Datenschutz und Digitalisierung – kein Ende abzusehen

Viele Unternehmen haben mit der Einführung der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) Ihre Hausaufgaben gemacht – oder zumindest damit begonnen. Es gibt kaum eine Organisation ohne Datenschutzerklärungen im Webauftritt, Vereinbarungen zur Auftragsverarbeitung sind geschlossen, die Mitarbeitenden zum Datenschutz verpflichtet, vielleicht bestehen sogar Löschkonzepte. Eine kommentierende Auseinandersetzung von Peter Strzeletz.

Die Flut von Einzelthemen

Für eine Vielzahl von Detailfragen sind Organisationsabläufe angepasst worden. Beispielhaft sei hier die Anfertigung und Verbreitung von Bildmaterial genannt. Nicht nur, dass neue Vereinbarungen zur Freigabe und zur Verwendung von Bildern entstanden sind – wir haben es vielmehr mit einer deutlichen Veränderung in der Kultur des Umgangs miteinander zu tun, wenn es zum Beispiel Kindertageseinrichtungen gelingt, das beliebige „Herumfotografieren“ mit dem Mobilgerät durch den kontrollierten Einsatz der hauseigenen (Digital-)Kamera zu ersetzen.

Doch es existieren zudem einige Nebenschauplätze, in denen der Datenschutz die Arbeitsweise verändert: Mit dem Urteil des OVG Lüneburg vom 22. Juli 2020 dürfen personenbezogene Daten per Telefax nur noch unter der Bedingung übertragen werden, dass die Telefaxverbindung auf beiden Seiten verschlüsselt ist. Schon lange ist klar, dass ein für jede Person einsehbares Telefaxgerät ein datenschutzrechtliches „No-Go“ ist.

Drucker, Kopierer und Scanner – besonders die beliebten Multifunktionsgeräte – sind vernetzte IT-Systeme und können jedes Netzwerk von innen und außen angreifbar machen. Datensicherheitskompetenz bei den liefernden Unternehmen? In meiner persönlichen Statistik als Datenschutzbeauftragter: Fehlanzeige.

Aber was sind, neben der großen Menge von Einzelfragen, die elementaren Themen? Die Corona-Pandemie hat sie aufgedeckt:

Gretchenfrage Amerika

Es gibt keine nennenswerten europäischen Systeme für die Digitalisierung der Zusammenarbeit in Unternehmen und die Durchführung von Videokonferenzen. Microsoft Teams bietet beides (auch noch kombiniert) und verzeichnet weltweit explodierende Nutzerzahlen; ebenso wie Zoom als Spezialist für Videokonferenzen. Das wäre nicht weiter schlimm, stünde der Nutzung dieser Produkte nicht der Datenschutz entgegen.

Bereits Nutzer von Office 365 mussten sich mit wackeligen Konstrukten wie dem „Privacy-Shield“ aus dem Datenschutzschlamassel herausmanövrieren. Der Begriff „Schlamassel“ ist in diesem Kontext schnell definiert: Firmen mit Sitz in den USA sind grundsätzlich verpflichtet, staatlichen Akteuren Zugriff auf beliebige Informationen zu geben, wo auch immer auf der Welt sich diese physikalisch befinden. Konsequenterweise vertritt die Berliner Beauftragte für Datenschutz und Informationssicherheit den Standpunkt, dass kein einziges Videokonferenzsystem ohne Verletzung der EU-DSGVO benutzt werden kann! Der Europäische Gerichtshof hat den „Privacy Shield“ zeitgleich für nichtig erklärt. Es verbleiben aktuell die „Standardvertragsklauseln“, die sich mit jeder Datenschutzerklärung aus Übersee herunterladen lassen. Tenor: „Wir nehmen den Datenschutz ernst. Wir garantieren für nichts.“

Was ist zu tun? Es gibt keine allgemeinen Lösungen. Wir empfehlen folgendes Vorgehen: Identifizieren Sie die größten Sicherheitsrisiken konkret und gehen Sie diese dokumentiert an.

Trend zur Cloud

Eine kurze Definition vorab: Lokal installierte Softwareprodukte werden von Anwendungen in Rechenzentren abgelöst. Das reicht vom Betrieb klassischer Software im Rechenzentrum über die externe Speicherung von Daten in Diensten wie Google Drive bis zu dem Punkt, die gesamte Benutzeroberfläche über das Internet zu beziehen und keinerlei Programmkomponenten mehr im lokalen Netzwerk oder auf dem Endgerät vorzuhalten. Der Datenschutz sieht diese Entwicklung grundsätzlich wohlwollend. Pointiert ausgedrückt, gibt es zwei herausragende Möglichkeiten, Daten mit hoher Wahrscheinlichkeit für unbefugte Dritte bereitzustellen: in einem selbstverwalteten Endgerät bzw. Netzwerk oder in einer E-Mail auf Ihrer Reise durch das Internet.

Vor dem Hintergrund dieser Annahme wird auch deutlich, dass ein schnell eingerichtetes Home-Office die Herausforderungen an Datensicherheit und Datenschutz zunächst vergrößert. Auch hier gilt aus der Sicht des Datenschutzpraktikers: Es muss an den Details gearbeitet werden, ohne die grobe Richtung der Digitalisierung hin zur Cloud aus den Augen zu verlieren. Konkret braucht es Schutzkonzepte, Handreichungen für den Umgang mit Apps und die Beachtung der kulturellen Seite. Und ganz wichtig: Mitarbeitende und Betroffene müssen mitgenommen werden!

Zum Autor:

Peter Strzeletz ist Geschäftsführer der Firma MICROPLAN GmbH mit Sitzen in Wuppertal und Berlin. Mit seiner Firma unterstützt er seit 25 Jahren gemeinnützige Organisationen mit Software im Umfeld von Microsoft Office.