PRODATIS®

The eBusiness Solution Company.

Mobiles Arbeiten: Bring your own Device revisited

Viele Beschäftigte arbeiten immer noch im Homeoffice, ein Teil davon mit privaten Geräten – und das oft völlig ungeregelt. Das hier vorgestellte Muster einer Betriebsvereinbarung ist eine gute Ausgangsbasis, mit der Unternehmen für klare und sichere Verhältnisse sorgen.

Die Corona-Pandemie hat sowohl die Digitalisierung der Prozesse als auch die Arbeit im Homeoffice quasi über Nacht vorangebracht. Selbst Unternehmen und Behörden, die die Arbeit im Homeoffice bis dato strikt abgelehnt hatten, sahen plötzlich Vorteile in der Arbeit von zu Hause.

Sie hatten allerdings das Problem, dass kurzfristig nicht hinreichend mobile IT-Geräte (Notebooks, Mini-PCs und Tablets) am Markt verfügbar waren. Damit stand verstärkt die Frage der Nutzung von privaten IT-Geräten im Raum.

Selbst Datenschutzaufsichtsbehörden erteilten aufgrund der Notsituation unter Auflagen befristete Freigaben für den Einsatz privater IT-Geräte bis in den Gesundheits- und Sozialbereich. Doch mittlerweile ist es geboten, diese Nutzung privater Geräte in geregelte Bahnen zu lenken.

Kontrollverlust vermeiden

Arbeiten Beschäftigte mit privaten IT-Systemen, ist eine große Sorge der Arbeitgeber, die Kontrolle zu verlieren. Denn der Arbeitgeber darf die privaten IT-Geräte nicht ohne Weiteres untersuchen. Hier sind Regelungen nötig, die diesen Kontrollverlust weitgehend vermeiden, ohne die Beschäftigten unnötig im Privatbereich zu tangieren.

Eine Regelung zur Nutzung privater IT-Systeme besteht aus zwei Teilen:

- einer Betriebsvereinbarung, die den allgemeinen Rahmen bestimmt, und
- einer individuellen Vereinbarung mit der oder dem Beschäftigten.

Betriebsvereinbarung

Das hier vorgestellte und an Unternehmen angepasste Beispiel für eine Betriebsvereinbarung orientiert sich an zwei Dokumenten:

- zum einen am Runderlass des niedersächsischen Kultusministeriums zur Nutzung der privaten IT-Geräte von Lehrern bei der Verarbeitung der Schüler- und

Elterndaten.

- zum anderen an einem Muster für einen entsprechend Antrag mit individueller Verpflichtung, das das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung veröffentlicht hat (beides abrufbar unter https://ogy.de/nibis-private-it-systeme-1).

Allgemeiner Rahmen

Das angepasste Muster enthält die wesentlichen Bestandteile der Betriebsvereinbarung. Auf die üblichen Einleitungsklauseln (Platzhalter ist § 1) und Schlussklauseln (§ 8 ff) mit Geltungsbereich, Kontrollrechten des Betriebsrats, Beschwerdeverfahren und Kündigung der Betriebsvereinbarung verzichten wir.

Denn hierzu gibt es in vielen Unternehmen individuelle, über Jahre ausgefeilte Standardformulierungen.

Die Betriebsvereinbarung gibt den allgemeinen Rahmen vor. Das Muster finden Datenschutz-PRAXIS-Leser zum Herunterladen hier im Download-Bereich.

Die Betriebsvereinbarung regelt den allgemeinen Rahmen wie z.B. die Grundsätze (§ 2), die Details des Genehmigungsverfahrens und die Dauer der Genehmigung (§ 3). § 4 legt fest, welche Daten Beschäftigte maximal auf privaten IT-Systemen verarbeiten dürfen.

Dieser Paragraf muss firmenindividuell erstellt werden. Das Muster gibt ein Beispiel. Alle Daten, die hier nicht aufgeführt sind, dürfen Mitarbeiter nicht auf privaten IT-Systemen verarbeiten.

Technisch-organisatorische Maßnahmen

§ 5 führt die mindestens einzuhaltenden technisch-organisatorischen Maßnahmen auf. Diese Maßnahmen kann die IT-Abteilung und/oder die oder der Informationssicherheitsbeauftragte ergänzen und konkretisieren.

Das ermöglicht es, die Vereinbarung über einen längeren Zeitraum nicht zu ändern und trotzdem die Maßnahmen an technische Entwicklungen anzupassen (Stichwort: Stand der Technik).

Aktuelles Betriebssystem, aktueller Virenscanner

Wesentlich ist z.B., das Betriebssystem und jedwede genutzte Software aktuell zu halten und alle Sicherheitsupdates einzuspielen. Bei einem virengefährdeten Betriebssystem – definitiv Windows, aber auch MacOS – muss ein aktueller Virenscanner installiert sein und auf dem Laufenden gehalten werden (Signaturupdates).

Verschlüsselung

Alle dienstlichen Daten müssen verschlüsselt sein. Es empfiehlt sich eine grundlegende Verschlüsslung der Festplatten im Rechner (Bitlocker oder VeraCrypt bei Windows und FileVault 2 bei MacOS) mit einer Pre Boot Authentication (PBA). Bei einer PBA muss der Mitarbeiter das Verschlüsselungspasswort vor dem Start des Betriebssystems eingeben.

Das schützt allerdings nicht gegen berechtige weitere Nutzer eines Familien-PC. Denn alle berechtigten Nutzer eines solchen PC müssen das PBA-Passwort kennen.

Deshalb muss auf einem Familien-PC ein eigenes Nutzerkonto für die dienstliche Nutzung vorhanden sein. Die personenbezogenen Daten sollten außerdem nochmals separat verschlüsselt sein. Besonders einfach geht das mit einer Containerverschlüsselung wie VeraCrypt.

E-Mail-Zugriff nur über Web

Der Zugriff auf dienstliche E-Mails erfolgt nur über eine Webmail-Oberfläche. Das stellt sicher, dass alle E-Mails auf Servern des Unternehmens bleiben und nicht – wie bei der Synchronisation mit einem E-Mail-Client – automatisch auf dem privaten IT-System gespeichert werden. Zusätzlich sollte der Mitarbeiter den Browser-Cache regelmäßig (automatisch) löschen.

Der Zugriff auf Unternehmensressourcen muss über VPN-Verbindungen erfolgen. Soweit ein Beschäftigter direkt aus dem Homeoffice auf vom Unternehmen genutzte Cloud-Services zugreift, muss mindestens eine Transport-Verschlüsslung (TLS 1.2 oder besser) stattfinden.

Ideal ist nach wie vor ein Zugriff aus dem Homeoffice auf

eine zentrale Infrastruktur per Remote Desktop oder eine vergleichbare Lösung. In dem Fall erfolgt die Verarbeitung und Speicherung der Daten im Unternehmen. Der Mitarbeiter sieht nur die Anzeige.

Das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung stellt auf dem Niedersächsischen Bildungsserver (NiBiS) im Datenschutzportal allgemein verständliche technisch-organisatorische Vorgaben als Konkretisierung für Lehrer und Schulen zur Verfügung.

Das ist eine gute Ausgangsbasis für eigene Anpassungen. Die Vorgaben finden sich unter https://ogy.de/nibis-private-it-systeme-2.

Passen die Softwarelizenzen?
Ein weiterer Aspekt der Nutzung von privaten IT-Systemen ist die Notwendigkeit, die Software auf diesen Geräten für eine kommerzielle Nutzung zu lizenzieren. Microsoft nennt das in seinen Lizenzverträgen „kommerzielle, gemeinnützige oder Einnahmen erwirtschaftende Aktivitäten".

Nutzt ein Mitarbeiter sein privates IT-System für die berufliche Arbeit, müssen die Softwarelizenzen das auch erlauben.

Individuelle Vereinbarung
Der individuelle Zusatz zur allgemeinen Betriebsvereinbarung ist nötig, weil die erforderlichen Vereinbarungen über das hinausgehen, was sich in einer kollektiven Regelung abbilden lässt. Das betrifft etwa die Erlaubnis, die Wohnung zu betreten oder auf den privaten Rechner zuzugreifen.

Der Betriebsrat kann in einer Betriebsvereinbarung nicht für die Beschäftigten in Dinge einwilligen, die sich auf den privaten Besitz beziehen. Hier muss die/der Beschäftige einwilligen.

Der Inhalt der individuellen Vereinbarung ergibt sich direkt aus der Betriebsvereinbarung. Insofern wiederholen sich Texte aus der Betriebsvereinbarung in der individuellen Verpflichtung. Das stellt zudem sicher, dass der Inhalt der individuellen Vereinbarung mitbestimmt bleibt.

Es ist sinnvoll, die individuelle Vereinbarung mit einem Antrag auf Nutzung der privaten IT-Geräte zu verbinden. Dann gibt es nur ein Formular für diesen Zweck im Unternehmen.

Gibt es in einem Unternehmen keinen Betriebsrat, kann die Geschäftsleitung eine Dienstanweisung erlassen, die inhaltlich die Regelungen der Betriebsvereinbarung übernimmt, und sie im Rahmen des Direktionsrechts in Kraft setzen. Dann stützt sich die individuelle Vereinbarung auf die Dienstanweisung.

Quelle:
www.heise.de