Datenschutz

afm Verhaltensregeln im Rahmen der afm Datenschutzrichtlinie

Stand 05-2022

In Ergänzung zur afm Datenschutzrichtlinie vom 25.05.2018 gelten die folgenden afm Verhaltensregeln und sind unbedingt einzuhalten.

Bei technischen Rückfragen wenden Sie sich bitte an die IT-Abteilung.

Inhalt

1. Social Engineering

a. Halten Sie firmenintern vorgegebene Richtlinien immer ein, auch in Stresssituationen!

b. Ein kritischer Umgang mit Anfragen via Telefon oder E-Mail ist sehr wichtig. Behandeln Sie geschäftskritische Informationen, Zugangsdaten und vertrauliche Daten von Mitarbeitern, Kunden und Lieferanten stets mit höchster Sorgfalt und seien Sie vorsichtig bei Ihnen unbekannten Personen.

c. Lassen Sie sich zu nichts überreden. Fallen Sie nicht auf Komplimente, übertriebene Höflichkeit oder Drohungen herein und geben Sie keine internen oder vertraulichen Informationen an unbekannte Personen und unberechtigte Dritte weiter.

d. Führen Sie vertrauliche Telefonate oder Gespräche nicht in der Öffentlichkeit bzw. seien Sie vorsichtig bei der Weitergabe von Informationen in persönlichen Gesprächen an öffentlichen Orten bzw. in sozialen Netzwerken.

2. Passwörter

a. Verwenden Sie zur Absicherung Ihrer Daten nur komplexe Passwörter, die aus Buchstaben, Ziffern und Sonderzeichen bestehen. Je mehr Zeichen Ihr Passwort hat, desto sicherer ist es.

b. Ändern Sie Ihr Passwort regelmäßig (z. B. alle 3 Monate) und auf jeden Fall auch dann, wenn Sie glauben, dass das Passwort ausgespäht wurde.

c. Geben Sie Ihr Passwort niemals an Dritte, insbesondere fremde Personen heraus – insbesondere nicht via E-Mail oder Telefon.

d. Behalten Sie Ihre Passwörter am besten im Kopf. Benötigen Sie dennoch eine Gedächtnisstütze, achten Sie auf ausreichende Sicherheit oder nutzen Sie einen Passwortsafe. Verstecken Sie sie nicht an allgemein bekannten Plätzen (z. B. unter der Tastatur oder unter der Schreibtischunterlage) oder unverschlüsselt auf Ihr Smartphone oder Ihren PC!

e. Achten Sie bei der Passworteingabe darauf, dass niemand Sie beobachtet. Warten Sie mit der Passworteingabe, bis Sie unbeobachtet sind.

f. Verwenden Sie für jede Anwendung ein anderes Passwort – kein Masterpasswort.

g. Mitarbeiter tauschen untereinander in KEINEM FALL Passwörter zur Vertretung aus. Sollte in Abwesenheit ein Zugang zum Benutzer-Account eines anderen Benutzers erfolgen, sollte dies idealerweise durch Übernahme der Rechte durch einen anderen Account erfolgen.

Jeder Mitarbeiter ist dafür verantwortlich, was unter seinem Account geschieht

Ein sicheres Passwort

- hat eine angemessene Länge von mindestens 8 Stellen, besser 10 bis 15 Zeichen – je mehr Zeichen desto besser,
- enthält sowohl Buchstaben (keine Umlaute) als auch Ziffern (0–9),
- enthält Groß- und Kleinbuchstaben und Sonderzeichen (z. B. #,$),
- enthält keine personenbezogenen Daten (z. B. Name des Haustiers),
- ist in keinem deutschen oder Fremdwörterbuch enthalten,
- wird in regelmäßigen Abständen (z. B. alle 3 Monate) geändert. Verwenden Sie bei der Erstellung neuer Passwörter keine bereits einmal genutzten Passwörter.

Methoden für sichere Passwörter

- *Akronymmethode*: Denken Sie sich einen Satz aus und benutzten Sie von jedem Wort nur den Buchstaben (oder nur den 2., den letzten etc.). Anschließend werden bestimmte Buchstaben in Zahlen oder Sonderzeichen verwandelt. Beispiel: I want to be called the Number 1> Iwtbct#1
- *Mehrwortmethode*: Überlegen Sie sich mindestens zwei Wörter und verbinden Sie die ersten Buchstaben jedes Wortes miteinander ohne ein Leerzeichen dazwischen.
  Beispiel: HerrMüllerundFrauSchneider > HMue#FSc

3. Virenschutz und Virenprüfung

a. Handeln Sie hier gemäß dem Motto: Vorbeugen ist der beste Schutz. Häufige Anzeichen für einen Virenbefall sind ungewöhnliche Fehlermeldungen, verzerrte Menüs und Dialogfelder, Anwendungen funktionieren nicht korrekt, Ihr PC reagiert häufig nicht oder läuft langsamer als normal. Im Falle einer Infizierung schalten Sie Ihren PC ab und informieren Sie die „IT-Sicherheit“ bzw. Ihren Vorgesetzten sowie weitere möglicherweise betroffene Mitarbeiter.

b. Sichern Sie Ihre Daten regelmäßig auf ein Drittmedium (z. B. externe Festplatte, USB-Stick). Dies gilt nicht für Mitarbeiter aus dem KWK, die über das zentrale System arbeiten und auch nicht für Daten, welche über den TerminalServer erfasst bzw. bearbeitet werden. Hier ist eine regelmäßige Datensicherung sichergestellt.

c. Aktualisieren Sie alle eingesetzten Software-Produkte unverzüglich nach Erscheinen der Patches bzw. nutzen Sie die automatische Update-Funktion Ihrer Software. Berichte in einschlägigen Newslettern zeigen, dass veröffentlichte Sicherheitslücken schon kurz nach Bekanntwerden ausgenützt werden.

d. Prüfen Sie Ihren PC regelmäßig, mindestens einmal in der Woche, abhängig von Ihrem Verhalten auch öfters, auf Viren. Dies betrifft hauptsächlich Arbeitsplätze außerhalb des KWK.

e. Nutzen Sie nur auf Viren geprüfte Datenträger. Lassen Sie die Datenträger, die Sie von anderen erhalten, vor Verwendung von der IT-Abteilung auf Viren prüfen.

f. Verwenden Sie nur Software aus vertrauenswürdigen Quellen.

g. Im Notfall: Im Falle einer Infizierung nehmen Sie Ihren PC vom Netz (ziehen des Stromsteckers) und informieren Sie die IT-Abteilung bzw. Ihren Abteilungsleiter sowie weitere möglicherweise betroffene Mitarbeiter.

4. E-Mail Sicherheit

a. Senden Sie sensible Kundendaten ausschließlich über den TerminalServer mit der jeweiligen afm-gruppe Domain. Der E-Mail-Versand über den TerminalServer erfolgt grundsätzlich mit einer TLS Verschlüsselung, die von einem überwiegenden Anteil auch privater Accounts bestätigt wird.

b. Signieren Sie Ihre E-Mails, damit der Empfänger sicher sein kann, dass die E-Mail tatsächlich von Ihnen kommt.

c. Antworten Sie nie auf Spam-Mails, öffnen Sie in der E-Mail enthaltene Links oder Anhänge nicht und löschen Sie die E-Mail umgehend.

d. Nutzen Sie Firmen-E-Mail-Adressen ausschließlich gemäß §1 der afm Nutzungsvereinbarung Kommunikationsmittel.

e. Gehen Sie mit Downloads von Programmen, Bildschirmschonern und Daten-Dateien aus dem Internet sorgsam um. Sie können Trojaner oder Viren enthalten.

5. Elektronische Unterschrift

Beim Einsatz von mobilen Endgeräten (z. B. Tablets) im Antragsprozess sind bezüglich der Vermeidung von Rechtsrisiken die folgenden Punkte unbedingt einzuhalten:

a. Eine elektronische Unterschrift mit einem entsprechenden Schreibgerät auf dem Tablet auf einem PDF Antrag im Unterschriftsfeld ist in der Regel wirksam. Von einem Kopieren der Unterschrift und Übertragung auf andere Antragsdokumente ist jedoch in jedem Fall abzusehen!

b. In einem potentiellen Rechtsstreit (z. B. mit Risikoangaben verbundene Obliegenheitsverletzung) ist der rechtswirksame Beweis, dass die Unterschrift durch den Unterschreibenden geleistet wurde nicht möglich. Holen Sie daher in jedem Fall eine separate nichtdigitale Bestätigung über die entsprechende Unterschriftsleistung ein. Dies gilt insbesondere für Antragsunterschriften von Versicherungen, die rechtspersönliche Erklärungen des VN wie Gesundheitsfragen und sonstige Risikoangaben im Leben – und Krankenversicherungsgeschäft beinhalten.

c. Lassen Sie im Falle der Antragsstrecke mit mobilen Endgeräten auch die afm Datenschutzerklärung zur Wirksamkeit mit einer physischen Unterschrift gegenzeichnen oder vollziehen Sie dies im Zusammenhang mit dem Maklerauftrag. Hinterlegen Sie anschließend dieses gegengezeichnete Dokument, ebenso wie die Erklärung zur elektronischen Unterschrift, im Kundenverwaltungsprogramm (Dokumente Kunde/Vertrag).

6. Mobilgeräte und Datenträger

a. Speichern Sie keine vertraulichen Daten unverschlüsselt auf Ihrem IT-Gerät. Bei Verlust des Gerätes kann somit nur ein materieller Schaden entstehen.

b. Sichern Sie Ihre lokalen Daten außerhalb der Terminal-Server Lösungen/Systeme regelmäßig auf einen Backup-Medium (Netzlaufwerk, weiterer Datenträger), mindestens jedoch wöchentlich, um Datenverlust zu vermeiden. Die Sicherungsdatenträger sind physisch getrennt und vor dem Zugriff Unberechtigter gesichert aufzubewahren.

c. Schützen Sie Ihre mobilen IT-Geräte vor Zugriff von Dritten. Sperren Sie Ihr Gerät mittels eines Passwortes oder PIN-Codes und sperren Sie den Bildschirm bei Inaktivität.

d. Lassen Sie nur kontrollierte Datenübertragungen zu. Schalten Sie insbesondere die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur dann ein, wenn Sie diese bewusst zur Kommunikation mit bekannten Geräten und Netzen nutzen.

e. Sorgen Sie bei Außerbetriebnahme bzw. Vernichtung eines Mobilgerätes oder Datenträgers dafür, dass alle darauf gespeicherten Daten sicher gelöscht bzw. unbrauchbar sind.

f. Spielen Sie vom Hersteller bereitgestellte Updates unverzüglich ein. Stellen Sie nicht mehr unterstützte Software zeitnah auf einen aktuellen Stand um.

7. Datenverluste

a. Leeren Sie Ihren Papierkorb auf dem PC nicht automatisch, sondern prüfen Sie in regelmäßigen Abständen, ob sich möglicherweise wichtige Daten darin befinden, die Sie aus Versehen gelöscht haben.

b. Speichern Sie Dateien unter einem anderen Dokumentnamen (z. B. mit Versionsnummer), wenn Sie frühere Versionen behalten möchten.

c. Fahren Sie Ihren Computer immer ordnungsgemäß herunter. Ansonsten können Dateien, die gerade bearbeitet wurden, verloren gehen.

d. Speichern Sie betriebliche Daten regelmäßig auf einem Netzlaufwerk oder sichern Sie die Daten auf einem verschlüsselten externen Datenträger. Testen Sie Ihr Backup auch regelmäßig auf dessen Funktionsfähigkeit. Dies gilt nicht für Mitarbeiter aus dem KWK, die über das zentrale System arbeiten und auch nicht für Daten, welche über den TerminalServer erfasst bzw. bearbeitet werden. Hier ist eine regelmäßige Datensicherung sichergestellt.

e. Beschriften Sie Ihre Datenträger sorgfältig nach einem einheitlichen System und schützen Sie diese vor Diebstahl.

8. Empfang von Besuch

Frechheit siegt! Das ist die einfachste Möglichkeit, um an sensible Daten im Unternehmen zu gelangen. Lassen Sie sich deswegen davon nicht davon abhalten - egal mit welchem Auftreten - nicht bekannte oder berechtigte Personen von datenschutzkritischer Infrastruktur fernzuhalten.

Grundsätzlich hat jeder (Handwerker, Dienstleister, Vertreter, außer bei Durchsuchungsbefehlen von Behörden) vor Betreten der Büroräume (außer Kundenbesuch Besprechungszimmer) sich auszuweisen und die Datenschutzbestimmungen zu unterzeichnen. Das hebt auch die Seriosität im Umgang mit dem Datenschutz.

Bitte prüfen:

a. Vor Betreten eines Büroraumes in Empfang nehmen, idealerweise an der Tür
b. Ist der Besuch angekündigt?
c. Wer ist Ansprechpartner im Haus?
d. Sind beim Ansprechpartner alle Akten verdeckt/aufgeräumt, ist der Bildschirmschoner aktiviert?
e. Telefon am entsprechenden Arbeitsplatz umgeleitet?
f. Benötigt der Kunde WLAN?
g. Ist der Kunde außerhalb des Besprechungsraumes immer in Begleitung?

9. Geltungsbereich

Diese Regeln gelten für die Mitarbeiter der Unternehmen der afm Gruppe sowie den angeschlossenen Handelsvertretern und deren Mitarbeiter.

10. Geltungsdauer

Die Verhaltensregeln im Rahmen der afm Datenschutzrichtlinie treten mit dem 25.05.2018 in Kraft. Sie gelten, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird.