SWISS
BUSINESS
PROTECTION

Newsletter April 2020

Datenschutz und Datensicherheit im Home Office

Das Coronavirus und die entsprechenden Massnahmen des Bundesrates und ausländischer Regierungen – Stichwort #stayhome (sowohl als Empfehlung wie auch als Ausgangsverbot), Ein- und Ausreisebeschränkungen bzw. -verbote etc. – stellen die gewohnten Arbeitsabläufe auf den Kopf. Ganze Unternehmen verlagern ihre Arbeitstätigkeit ins Home Office ihrer Mitarbeitenden. Wer nicht bereits vor der Pandemie im Home Office arbeiten liess, wurde plötzlich vor grössere rechtliche, technische und organisatorische Herausforderungen gestellt. Bereits heute ist zudem absehbar, dass die Coronapandemie unsere Arbeitsweise wohl nachhaltig ändern und uns das digitale Arbeiten im Home Office in viel stärkerem Ausmass als bisher bleiben wird, da die Anfangshürden gemeistert und der Nutzen solcher Arbeitsformen erkannt worden sind. Dementsprechend kommen Unternehmen nicht darum herum, ihren Complianceanforderungen in Bezug auf Datenschutz, Datensicherheit und Arbeitsrecht nachzukommen, diese bei jedem einzelnen Tool zu prüfen und bestehende Datenschutz- und/oder ICT-Nutzungsweisungen zu ergänzen oder gänzlich neue Weisungen für das Arbeiten im Home Office zu erstellen. Dies sei im Folgenden anhand einiger, nicht abschliessender Beispiele dargelegt:

Die datenschutzrechtlichen Herausforderungen im Home Office beginnen bereits mit der eingesetzten Hardware: Handelt es sich dabei um private Geräte der Mitarbeitenden (Bring Your Own Device; BYOD), setzt das Unternehmen auf eine Flottenstrategie von Corporate Owned, Personally Enabled (COPE) oder handelt es sich um reine Unternehmensdevices, die nicht privat eingesetzt werden dürfen? Unproblematisch ist die reine Unternehmenslösung, während BYOD und COPE zu kniffligen Fragen bezüglich Trennung der privaten Daten der Mitarbeitenden von Unternehmensdaten und betreffend Zugriff des Unternehmens auf diese Geräte darauf gespeicherten privaten Daten führen. Solche Zugriffe können sowohl im Einzelfall als auch systematisch über eingesetzte Tools zum Mobile Device Management (MDM) oder umfassender über das Enterprise Mobility Management (EMM) erfolgen. Eng damit verbunden sind Überlegungen zum Ort der Datenablage und zur Umsetzung von Datenaufbewahrung, -archivierung und -löschung.

All dies – und noch viel mehr, beispielsweise Zugriffsberechtigungen, Passwort-Policies etc. – ist im Rahmen von Datenschutz- und ICT-Nutzungsweisungen zu regeln und über MDM, EMM als auch mittels zusätzlicher Lösungen wie VPN-Verbindungen zwischen Arbeitnehmer und Unternehmen sowie Festplattenverschlüsselung und Antivirenschutz auf den eingesetzten Geräten technisch sicherzustellen.

Weiter muss sich ein Unternehmen beim Einsatz von Home Office fragen, ob mit den eingesetzten Tools für Kommunikation, Kollaboration oder Datenaustausch Personal- oder andere Personendaten ins Ausland bekanntgegeben werden und die datenschutzrechtlichen Anforderungen an ein solches Outsourcing erfüllt werden, sei dies nach DSG, DSGVO oder der Berufsgeheimnisbestimmungen. Selbst wenn diese Fragen unternehmensseitig abgeklärt wurden, ist die Zulässigkeit von Datenbekanntgaben oftmals nicht abschliessend gewährleistet. So übermittelte gemäss Berichten des Swiss IT Magazine und von golem.de die derzeit boomende Videokonferenzlösung *zoom* bis vor kurzem über ihre iOS-App Daten an Facebook, selbst wenn der betreffende User auf dieser Social Media-Plattform über kein Konto verfügte. Übermittelt wurden offenbar das jeweilige Öffnen der App sowie Angaben über Hardware der Anwender wie Modellkennung, Bildschirmgrösse, Zeitzone, Aufenthaltsort oder genutzte Provider sowie insbesondere die Werbe-ID von Facebook, über welche mittels Aggregation der Daten aus anderen Apps Verknüpfungen zu Krankheiten, Reiseverhalten, Dating und weiteren Informationen des betroffenen Users möglich sind. Dies alles ohne entsprechende Hinweise in der Datenschutzerklärung des Anbieters. Nach Angaben von *zoom* habe man von der Datenweitergabe an Facebook angeblich nichts gewusst und diese mittlerweile unterbunden.

Schliesslich verfügen die im Rahmen von Home Office eingesetzten Tools teilweise auch über Trackingfeatures, die es Hosts oder Moderatoren erlaubt festzustellen, wenn die Teilnehmenden in anderen Browserfenstern aktiv sind. Eine systematische Verhaltensüberwachung der Mitarbeitenden ist aber sowohl aus datenschutz- wie arbeitsrechtlicher Sicht unzulässig und lediglich zum Zweck von Leistungs- oder Sicherheitskontrollen gerechtfertigt.

Somit ergeben sich bereits aufgrund dieser nicht abschliessenden Auslegeordnung eine ganze Reihe von Aspekten, die durch das Unternehmen zu prüfen und im Rahmen bereits bestehender Datenschutz- und ICT-Nutzungsweisungen oder gänzlich neuer Weisungen für das Arbeiten im Home Office zu regeln und technisch umzusetzen sind. Wichtig ist daher, dass jedes Unternehmen bei seinen individuellen Settings sämtliche regelungs- und umsetzungsbedürftigen Themen umfassend ermittelt und zeitnah die entsprechenden Compliancemassnahmen umsetzt.

Dr. iur. Reto Fanger ist Founding Partner der Swiss Business Protection AG (www.swissbp.ch), Rechtsanwalt und Gründer/Inhaber der ADVOKATUR FANGER – Anwaltsboutique für ICT-, Daten-, Medien- und Arbeitsrecht, Luzern (www.advokatur-fanger.ch), Dozent an der Hochschule Luzern (HSLU), Lehrbeauftragter an der Universität Luzern sowie Co-Tagungsleiter des Lucerne Law & IT Summit (LITS) an der Universität Luzern.