HOTELGRUPPE FAMILIE ULTSCH

Richtlinien für Mitarbeiter
in Verbindung mit der DSGVO

I Versionsstände

Version	Datum	Kommentar	Bearbeiter
1	23.05.2018	Erstfassung	Johannes Neulinger

Einleitung

Datensicherheit geht uns alle an!

In fast jedem Unternehmen werden mittleiweile Daten vorwiegend elektronisch verarbeitet. Die verarbeiteten Daten reichen von Kundendaten, personenbezogene Daten, über Finanzdaten bis hin zu besonders schützenswerte Daten. Viele Unternehmen sind darüber hinaus mit Daten konfrontiert, die keinesfalls in Hände Dritter fallen dürfen – sei es aus Gründen des Datenschutzes oder weil es sich um vertrauliche Unternehmensdaten zu neuen Produkten, Strategien oder Verkaufsergebnissen handelt.

Datensicherheit im Allgemeinen und speziell IT-Sicherheit sind daher unverzichtbar für den Unternehmenserfolg. Unternehmensdaten müssen bestmöglich geschützt werden. Dies gilt sowohl für den Versuch, diese Daten auszuspionieren, als auch für die Gefahr des Datenverlustes durch technische Gebrechen.

Die nachfolgenden Punkte sind sowohl für das Unternehmen in dem sie arbeiten von großer Bedeutung, aber auch sie persönlich profitieren privat von dieser Richtlinie.

Mit ihrer Unterschrift bestätigen sie, dass sie diese Richtlinien beachten und umsetzen werden.

Sicherer Umgang mit personenbezogenen Daten

Personenbezogene Daten sind all jene Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben.

Besondere personenbezogene Daten umfassen Informationen über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit. Sie sind besonders schützenswert. (sensible Daten)

Betroffene haben vor allem das Recht auf informationelle Selbstbestimmung. Das Speichern und Verarbeiten von personenbezogenen Daten ist nur unter Zustimmung des Betroffenen zulässig.

Bitte beachten sie folgende Punkte:

- Personenbezogene Daten müssen geheim gehalten werden. Nur bei schriftlicher Zustimmung des Betroffenen dürfen diese Daten an Dritte weitergegeben werden.
- Bei Weitergabe der Daten muss auf einen sicheren Kommunikationsweg geachtet werden. Ein unverschlüsseltes E-Mail erfüllt diese Anforderung NICHT.
- Nach dem Ausscheiden aus dem Betrieb oder dem Wechsel der Arbeitsstelle dürfen sie personenbezogene Daten, die ihnen beruflich zugänglich gemacht wurden, nicht weitergeben oder für andere Zwecke nutzen.

Social Media

Soziale Medien wie Facebook, Instagram, Twitter, Snapchat und Co erfreuen sich immer größerer Beliebtheit. Sozialen Medien bringen viele Vorteile mit sich. Man Informiert sich über Rezepte, oder wie ein elektronisches Gerät funktioniert und kann sich gleich mit anderen Personen darüber austauschen. Jedoch haben soziale Medien auch einige Nachteile.

Speziell für Firmen werden soziale Medien mehr und mehr zum Problem in Punkto Sicherheit. Dieses Sicherheitsproblem wird meist ungewollt von Mitarbeitern verursacht, die nur schnell mal ein Foto vom Arbeitsplatz posten, oder nur kurz preisgeben, wann die gesamte Firma auf Skiurlaub fährt. Generell sollte man sich vor Augen führen, dass JEDE Information, sei sie noch so unwichtig, für irgendjemanden wichtig sein kann – dies sollte auch im privaten Umfeld beachten werden. Ein Foto von ihrem Arbeitsplatz kann z.B. Ordner zeigen, wo Kundennamen ersichtlich sind. Die Information, dass das gesamte Unternehmen auf Skiwochenende fährt, könnte einem Hacker das nötige Zeitfenster aufzeigen, um sich digital Zutritt zu verschaffen. Daher gehen sie mit Informationen, die sie preisgeben, besonders sorgsam um.

Bitte berücksichtigen sie folgende Punkte:

- Posten sie keine Fotos von ihrem Arbeitsplatz
- Posten sie keine Statusinformationen die das Unternehmen betreffen
- Geben sie in keinen Foren oder sozialen Medien irgendwelche Informationen über das Unternehmen, in dem sie arbeiten, preis
- Verwenden sie Pseudonyme für unbedingt notwendige Fragen in Foren oder soziale Medien, die das Unternehmen betreffen
- Nennen sie keine Namen. Weder ihren eigenen, noch den Namen des Unternehmens.

Clear Desk Policy

Unter der Clear Desk Policy versteht man, dass Mitarbeiterinnen und Mitarbeiter alle vertraulichen Dokumente, die sich auf ihrem Arbeitsplatz befinden, verschließen. Unberechtigte Personen (Reinigungspersonal, unbefugte Kolleginnen und Kollegen, oder Besucher) dürfen keinen Zugriff darauf erhalten.

Bitte beachten sie folgende Punkte:

- Bei Verlassen des Arbeitsplatzes müssen alle Ausdrucke, Kopien oder dergleichen so verstaut werden, dass diese Dokumente nicht für Dritte zugänglich sind (Schreibtisch, versperrbaren Kästen, Datenträgersafe).
- Lassen sie keine Ausdrucke im Drucker/Kopierer liegen.
- Bewahren sie unter keinen Umständen Passwortnotizen an Ihrem Arbeitsplatz auf.
- Sperren sie Ihren Computer, wenn sie Ihren Arbeitsplatz verlassen (z. B. unter Windows mit „Windows-Taste + L“)! Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko. Unbefugte könnten so Zugang zu vertraulichen Daten erhalten.

Persönliche Passwörter

Stellen sie sich ein Passwort wie einen Schlüssel zu ihrer Wohnung oder zu ihrem Haus vor. Zuhause möchte sie auch ein gutes Schloss besitzen, welches vor einem unbefugten Zutritt schützt. Genauso verhalten sich auch Passwörter. Passwörter schützen vor unbefugten Zutritt.

Bitte beachten sie folgende Punkte:

- Passwörter werden bei uns meist betriebsintern vorgegeben.
- Verwenden sie nie das gleiche Passwort für unterschiedliche Zugänge. (keine Firmenpasswörter privat verwenden)
- Verwenden sie Kennwörter, die mindestens 8 Zeichen haben. Ein Passwort muss aus einem Großbuchstaben, Kleinbuchstaben, Ziffer und einem Sonderzeichen bestehen um halbwegs sicher zu sein.
- Niemals Namen, Vornamen, Geburtsdaten, Tel.-Durchwahlen, etc. verwenden. Diese werden bei Angriffen zuerst ausprobiert.
- Verwenden sie keine Begriffe aus einem Wörterbuch (auch nicht in einer anderen Sprache). Es gibt Programme, die Wortlisten mit mehreren tausend Begriffen sofort abrufen und so mögliche Passwörter finden. Auch Eigennamen, geografische Begriffe etc. dürfen nicht verwendet werden.
- Trivial-Passwörter (hallohallo, abcdefgh, 08/15, 1234 etc.) sind ebenfalls ungeeignet. Sie können von Anderen leicht beim Beobachten der Passworteingabe erkannt werden.
- Geben sie ihr Passwort niemanden weiter! Auch Kollegen oder IT-Betreuung benötigen ihr Kennwort nicht.
- Ändern sie ihr Kennwort in regemäßigen Abständen (mind. alle 180 Tage).
- Überlegen sie sich einen Satz und verwenden sie nur die Anfangsbuchstaben für ihr Passwort.
    - Die Arbeit beginnt jeden Tag um 7 Uhr - DAbjTu7U
    - Am Samstag arbeite ich von 9 bis 13 Uhr - ASaiv9-13U
    - am 26. 10. ist Nationalfeiertag - a26.10.=N
- Sie sind für ihr Kennwort verantwortlich! Sollten sie den Verdacht haben, dass ein Dritter ihr Kennwort kennt, ändern sie dieses sofort.

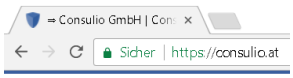
Zugangsdaten von Web-Portalen

Die Zugangsdaten für Web-Portale, oder sonstige Dienste die eine Autorisierung vorsehen, müssen in sicherer Form gespeichert werden. E-Mail oder Dateiablage ist hier nicht zulässig.

Selbstverständlich dürfen keine Zugangsdaten nach Austritt aus dem Unternehmen gespeichert, verwendet, oder in irgendeiner Form weiterverarbeitet werden.

Verschlüsselte Kommunikation

Bitte achten sie auf eine verschlüsselte Kommunikation. Ihr Browser beispielsweise signalisiert dies mit einem Schloss. Alle übermittelten Daten und alle Daten, die sie zum Beispiel in ein Formular auf dieser Webseite eingeben, sind demnach verschlüsselt. (SSL-Verschlüsselung)



Dokumente und Datenträger richtig entsorgen

Sorglos weggeworfene Dokumente stellen ein ernstes Sicherheitsproblem dar, wenn diese Daten in falsche Hände geraten. Aus diesem Grund müssen Dokumente, Datenträger (USB Stick, Festplatte, SD Karte, CD/DVD…) sicher entsorg werden. Für die sichere Entsorgung eignet sich ein Dokumenten-Schredder oder z.B. ein Dienstleistungsunternehmen, welches sich auf die sichere Entsorgung spezialisiert hat. Das Dienstleistungsunternehmen stellt ihnen anschließend ein Zertifikat aus, welches die fachgerechte Entsorgung bestätigt. Sollten beide oben genannten Entsorgungen nicht möglich sein, so ist das Dokument sohin unkenntlich zu machen, dass niemand Rückschlüsse auf den Inhalt ziehen kann.

Bitte beachten sie folgende Punkte:

- Werfen sie Datenträger oder wichtige Dokumente auf keinen Fall unvernichtet in den Papierkorb! Sofern es sich um Inhalte handelt, die Außenstehenden nicht zugänglich gemacht werden dürfen, müssen die Datenträger und Dokumente sicher entsorgt werden. Beachten sie, dass diese Vorgehensweise auch bei Archivmaterial einzuhalten ist.
- Übergeben sie die nicht mehr benötigten Datenträger den Verantwortlichen Ihrer IT-Abteilung bzw. einer eigens zu diesem Zweck bestimmten Person, die für die sichere Entsorgung zuständig ist.

Speicherung von Daten

Bitte versichern sie sich, dass Daten nur an den dafür definierten Bereichen gespeichert werden. Die Daten sollten zumindest auf einem Netzlaufwerk, oder in einem dafür vorgesehenen Dokumentenmanagement gespeichert werden. Eine Speicherung z.B. auf lokalen Datenträgern wie dem Desktop ihres Rechners, oder angeschlossene USB Sticks dürfen dafür nicht verwendet werden.

Umgang mit mobilen IT-Geräten

Mobile IT Geräte (Notebooks, Smartphones...) stellen durch ihre mobile Verwendung ein erhöhtes Sicherheitsrisiko dar. Portable Geräte sind für Diebe ein attraktives Ziel.

Bitte beachten sie folgende Punkte:

- Lassen sie das Gerät nicht unbeaufsichtigt.
- Überlassen sie das Gerät nicht anderen Personen.
- Achten sie bei Passworteingabe am Gerät auf ihren Sichtschutz – ähnlich wie bei einem Bankomaten.
- Verwenden sie ihren privaten Cloud-Speicher nicht für Unternehmensdaten.
- Installieren sie nur Anwendungen, die ihnen als vertrauenswürdig und sicher bekannt sind und von ihrer IT-Abteilung frei gegeben wurden.
- Melden sie einen Diebstahl oder Verlust sofort der IT-Abteilung.
- Achten sie auf eventuelle Daten- und Gesprächspaketvolumen um zusätzliche Kosten für das Unternehmen zu vermeiden.

Internetnutzung

Auch beim normalen Surfen im Internet lauern Gefahren, die nicht gleich als solche erkannt werden. Es liegt in ihrer eigenen Verantwortung, solche Bedrohungen zu erkennen und entsprechend darauf zu reagieren.

Bitte beachten sie folgende Punkte:

- Gebrauchen sie ihren Hausverstand! Wenn sie z.B. keinen Handy Vertrag mit A1 oder T-Mobile haben, handelt es sich bei eingegangen E-Mails von A1 oder T-Mobile meistens um betrügerische E-Mails.
- Übermitteln sie keine persönlichen Daten, vor allem nicht, wenn die Verbindung nicht als Sicher (HTTPS) markiert wird.
- Websites, die mit dem Download kostenloser Zusatzsoftware oder unseriösen Gewinnspielen locken, ist grundsätzlich zu misstrauen.
- Das Herunterladen von Dateien kann – abgesehen von der Gefahr des Einschleppens von Schadsoftware – auch zu lizenz- und urheberrechtlichen Problemen führen. Das gilt auch für Software, die nicht installiert oder ausgeführt wurde und nur auf dem Bürorechner gespeichert ist.
- Meiden sie Hackerseiten und solche, auf denen kommerzielle Software, möglicherweise in gecrackter Form, zum Download angeboten wird.
- Rufen sie keine Websites mit pornografischen, gewaltverherrlichenden oder strafrechtlich bedenklichen Inhalten auf. Das kann gravierende rechtliche Probleme – auch für ihr Unternehmen – nach sich ziehen.
- Fragen sie lieber einmal zu viel bei ihrer IT-Abteilung nach.

Protokollierung

Zu beachten ist, dass jeder Datenverkehr einer Protokollierung und Auswertung unterliegt, um eventuelle Datenverletzungen oder Schadcodeverbreitung frühzeitig erkennen und unterbinden zu können. Die Auswertung erfolgt nur in Verbindung der Geschäftsleitung unter Wahrung des Datenschutzes.

SSL Interception

Durch die Verwendung von verschlüsselten Verbindungen wird es leider auch Schadsoftware (Ransomware) ermöglicht, verschlüsselt und somit unentdeckt zu kommunizieren. Um dies zu verhindern, werden bestimmte Datenpakete an einem zentralen Punkt durchleuchtet. Davon ausgenommen sind Finanzdienstleister, Behörden, Rechtsanwälte, Gewerkschaften und Medizinische Einrichtungen.

E-Mail Nutzung

E-Mail gehört schon fast zur Standardausrüstung eines Arbeitsplatzes. Dadurch lohnt es sich auch für Kriminelle diese Form der Kommunikation zu nutzen. Somit landen aber auch Spam-, Hoax- oder Phishing-Mails sowie mit Schadprogrammen verseuchte Nachrichten in ihrem Posteingang. Solche unerwünschten Nachrichten – mit mehr oder weniger gefährlichem Inhalt – machen ca. zwei Drittel des weltweiten E-Mail-Aufkommens aus.

Bitte beachten sie folgende Punkte:

- Öffnen sie keine E-Mails, wenn ihnen Absender oder Betreffzeile verdächtig erscheinen.
- Öffnen sie niemals Dateianhänge, die ihnen verdächtig vorkommen. Auch bei vermeintlich bekannten und vertrauenswürdigen Absendern ist zu prüfen: Passt der Text der E-Mail zum Absender (englischer Text von deutschsprachigem Absender, unsinniger Text, fehlender Bezug zu aktuellen Vorgängen etc.)? Erwarten sie die beigelegten Dateien und passen sie zum Absender, oder kommen sie völlig unerwartet?
- Öffnen sie keine E-Mails mit Spaßprogrammen, da diese Schadsoftware enthalten können.
- Sogenannte Phishing-Mails, die zur Übermittlung von persönlichen Online-Banking-Daten oder Passwörtern (z.B. PIN oder TAN) auffordern, müssen gelöscht werden. Die angeforderten, vertraulichen Informationen dürfen sie auf keinen Fall weitergeben.
- Oftmals kann in einem E-Mail ein Link angeklickt werden, um eine Webseite aufzurufen. Seien sie dabei vorsichtig: In betrügerischen E-Mails wird diesen Links oft eine völlig andere Internet-Adresse hinterlegt, als im Mail zu sehen ist. Beim Anklicken wird dann eine gefälschte Phishing-Webseite aufgerufen oder sogar Schadsoftware installiert. Sicherer ist es, den Link mittels „Hyperlink kopieren“ in den Browser zu übertragen und ihn vor dem Aufrufen noch einmal zu überprüfen.
- Beantworten sie keine Spam-Mails! Die Rückmeldung bestätigt dem Spam-Versender nur die Gültigkeit Ihrer Mail-Adresse und erhöht dadurch Ihr Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.
- Benachrichtigen sie auch Ihre Kolleginnen und Kollegen über verdächtige Zusendungen. Besprechen sie die aktuellen E-Mails, die sie als Phishing-Versuche oder Virus-Mails erkannt haben, um gemeinsam die typischen Kennzeichen kennenzulernen. Sie können auf diese Weise sehr rasch Ihre Erkennungsfähigkeit trainieren und verbessern.
- Fragen sie ihre IT-Abteilungen, falls sie sich unsicher sind.
- Denken sie bei ihrem Urlaubsantritt oder bei Abwesenheit an den Abwesenheitsassistenten, um die Absender über ihre Abwesenheit zu informieren.

Social Engineering

Unter Social Engineering versteht man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten. Vorwiegend wird dieser Angriff per Telefon oder E-Mail durchgeführt. Ein aktuelles Beispiel ist der Angriff auf die Firma FACC. Durch eine gefälschte E-Mail-Adresse wurden mehrere Millionen Euro erbeutet. Bis heute konnte der Angreifer nicht dingfest gemacht werden.

Social Engineers geben sich gerne als Mitarbeiterinnen oder Mitarbeiter aus. Vielleicht behaupten sie auch, eine Behörde oder ein wichtiges Kundenunternehmen zu vertreten oder zu Ihrer IT-Abteilung zu gehören. Ihre Opfer werden durch firmeninternes Wissen oder Kenntnisse spezieller Fachbegriffe getäuscht, die sie sich zuvor durch Telefonate oder Gespräche mit anderen Kollegen erworben haben. Beim Angriff appellieren sie dann als „gestresster Kollege“ an Ihre Hilfsbereitschaft oder drohen als „Kunde“ mit dem Verlust eines Auftrages. Kommt ein Social Engineer bei einer Mitarbeiterin oder einem Mitarbeiter nicht ans Ziel, wird der Angriff bei der nächsten Ansprechperson wiederholt – bis er erfolgreich ist.

Bitte beachten sie folgende Punkte:

- Seien sie bei Telefonanrufen oder E-Mails skeptisch, speziell wenn der Wunsch oder der Auftrag der Kollegin oder des Kollegen außergewöhnlich ist.
- Falls möglich, besprechen sie die Angelegenheit mit ihrem Kollegen oder mit ihrer Kollegin persönlich.
- Fragen sie bei verdächtigen E-Mail ihre IT-Abteilung.
- Bedenken sie, dass Social Engineering sehr oft angewandt wird, aber meistens lange Zeit unentdeckt bleibt.
- Geben sie keine vertraulichen Informationen per Telefon oder E-Mail weiter.

Private Nutzung der IT

Die Nutzung der IT für private Zwecke ist untersagt. Dies betrifft sowohl die Nutzung der Geräte an sich (PC, Laptop, Smartphone…) als auch ihr Firmenpostfach (E-Mail) und den Firmeninternetanschluss. Sollte die private Nutzung von ihrer Seite notwendig sein, holen sie sich bitte eine schriftliche Ausnahmebestätigung von ihrem Vorgesetzten.

Warnungen und Fehlermeldungen

Warnungen oder Fehlermeldungen die sie selbst nicht verursacht haben, bzw. die sie nicht lösen können, müssen unverzüglich der IT Abteilung gemeldet werden.

Wechselmedien

Als Wechselmedien gelten alle externen Datenträger wie z.B. USB-Sticks, SD Karten, externe Festplatten, CD's, DVD's, Smartphones die per USB angeschlossen werden. Der Einsatz stellt ein großes Sicherheitsrisiko dar. Speziell wenn diese Datenträger aus externer Quelle standen. Auf diesen Wechselmedien kann sich Schadsoftware verstecken, welche das gesamten Firmennetzwerk lahmlegen kann. Generell ist die Verwendung von Wechselmedien untersagt. Bitte beantragen sie eine Ausnahmengenehmigung, falls sie dennoch Wechselmedien verwenden müssen.

Installation von Applikationen

Die Installation von Applikationen ist untersagt. Dies gilt sowohl für Windows Geräte (PC's, Notebooks, Server), aber auch für Firmeneigene Mobilgeräte wie Smartphone und Tablets. Falls sie eine Applikation benötigen, senden sie eine schriftliche Anfrage an ihre IT Abteilung. Auch harmlos wirkende Applikationen können Schadsoftware enthalten, oder sind Lizenzrechtlich nicht für den Firmeneinsatz freigegeben.

Austritt aus dem Unternehmen

Bei Austritt aus dem Unternehmen behält sich der Arbeitgeber das Recht vor, E-Mail-Adressen des ausscheidenden Mitarbeiters weiter zu verwenden, um den Unternehmensablauf nicht zu beeinträchtigen. Darüber hinaus verpflichtet sich der Mitarbeiter, sämtliche Dokumente, IT-Equipment und Unterlagen bei Austritt unaufgefordert dem Unternehmen bereit zu stellen. In einem Beschäftigungsverhältnis ist in der Regel der Arbeitgeber der Inhaber des generierten Geistigen Eigentums. Speziell im Hinblick auf Dokumente, Berechnungen oder dergleichen ist dies ein wesentlicher Punkt.

Eine willkürliche Löschung von Dokumenten, E-Mails, oder sonstigen firmenrelevanten Daten ist untersagt.