



## WORAUF REISEBÜROS IN SACHEN DATENSCHUTZ ACHTEN SOLLTEN

- Bildschirme abdunkeln: Gerade wenn man durch Fensterscheiben von außen gut in die Bildschirme sehen kann, empfiehlt es sich diese mit speziellen Privacy-Folien vor neugierigen Blicken zu schützen.
- Verzichten Sie möglichst auf Videoüberwachung oder haben Sie zumindest keine aktiv, wo Kunden beraten werden und ihre Dokumente ausgehändigt bekommen bzw. ihren Personalausweis oder ähnliches vorzeigen. Auf jeden Fall müssen Kunden auf eine mögliche Videoüberwachung aufmerksam gemacht werden.
- In einem Reisebüro gibt es ständig "Laufkundschaft", also kleben Sie keine Passwörter etc. an den Bildschirm oder lassen diese herumliegen. Am besten schreiben Sie überhaupt keine Passwörter auf. Auch personenbezogene Daten der vorherigen Buchenden sollten schnellstens sicher weggeräumt werden.
- Mitarbeiter sollten regelmäßig Datenschutz-Schulungen erhalten und kontinuierlich über die technischen Möglichkeiten von Datenmissbrauch entsprechend aufgeklärt werden.
- Personalausweise sollten nicht kopiert werden. Ein vorzeigen der Ausweise sollte für eine Reisebuchung ausreichend sein.
- Namensschilder Ihrer Angestellten mit vollen Namen, sollten überdacht werden.
- Bei Profilerstellungen/Registrierungen von Kunden, die von Dauer sind und auch außerhalb der Reise verwendet werden können auf Freiwilligkeit hinweisen
- Bei Werbemaßnahmen des Reisebüros, müssen die Kunden vorher ausdrücklich zustimmen.
- Fotos von Familie / Kinder. Es ist schön wenn Ihre Mitarbeiter sich gerne erinnern möchten, dass Sie Kinder/Familie haben. Aus Datenschutzgründen sollten Sie jedoch keine Familienfotos öffentlich sichtbar platzieren, da diese jederzeit ab fotografiert und ungewollt im Internet landen können.

### Technik

- Verschlüsseln der Laufwerke (Festplatten u. USB Sticks) / Betriebssysteme (mit einem sicheren Passwort). Nicht nur zum Schutz vor Hacks ist es sinnvoll zu verschlüsseln, sondern auch bei einem möglichen Diebstahl der Festplatten oder wenn Sie diese Entsorgen möchten!
- Einsatz von Betriebssystemen/Software sollte überdacht werden. Neugierige Betriebssysteme mit aktiver Sprachsteuerung (z. B. Cortana) sollten nicht eingesetzt werden, um die Privatsphäre Ihrer Kunden und Mitarbeiter zu schützen. Gerade in Reisebüros werden sprachlich sensible personenbezogene Daten wie Name, Geburtstag, Adresse, Kreditkarteninformationen und Passnummer übermittelt.



- Sämtliche Sprachsteuerung / aktive Mikrofone auf privaten Endgeräten (z. B. Smartphones) sollten (aus vorherigen Absatz genannten Gründen) abgestellt werden. Am besten sollte das Smartphone während der Arbeit ausgeschaltet werden.
- Login von "zu Hause" vermeiden. Vermeiden Sie es, dass Mitarbeiter von zu Hause auf Buchungsdaten zugreifen können. Das "Heimnetz" ist bei den Otto-Normalverbraucher meist nicht sonderlich sicher eingerichtet und zudem besteht die Gefahr, dass Dritte Kenntniss der Daten bekommen (z. B. Lebensgefährten, Freunde etc.), der Person mit Zugang von zu Hause aus. Zudem kann es sein, dass Mitarbeiter "smarte Assistenten" (Alexa, Cortana etc.) zu Hause aktiv haben und diese die Namen und personenbezogenen Daten aufnimmt, wenn Ihr Mitarbeiter diese vorliest oder den Kunden anruft.
- Das Reisebüro sollte sich mit Auftragsverarbeitungsverträgen absichern, wenn es mit Dritten zusammenarbeitet (z. B. für den IT-Support für das Reisebüro, Werbemaßnahmen, Partner an denen die Gästedaten weitergegeben werden usw.)
- Sofortiges Anlegen von Kundenprofilen sollte unterlassen werden.
- Kundenprofile sollten auch wieder gelöscht werden. Gerade im Hinblick auf mögliche Hacks, sollten Daten nicht von Dauer gespeichert werden. Nicht alle Kunden kommen wieder oder vergessen sogar, dass sie diese Daten dort noch gespeichert haben. Dadurch entstehen auch beim Reisebüro viele Karteteileichen.
- Suchen Sie auf Social Media Kanälen nicht nach Ihren Kunden, auch nicht für mögliche Werbezwecke oder weil Sie eine Fanpage haben.
- Vermeiden Sie das private Surfen auf Facebook & Co.! Wie Sie in unserem Beitrag gelesen haben, gibt es in zahlreichen Webbuchungsmanagern und Hotelmanagern zahlreiche Tracker von Facebook, Google und Co.

