DaTeNSCHuTZ
Lorenz Macke
Hannover
Ihr persönlicher Datenschutzbeauftragter www.DtnSchtz.de

Personenbezogene Daten im Home Office schützen

Die Maßnahmen zur Kontrolle und Eindämmung von Covid-19 / Corona führen dazu, dass mehr Personen im Home Office arbeiten als sonst. Nachfolgend ein paar Tipps zur Sicherheit der (personenbezogenen) Daten, wenn außerhalb des üblichen Büro Arbeitsplatzes gearbeitet wird. Diese Liste kann bereits bestehenden Regelungen widersprechen oder ergänzen. Diese Liste kann beliebig erweitert werden…

Geräte:
-> Passen Sie auf, dass Geräte wie (*USB Sticks,*) Telefongeräte, Laptops oder Tablets nicht verloren gehen oder liegengelassen werden.

-> Stellen Sie sicher, dass jedes Gerät über die nötigen Updates verfügt, sei es Systemupdates aber auch Updates der verwendeten Software und Anti-Virenprogramme.

-> Stellen Sie sicher, dass Ihr Computer, Laptop oder sonstiges Gerät in einer sicheren Umgebung genutzt wird, wo Sie es selbst im Auge behalten können. Minimieren Sie die Möglichkeit, dass jemand anderes den Bildschirminhalt sehen kann, besonders dann, wenn Sie mit sensiblen Daten arbeiten.

-> Sperren Sie Ihr Gerät bevor Sie es unbeaufsichtigt lassen.

-> Stellen Sie sicher, dass Ihr Gerät ausgeschaltet, nach Möglichkeit abgeschlossen und sicher verwahrt ist, wenn Sie es nicht benötigen.

-> Benutzen Sie wirksamen Zugriffsschutz (wie 2 Faktor Authentifizierung und sichere Passwörter). Soweit verfügbar benutzen Sie eine Verschlüsselung, um den Zugriff auf das Gerät zu beschränken und um Risiken zu mindern, falls das Gerät verloren oder liegengelassen wird. (*Meldepflicht beachten!*)

-> Wenn ein Gerät verloren ging oder gestohlen wurde (*Melden!*), sind umgehend Schritte einzuleiten, welche den Speicher des Gerätes per Fernsteuerung löscht – sofern möglich.

-> Sprachassistenten/ Geräte / APPs sind zu deaktivieren. Der Zugriff auf Mikrofone ist weitestgehend zu deaktivieren. Ansonsten sind Gespräche außerhalb der Reichweite solcher Geräte zu führen.

Emails:
-> Berücksichtigen Sie alle Regelungen in Ihrem Betrieb, die sich auf E-Mails beziehen.

-> Benutzen Sie bevorzugt dienstliche E-Mail Accounts statt private E-Mail Accounts. Wenn Sie doch Ihren privaten E-Mail Account nutzen müssen, dann stellen Sie sicher, dass der Inhalt und die Anhänge verschlüsselt sind, und vermeiden Sie, dass personenbezogene oder geheime Informationen in der Betreff-Zeile sind.

Quelle: Irische Aufsichtsbehörde für Datenschutz, übersetzt und angepasst. V_03 28.03.2020

-> Bevor Sie eine E-Mail senden, stellen Sie sicher, dass Sie den(die) richtige(n) Empfänger ausgewählt haben, vor allen Dingen dann, wenn Sie umfangreiche oder sensible personenbezogene Daten versenden.
Cloud und Netzwerk Zugang:
-> Wenn es möglich ist, nutzen Sie nur die seitens des Betriebes als vertrauenswürdig eingestuften Netzwerke und Cloud Dienste und halten die diesbezügliche Regeln/Richtlinien sowie Handlungsanweisungen ein, was Zugriff, Login und Datenübertragung betrifft.

-> Wenn Sie ohne Cloud oder Netzwerkzugriff arbeiten, stellen sie sicher, dass lokal gespeicherte Daten auf angemessene Weise gesichert werden.

Papierdokumente:
-> Es ist wichtig zu beachten, dass der Datenschutz nicht nur für elektronisch gespeicherte oder verarbeitete Daten gilt, sondern auch für personenbezogene Daten in manueller Form (z. B. Papierunterlagen), wenn diese Teil der elektronischen Verarbeitung sind oder sein sollen.

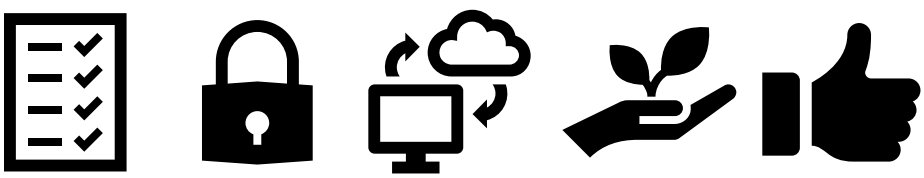
-> Wenn Sie im Home Office mit Papierunterlagen arbeiten, ergreifen Sie Maßnahmen, um die Sicherheit und Vertraulichkeit dieser Unterlagen zu gewährleisten, z. B. indem Sie die Papierunterlagen bei Nichtgebrauch in einem Aktenschrank oder einer Schublade aufbewahren und bei Nichtgebrauch sicher entsorgen (z. B. zerkleinern) und sicherstellen, dass sie nicht an einem Ort zurückgelassen werden, an dem sie verlegt oder gestohlen werden könnten.

-> Wenn Sie mit Aufzeichnungen arbeiten, die in die Kategorie der besonders schützenswerten personenbezogenen Daten fallen (z. B. Gesundheitsdaten), sollten Sie besonders darauf achten, deren Sicherheit und Vertraulichkeit zu gewährleisten, und diese Aufzeichnungen nur dann von dem bisherigen sicheren Aufbewahrungsort (Geschäftsräume) entfernen, wenn die Arbeit (im Home Office) ausgeführt werden muss.

-> Wenn möglich sollte für Andere (z.B. Mitarbeitende) nachvollziehbar festgehalten werden, welche Unterlagen und Datenträger *(verschlüsselt)* mit nach Hause genommen wurden, damit nachvollziehbar ist, wo sich die Unterlagen befinden, auch für mögliche Nachfragen.

Für weitere Informationen können sich die Betriebe an Ihren Datenschutzbeauftragten wenden. Ist (noch) keiner vorhanden, könnten die Webseiten der Aufsichtsbehörden Auskünfte geben, oder der IT-Betreuer kann helfen.

Mitarbeiter fragen den Vorgesetzten, den IT-Betreuer oder den Datenschutzbeauftragten.



-> Bleiben Sie, Ihre Geräte und Ihre Daten gesund!