Schäden entstehen. In un-

serer vernetzten und hochtechnisierten Geschäftswelt kann es sogar Existenz bedrohende Folgen haben, wenn Sie vernichtete, irrtümlich gelöschte oder böswillig gestohlene Daten nicht wiederherstellen können.

Datensicherungen sollen gewährleisten, dass Geschäftsprozesse sowie der IT-Betrieb zeitnahe wiederaufgenommen werden können. Datensicherungen müssen regelmäßig durchgeführt werden. Die erstellten Backup-Datenträger müssen sicher sowie geschützt vor dem Zugriff unbefugter Dritter aufbewahrt werden. Um die Vertraulichkeit der gesicherten Daten zu gewährleisten, sollten alle gespeicherten Daten verschlüsselt sein.

Die beste Datensicherung ist vollkommen nutzlos, wenn sich die gesicherten Daten im Fall der Fälle nicht wieder in die IT-Systeme und Endgeräte einspielen lassen. Sie sichern Ihre Daten ja nicht der Datensicherung willen, sondern um die Daten nach einem Verlust wiederherstellen zu können. Also testen Sie das Wiederherstellen der gesicherten Daten ab und zu, um zu prüfen, ob sich die Daten wie gewünscht und problemlos zurückspielen lassen.

Mitarbeiter sensibilisieren und schulen

Datenschutz und IT-Sicherheit können nur dann erfolgreich und effizient umgesetzt werden, wenn alle Mitarbeiter – interne und externe, angestellte und selbständige, im Büro und im Homeoffice – für relevante Gefährdungen sensibilisiert werden. Wesentlich ist es, allen Mitarbeitern die Abhängigkeit von Daten und Informationen aufzuzeigen. Denn der „Faktor Mensch“ ist einer der größten Risikofaktoren im Zusammenhang mit Datenschutz und IT-Sicherheit.