IT-Nutzungs- und Sicherheitsrichtlinie

Der ND Versicherungsmakler GmbH

Verantwortliche Stelle:

ND Versicherungsmakler GmbH
Schwedenstraße 11
96317 Kronach
info@ndversicherungsmakler.de

Management / Geschäftsführung:

Lucas Bernreuther (Geschäftsführer)
Christian Neubauer (Inhaber)

Datenschutzbeauftragter

Lucas Bernreuther
Schwedenstraße 11
96317 Kronach
Tel.: 09261—10150
Lucas.bernreuther@ndversicherungsmakler.de

IT-/Systemadministrator

Mann-IT GmbH
Fasanenstraße 12
96114 Hirschhaid
info@mann-it.de

Vorwort

Für die ND Versicherungsmakler GmbH hat der sichere Umgang mit den personenbezogenen Daten seiner Kunde, Mitarbeiter und Dienstleistern strategische Bedeutung.
Als Mitarbeiter tragen Sie dazu wesentlich bei, dieses Ziel einzuhalten. Im Folgenden werden die internen Richtlinien zur Sicherheit in der Verarbeitung personenbezogener Daten definiert.
Die Mitarbeiter verpflichten sich in einer Zusatzerklärung zum Mitarbeitervertrag auf die Einhaltung des Datenschutzes im Betrieb.

1. Allgemeines

Die IT-Einrichtungen der ND Versicherungsmakler GmbH sind ausschließlich zur betrieblichen Nutzung für den im Mitarbeitervertrag geregelten Zweck vorgesehen. Dem Mitarbeiter werden die Arbeitsmittel vollständig vorkonfiguriert zur Erfüllung der jeweiligen Aufgaben zur Verfügung gestellt.
Es ist kein weiteres eigenmächtiges Eingreifen in die Konfiguration gestattet.
Die betriebliche IT steht in der Regel werktags von 9 bis 17 Uhr zur Verfügung.

Außerhalb dieser Zeiten können jederzeit Wartungsarbeiten und Systemneustarts durchgeführt werden.
Der Mitarbeiter hat pflichtbewusst, umfangreich und wahrheitsgemäß mit der IT-Abteilung zu kooperieren und kommunizieren.
Für Vorsatz, grobe Fahrlässigkeit oder Begehen einer Straftat haftet der Mitarbeiter persönlich.

2. IT-Nutzung

Private Nutzung betrieblicher IT

Dem Mitarbeiter ist es untersagt, die zur Verfügung gestellte betriebliche IT in jeglicher Form privat zu nutzen.

Dies betrifft insb.
- das Laden, Speichern und Bearbeiten privater Dokumente
- die Benutzung privater Datenträger
- die private Benutzung von Browsern oder sonstiger Internetfähiger Software zum Abruf von Information, Daten oder Apps
- Versand und Empfang von privaten Nachrichten, Bildern oder Videos per eMail, Chat, Messanger oder sonstiger Kommunikationssoftware

Zudem ist es dem Mitarbeiter nicht gestattet
- eigenmächtige Änderungen an Hard- oder Software oder Konfiguration vorzunehmen
- Programme, Apps oder sonstige Software selbstständig zu installieren
- die IT zu einem anderen als dem betrieblichen Zweck zur Erfüllung seiner Aufgabe zu nutzen
- private Lieferungen an die Geschäftsadresse zu veranlassen
- Sicherheitseinrichtungen zu umgehen
- Private Geräte zum Laden an die USB-Anschlüsse der betrieblichen IT anzuschließen

Die Mustermakler GmbH behält sich stichprobenartige oder bei Verdacht auf Missbrauch weitergehende Kontrollen vor.

Ebenso ist es dem Mitarbeiter untersagt, private IT im Firmennetzwerk zu nutzen.
Die Foto-Funktion von privater IT ist bei Betreten der Betriebsräume zu deaktivieren.
Fotoaufnahmen in den Betriebsräumen sind grundsätzlich vom Vorgesetzten zu genehmigen.

Behandlung & Pflege

Die zur Verfügung gestellte IT ist sorgsam zu behandeln und regelmäßig mit den vorgegebenen Hilfsmitteln zu reinigen (Bildschirm, Tastatur, Maus).
Eine weitergehende Wartung wird ausschließlich durch Mitarbeiter der IT-Abteilung durchgeführt.
Defekte sind umgehend der IT-Abteilung zu melden. Außer Sichtprüfungen (bspw. Kabel entfernt) hat der Mitarbeiter keine eigenständigen Reparaturversuche zu unternehmen.

Weitergehender Umgang mit Störungen werden gesondert in den Notfallplänen geregelt.

Mobile Devices

Mitarbeiter, denen mobile Geräte (bspw. Notebooks, Smartphones) zur Verfügung gestellt bekommen, beachten folgende Grundsätze:
- keine eigenmächtige Installation von Software oder Apps
- Passwortschutz bei Nichtbenutzung
- sichere Aufbewahrung
- fremde Netzwerke nur mit aktivierter VPN-Verbindung nutzen
- umgehende Meldung bei Verlust oder Beschädigung
- keine dauerhafte lokale Speicherung betrieblicher Daten
- die Geräte sind sorgsam zu behandeln und vor Beschädigung zu schützen
- vor Zugriff oder Zugang für Dritte (bspw. Sicht auf Bildschirm an öfftl. Plätzen, Mithören von Telefonaten) ist zu das Device zu schützen
- die Verschlüsselung der Datenträger ist zu aktivieren

Drucker

Ausdrucke sind entweder per PIN abzusichern oder umgehend am Drucker abzuholen.
Insb. bei Druck von Personalunterlagen ist besondere Sorgfältigkeit geboten.
Fehldrucke sind direkt am Drucker im Aktenvernichter zu entsorgen.

Bitte nutzen Sie Ausdrucke nur, wenn eine Bearbeitung am Bildschirm ausgeschlossen ist.

Dateien

Alle personenbezogenen Dateien sind beim Kunden im Maklerverwaltungsprogramm abzulegen.
Sollte dies nicht möglich sein, sind die dafür vorgesehenen Netzwerklaufwerke zu nutzen.
Andere betriebliche Dateien sind grundsätzlich in den vorgesehenen Ordnern der Netzwerklaufwerke zu sichern.
In Bearbeitung befindliche Dateien können temporär im persönlichen Ordner des Netzwerklaufwerks gesichert werden.
Eine lokale Speicherung ist nur in einzelnen Ausnahmefällen (Serverausfall, nur lesender Zugriff bis zur unmittelbaren Löschung) erlaubt.

Telefon

Keine Auskunft zu personenbezogenen Daten bei nicht authentifizierten Anrufen (Ein-/Ausgehend), ggf. Verweis auf schriftlichen Versand der Auskunft.
Die private Nutzung ist in geregeltem Umfang erlaubt.
Es ist untersagt, kostenpflichtige Angebote zu nutzen. Bei betrieblicher Notwendigkeit Vorgesetzten informieren.

Nutzung von eMail

Die private Nutzung der betrieblichen eMail-Adresse und -Programme ist untersagt.

Der Empfänger der eMail ist vor dem Versand nochmals als Berechtigter zum Erhalt der enthaltenen Information zu prüfen.
Grundsätzlich ist der gesamte eMail-Verkehr aus dem Maklerverwaltungsprogramm zu führen.
Bei Selektion eines Empfängers aus einer Auswahl-Liste von Vorschlägen (bspw. „AN:“-Feld in Outlook) ist besondere Kontrolle vor Versand auszuüben.
Die Felder CC: und BCC: müssen korrekt verwendet werden.
Vor dem Versand an mehrere Empfänger ist zu prüfen, ob diese notwendigerweise die Information erhalten müssen.

Attachments

Unbekannte oder unerwünschte eMails mit Anhängen sind in keinem Fall zu öffnen und umgehend ungelesen zu löschen.
Unbedenkliche Attachments sind DOCX, XLSX, PPTX, PDF, PNG.
Alle anderen Anhänge sind vom Mitarbeiter nicht zu öffnen. Bei Bedarf ist die IT-Abteliung zu informieren.

SPAM

Es wird ein vorgegebener SPAM-Filter zur Aussortierung betrieblich unerwünschtem eMail-Verkehr genutzt.
Der Mitarbeiter hat keinen Anspruch auf Zustellung einer bestimmten eMail.
Es tritt in Einzelfällen auch das Löschen erwünschter eMails auf. Bei Verdacht nimmt der Mitarbeiter Kontakt mit dem IT-Administrator auf.
Besondere Vorsicht ist bei unbekannten Absendern mit Links in der eMail zu wahren. In keinem Fall darf der Link angeklickt werden.

Passwörter

Die Vergabe von Passwörtern stellt den Zugangsschutz zu personenbezogenen Daten dar.
Passwörter sind vom Mitarbeiter gegenüber allen anderen Personen (auch IT-Administration, Geschäftsleitung, Datenschutzbeauftragter) geheim zu halten und nicht schriftlich zu notieren.
Für Mitarbeiter, die umfangreiche Passwörter verwalten müssen, wird ein Passwort-Safe zur Verfügung gestellt.
Die Passwortrichtlinien sind einzuhalten.
Arbeiten mit Administrationsrechten werden ausschließlich von befugten Personen oder der IT-Abteilung ausgeführt.
Bei Verlust eines Passwortes wird die IT-Abteilung informiert (s. Notfallpläne).
Für unterschiedliche Anwendungen sind unterschiedliche Passwörter zu verwenden.

3. Betriebliche Organisation und IT-Sicherheit

Der beste Schutz vor Sicherheitsverletzungen sind geschulte Mitarbeiter.
Die ND Versicherungsmakler GmbH legt Wert auf umfangreiche Qualifizierung und Weiterbildung.

Folgende Richtlinien dienen dem Mitarbeiter zur Einhaltung des Sicherheitsniveaus.
Zur Unterstützung der Mitarbeiter bei der Einhaltung der Sicherheitsrichtlinien stellt der Betrieb technische und organisatorische Maßnahmen zur Verfügung.

Clean-Desk-Policy

Auf dem Schreibtisch und dem virtuellen Desktop befinden sich grundsätzlich nur Akten und Dateien, die zur Bearbeitung des aktuellen Sachverhaltes dienen. Nach Abschluss werden diese wieder eingeordnet.
Bei Verlassen des Arbeitsplatzes oder Betreten des Raumes betriebsfremder Personen sind alle offenen Akten zu schließen und der Bildschirm vor Einsicht zu schützen.
Es erfolgen keine schriftlichen Notizen (Post-IT, Schreibunterlage, usw.) außerhalb des Maklerverwaltungsprogrammes.

Verlassen des Arbeitsplatzes

Bei Arbeitsende ist der PC herunterzufahren, Schreibtisch von offenliegenden Akten zu befreien, Fenster und Türen zu schließen.
Der Arbeitsplatz muss sicher vor Einsicht oder Zugang Dritter zu personenbezogenen Daten gesichert sein.

Virenschutz

Es wird ein mehrstufiger Virenschutz zur Verfügung gestellt.
Unbekannte Dateien oder Dateien von unbekannten Empfängern sind nicht zu öffnen.
Betrieblich nicht zugelassene mobile Datenträger (CD/DVD, USB-Stick, externe Festplatten, Speicherkarten) dürfen vom Mitarbeiter nicht an die IT-Systeme angeschlossen werden. Bei Bedarf wird die IT-Abteilung informiert.
Besteht der Verdacht auf Virenbefall sind umgehend alle Arbeiten einzustellen und die IT-Abteilung oder der Vorgesetzte zu informieren. Selbstreparaturversuche sind zu unterlassen.

Besuch

Besucher der Betriebsräume werden in die ausgewiesenen Besucherzonen geleitet.
Ein Zutritt zu den Büroräumen ist nur in Begleitung eines Mitarbeiters gestattet.
Telefonate und Akten sind vor Besuchern geheim zu halten.
Besucher erhalten keinen Zugang zu internen IT-Systemen.
Bei Bedarf steht ein Gäste-WLAN zur Verfügung.

HomeOffice

Mitarbeiter können bei Bedarf und in Absprache nach den Regelungen im Mitarbeitervertrag im HomeOffice arbeiten.
Das Schutzniveau der betrieblichen Anforderung ist dabei in keinem Fall zu unterschreiten.
Mitgenommene Akten sind vor dem Zugriff und Zugang Dritter geheim zu halten.
Es erfolgt keine lokale Speicherung betrieblicher Daten auf privater IT.
Der Zugang zum Firmennetzwerk erfolgt ausschließlich per VPN-Verbindung.

Sicherheitsvorkehrungen

Jegliche Umgehung betrieblicher Sicherheitsmaßnahmen ist dem Mitarbeiter untersagt.
Hierzu zählen unter anderem:
- deaktivieren von Passwortschutz
- Umgehung der betrieblichen Internetverbidung (Proxy-Server)
- deaktivieren von Virenschutz, Firewall und Sicherheitssoftware
- eigenmächtige Inbetriebnahme externer Datenträger
- Ausführen nicht betrieblich genehmigter Software und Apps
- Maßnahmen, die zur Verschlechterung des Datenschutzniveaus führen

Fernwartung

Dem Mitarbeiter ist bewusst, dass die IT-Abteilung die Möglichkeit zur Fernwartung für Support und Administrationszwecke erhält.
Der Zugriff erfolgt immer in Absprache mit dem Mitarbeiter.

Akten

Papierdokumente sind in der jeweiligen Ablage einzuordnen.
Akten mit besonderem Schutzbedürfnis (Mitarbeiter-/Personalakten) sind gesondert unter Verschluss aufzubewahren.
Bei Verwendung außerhalb der Betriebsräume ist besondere Vorsicht auf Verlust und Einsichtmöglichkeit durch Dritte zu wahren.
Nicht mehr benötigte Akten sind ordnungsgemäß zu entsorgen oder einem speziellen Dienstleister zur Vernichtung zu übergeben.

Private Nutzung

Zur privaten Nutzung in Pausenzeiten stellt der Betrieb geeignete Hardware (bspw. Tablet) zur Verfügung. Dies ist zur Nutzung von browserfähiger Software geeignet (Web-Mail, Surfen, ...).
Die Mitarbeiter nutzen die Hardware sorgfältig. Es werden keine persönlichen Daten auf dem Gerät gespeichert. Nach Benutzung meldet sich der Mitarbeiter von allen genutzten Diensten ab und schließt alle offenen Browser-Fenster.
Die Mustermakler GmbH behält sich das Recht vor, die Nutzung jederzeit ohne Angabe von Gründen zu beenden.
Es besteht kein Anspruch auf Nutzung durch die Mitarbeiter.

Ahndung von Verstößen

Bei grober Fahrlässigkeit oder vorsätzlicher Verletzung dieser Sicherheitsrichtlinien behält sich der Arbeitgeber das Recht auf disziplinare Maßnahmen gegenüber dem Mitarbeiter vor.

Zutritt / Zugang zu Serverräumen

Zutritt zu den Serverräumen haben nur berechtigte Personen.
Die Serverräume sind ausschließlich zur Verwahrung von IT-Komponenten gedacht.
Die Serverräume werden mit einem gesonderten Alarmsystem gesichert. Bei Videoüberwachung ist eine entsprechende Kennzeichnung anzubringen.
Der Serverraum und der Serverschrank sind verschließbar. Schlüsselausgabe erfolgt nur an berechtigte Personen gegen Unterschrift.

Social Hacking

Die Kommunikation personenbezogener Daten erfolgt ausschließlich an eindeutig authentifizierte Personen.
Behörden werden in keinem Fall die mündliche Herausgabe von Daten verlangen.
Bei ungewöhnlichen Anweisungen durch Vorgesetzte werden diese auf einem zweiten Kommunikationsweg um Bestätigung gefragt.
Bei nicht eindeutig identifizierten Kommunikationspartnern erfolgt nur schriftliche Auskunft an die im Verwaltungsprogramm hinterlegte Adresse.
Übt die betroffene Person Druck zur Herausgabe von Daten auf den Mitarbeiter aus, ist der Vorgesetzte zu informieren.
Ansonsten ist der Mitarbeiter auf Geheimhaltung betrieblicher Informationen verpflichtet.

Datenpannen

Kommt dem Mitarbeiter eine Datenpanne zur Kenntnis, befolgt dieser die Anweisungen zur „Meldepflicht von Datenschutzverstößen“.
Es werden keinerlei Schritte außerhalb der Anweisungen eigenmächtig ausgeführt.
Bei Kenntnisnahme und vor weiterer Bearbeitung und Kommunikation ist der Datenschutzbeauftragte und/oder die Geschäftsleitung zu konsultieren.