# IT-Sicherheit und der Umgang mit IT-Geräten

Unternehmen müssen geeignete Massnahmen ergreifen, um eine angemessene Datensicherheit gewährleisten zu können. Diese Massnahmen beziehen sich auch auf den Umgang von Mitarbeitenden mit IT-Geräten. Die diesbezüglichen Vorgaben werden üblicherweise in einem IT-Reglement festgehalten, welches für die Mitarbeitenden verbindlich ist. Im Folgenden legen wir den üblichen Inhalt solcher IT-Reglemente dar.

**Von Stefan Eichenberger und Marius Vischer**

## Gewährleistung der Datensicherheit

Am 1. September 2023 tritt in der Schweiz das revidierte Datenschutzgesetz (revDSG) in Kraft, welches in weiten Teilen eine Angleichung an die Rechtslage in der Europäischen Union (DSGVO) zur Folge hat. Damit tritt das Thema Datenschutz auch in der Schweiz vermehrt in den Fokus.

Die Revision hat im Wesentlichen einen Ausbau der Governance von Unternehmen zur Folge (Datenschutzerklärung, Bearbeitungsverzeichnisse, Datenschutz-Folgenabschätzungen etc.).

In Bezug auf die Datensicherheit müssen Unternehmen wie bisher durch geeignete technische oder organisatorische Massnahmen (sog. TOMs) eine dem Risiko angemessene Datensicherheit gewährleisten. Dies bedeutet, dass diejenigen Massnahmen zu ergreifen sind, welche in Anbetracht des Zwecks der Datenbearbeitung, des Risikos, des Stands der Technik und der Implementierungskosten erforderlich und angemessen sind.

Typische Massnahmen zur Erreichung angemessener Datensicherheit sind z. B. Zugriffsbeschränkungen, Zugangsbeschränkungen, Datenverschlüsselung, Backup, Bewachung, Alarmanlagen, aber auch Reglemente, Weisungen und Schulungen.

Zwar bleiben die Anforderungen in Bezug auf die Datensicherheit auch unter dem revDSG im Wesentlichen unverändert. Was sich jedoch stetig verschärft, ist die Bedrohungslage. Hackerangriffe nahmen über die letzten Jahre stark zu. Eine Auseinandersetzung mit der Datensicherheit, allenfalls unter Hinzuziehung von externen Spezialisten, gewinnt vor diesem Hintergrund an Aktualität und ist zwingend geboten.

Was eine angemessene Datensicherheit ist, müssen die Unternehmen selbst entscheiden. Die getroffenen Massnahmen müssen keinen absoluten Schutz bieten, sondern in einem vernünftigen Verhältnis zum Risiko einer Verletzung der Datensicherheit stehen. Wir empfehlen, dass Unternehmen die diesbezüglichen Überlegungen und die getroffenen Sicherheitsmassnahmen dokumentieren, auch mit Blick auf die Strafbestimmung des revDSG, welche die vorsätzliche Nichteinhaltung der Mindestanforderungen unter Strafe stellt.

## Inhalt des IT-Reglements

Allerdings ist es mit dem Ergreifen dieser Massnahmen nicht getan. Oft sind es die Mitarbeitenden, die Einfallstor einer Sicherheitsverletzung sind. Sie sollten deshalb informiert werden, wie mit den vom Arbeitgeber zur Verfügung gestellten Arbeitsgeräten oder den im Arbeitskontext verwendeten privaten Geräten umgegangen werden soll. Auch sollten regelmässig entsprechende Schulungen durchgeführt werden.

Obwohl Unternehmen in der Schweiz keine Pflicht haben, ein für die Mitarbeitenden bindendes IT-Reglement zu erlassen, geschieht eine solche Information der Mitarbeitenden in der Regel über ein solches. Dies bietet sich auch an, denn wird das IT-Reglement als einseitige Weisung des Arbeitgebers (im Sinne von Art. 321d OR) ausgestaltet, ist es für die Mitarbeitenden verbindlich, ohne dass sie zustimmen müssen. Eine blosse Kenntnisnahme im Sinne einer Information (z. B. durch einen Hinweis im Arbeitsvertrag) sowie idealerweise einer Schulung reicht aus. Wir empfehlen, im Reglement explizit darauf hinzuweisen, dass es sich dabei um eine arbeitsrechtliche Weisung handelt.

Das Reglement ist regelmässig auf Aktualität hin zu überprüfen. Im Falle der Ausgestaltung der Reglements als arbeitsrechtliche Weisung bedarf es bei einer Anpassung oder Weiterentwicklung zwar wiederum einer Information und allenfalls einer Schulung der Mitarbeitenden, jedoch (weiterhin) keines Einverständnisses. Würde es als Zusatzvereinbarung zum Arbeitsvertrag ausgestaltet, müsste jeweils jeder Mitarbeitende einzeln Änderungen zustimmen.

Der Inhalt des IT-Reglements geht typischerweise über reine Datensicherheitsthemen hinaus. Unseres Erachtens sollte es sich zu folgenden Themen äussern, wobei nachfolgend auf gewisse Punkte vertiefter eingegangen wird:

- vertraulicher Umgang mit betrieblichen Daten
- Umgang mit betrieblichen IT-Geräten
- Aufzählung von verbotenen Aktivitäten
- Regeln in Bezug auf die Nutzung von Internet und Social Media während der Arbeitszeit
- Vorgaben zur privaten Nutzung des geschäftlichen E-Mail-Accounts, Verpflichtung zur Kennzeichnung privater E-Mails als privat
- Zulässigkeit der Verwendung privater Geräte
- Hinweis auf Überwachungsmöglichkeiten des Arbeitgebers
- Androhung von Konsequenzen beim Verstoss gegen das Reglement

## Nutzung der betrieblichen IT-Geräte

Typischerweise wird festgehalten, dass Mitarbeitende die ihnen zur Verfügung gestellten IT-Geräte (Laptops, Tablets, Smartphone etc.) sorgfältig zu behandeln haben. Auch wird festgehalten, ob und gegebenenfalls in welchem Umfang die private Nutzung der betrieblichen IT-Geräte erlaubt ist. In der Regel

wird eine eingeschränkte private Nutzung erlaubt, wobei darauf hingewiesen wird, dass sich die private Nutzung nicht negativ auf die Produktivität der Mitarbeitenden auswirken darf.

Weiter enthält das Reglement üblicherweise einen Katalog von Handlungen, die verboten sind. Beispiele sind:

- das Verlassen des Arbeitsplatzes ohne Sperren oder Abmelden des Benutzers (Daten sind auch intern vor unberechtigtem Zugriff zu schützen)
- die Verwendung von IT-Geräten, um anstössige Inhalte abzurufen oder herunterzuladen (u.a. pornografische, beleidigende, diskriminierende, rassistische oder diffamierende Inhalte)
- die Installation bzw. Nutzung von Software oder Cloud Services, die von der internen IT nicht freigegeben wurden
- das Speichern, Ausführen oder Verbreiten von jeglicher Schadsoftware
- der Einsatz von privaten Konten bei freigegebenen Cloud Services (z.B. privates Microsoft-365-Konto)

## Nutzung der privaten IT-Geräte

Das IT-Reglement äussert sich in der Regel auch zur Frage, ob private Geräte (z.B. das eigene Smartphone) für geschäftliche Zwecke verwendet werden dürfen oder gar müssen (im Sinne von «Bring Your Own Device»).

Die Problematik bei der Nutzung der privaten Geräte zu geschäftlichen Zwecken liegt u.a. darin, dass die privaten Geräte nicht von der betrieblichen IT überwacht und geschützt werden; insbesondere wurden die darauf installierten Apps nicht durch diese geprüft und freigegeben. Private Geräte können mithin eine Gefahr für die Datensicherheit darstellen. Darauf sollten die Mitarbeitenden sensibilisiert werden.

Häufig machen die Arbeitgeber den Mitarbeitenden Vorgaben in Bezug auf den Passwortschutz von Smartphones und Tablets, weil nur schon der Einsatz von sechs Zahlen oder von wenigen Buchstaben und Sonderzeichen einen gegenüber den üblichen vier Zahlen wesentlich höheren Schutz bietet bzw. die Zeit, die ein Angreifer braucht, den Passwortschutz zu überwinden, wesentlich erhöht.

Wird das Smartphone für geschäftliche Zwecke verwendet, wird meistens auch der betriebliche E-Mail-Account synchronisiert. E-Mails können besonders sensitive Daten enthalten. Deshalb sollte der Arbeitgeber die Möglichkeit haben, bei einem Verlust des privaten Geräts vertrauliche, betriebliche Daten zu löschen, um diese möglichst unmittelbar vor einem unberechtigten Zugriff von Dritten zu schützen.

## Mobiles Arbeiten

Da das mobile Arbeiten mittlerweile zum Standard gehört, sollte sich das Reglement auch dazu äussern. Beim Arbeiten von unterwegs ist darauf zu achten, dass keine vertraulichen Informationen Dritten zugänglich gemacht werden, z.B. durch Telefonieren in der Öffentlichkeit. Beim Arbeiten mit dem Laptop sollten vertrauliche Daten von Dritten nicht eingesehen werden können. Bei häufigem Arbeiten von unterwegs (z.B. im Zug) sollte dem Mitarbeitenden von der IT ein entsprechender Sichtschutz zur Verfügung gestellt werden. Selbstverständlich müssen die Geräte stets beaufsichtigt und auch an sicheren Orten passwortgeschützt zurückgelassen werden.

Bei regelmässigem Arbeiten im Homeoffice empfiehlt sich der Erlass eines separaten Homeoffice-Reglements, welches die wichtigsten Punkte regelt (z.B. zeitliche Rahmenbedingungen, Kostenregelung für Spesen, Verhalten im Homeoffice inkl. Störungen, Arbeitsschutz).

## Meldepflicht

In Bezug auf alle Geräte, die betrieblich genutzt werden, gilt, dass bei einem Verlust umgehend eine intern zuständige Person oder Abteilung zu informieren ist, welche notwendige Schritte einleiten kann, wie beispielsweise die Löschung sämtlicher Daten auf dem Gerät und die Abklärung von Meldepflichten (siehe sogleich).

Eine interne Meldepflicht sollte auch für den Fall vorgesehen werden, dass ein Mitarbeitender eine E-Mail mit zweifelhaftem Absender oder merkwürdigen Formulierungen erhält (z.B. Erhalt einer Phishing-E-Mail) oder der Mitarbeitende Kenntnis eines Datensicherheitsvorfalls auf den Arbeitgeber erhält (z.B. Hackerangriffe, E-Mail-Versand mit heiklen Daten an einen falschen Abnehmerkreis).

Kommt es tatsächlich zu einem Datensicherheitsvorfall, muss der Arbeitgeber imstande sein, umgehend die notwendigen Schritte einzuleiten und abzuklären, ob allenfalls eine Meldepflicht beim EDÖB besteht, welche mit dem revDSG eingeführt wird, wenn eine Verletzung der Datensicherheit zu einem hohen Risiko für die Persönlichkeit oder der Grundrechte der betroffenen Person führt.

## Überwachung und Sanktionen

Schliesslich schafft ein Unternehmen mit dem IT-Reglement eine Rechtsgrundlage für die Anordnung von Überwachungsmassnahmen und das Ergreifen von arbeitsrechtlichen Sanktionen bei Nichteinhaltung des Reglements. Sowohl mögliche Überwachungsmassnahmen als auch Sanktionen sollten im Reglement näher umschrieben werden, damit sie rechtskonform sind.

## AUTOREN

**Dr. Stefan Eichenberger** ist Partner bei epartners Rechtsanwälte in Zürich. Er berät und unterstützt seine Klienten insbesondere in folgenden Tätigkeitsgebieten: Vertragsrecht (insbesondere Arbeitsrecht), Gesellschaftsrecht, Erbrecht, Datenschutzrecht, Steuerrecht sowie in der Prozessführung.

**Marius Vischer** ist Rechtsanwalt und Partner bei epartners Rechtsanwälte in Zürich. Er ist schwerpunktmässig im Vertragsrecht, im IT- und Technologierecht, im Datenschutz- sowie im Wettbewerbsrecht tätig; er ist sowohl beratend als auch prozessierend tätig und gibt regelmässig Schulungen und leitet Workshops.