Arbeiten von zu Hause

Auch im Homeoffice gilt die DSGVO

Arbeiten von zu Hause

In den letzten Monaten ist das Thema Homeoffice etwas in den Hintergrund geraten. Mit der Corona-Pandemie erlangt es jetzt einen außergewöhnlichen Stellenwert.

Für alle Datenschutz-Verantwortlichen und betroffenen Mitarbeiter soll dieser Artikel eine Hilfestellung sein, um den Homeoffice-Arbeitsplatz sicher zu gestalten. Denn wenn Homeoffice auch dabei hilft, das Corona-Virus einzudämmen, ist auch hier die Gefahr gegeben, sich einen Cyber-Virus einzufangen.

Mit „Homeoffice“ meine ich nicht nur das Arbeiten von zu Hause aus, sondern auch von jedem anderen denkbaren Ort, an dem eine Internetverbindung aufgebaut werden kann (mobiles Büro).

Das typische Homeoffice ist allerdings die Arbeit vom heimischen Schreibtisch aus. Und natürlich sind auch dort die datenschutzrechtlichen Anforderungen in vollem Umfang einzuhalten.

Auch im Homeoffice gilt die DSGVO

Verantwortlicher im Sinne des Art. 4 Nr. 7 der Datenschutzgrundverordnung bleibt auch beim Homeoffice der Geschäftsführer bzw. der Vorstand. Bei einer Datenübertragung von Firmenservern oder von der Unternehmens-Cloud auf das betreffende Endgerät handelt es sich nicht um eine Datenübertragung im Sinne der DSGVO. Sie benötigen also keine Rechtsgrundlage für die Übertragung der Daten ins Homeoffice oder das mobile Büro.

Geeignete technische und organisatorische Maßnahmen sind zwingend

Wenn es also keinen Unterschied macht, ob der Mitarbeiter zu Hause oder im Büro ist, liegt der entscheidende Unterschied in den technischen und organisatorischen Schutzmaßnahmen gemäß Art. 32 DSGVO.

Die Mitarbeiter müssen also grundsätzlich sicherstellen, dass keine unberechtigten Personen Kenntnis von betrieblichen Daten, insbesondere von personenbezogenen Daten erhalten.

Was im Büro schon allein durch eine Zutrittskontrolle sichergestellt werden kann, ist am heimischen Schreibtisch oder im mobilen Büro nicht so einfach zu gewährleisten.

In der eigenen Wohnung bewegen sich Familienmitglieder und Besucher, im mobilen Büro zusätzlich noch unbekannte Dritte. All diesen Gruppen muss der Zugriff auf die Informationen effektiv verwehrt werden.

Geeignete Maßnahmen hierfür sind z.B. ein individueller Zugriffsschutz und eine verschlüsselte VPN-Verbindung (Virtual Private Networks).

Ein VPN stellt sicher, dass die Daten nur über einen geschützten Transportweg transferiert werden, der unabhängig von einer gesicherten Internetverbindung selbst genügend Schutz bietet. Insbesondere durch die Verschlüsselung werden die Daten für eventuelle Angriffe während der Übertragung nutzlos.

Stellen Sie Spielregeln für das Ausdrucken auf

Aber nicht nur die Technik birgt Datenschutzrisiken. Kann der Mitarbeiter einen Drucker nutzen, muss er darauf achten, auch die Ausdrucke zu schützen. Sofern die Unterlagen personenbezogene Daten beinhalten, dürfen sie z.B. nicht einfach im Hausmüll entsorgt werden. Je nach Schutzgrad der Daten wird daraus schnell ein meldepflichtiger Datenschutz-Vorfall. Das gilt übrigens auch für handschriftliche Notizen. Während Arbeitgeber ihren Mitarbeitern im Büro geeignete Entsorgungsmöglichkeiten zur Verfügung stellen können, können derartige Vorkehrungen zu Hause fehlen.

Überlegen Sie als Verantwortlicher also, Ihrem Mitarbeiter einen Shredder (z.B. den Leitz-Mülleimer 2.0) für das Homeoffice zur Verfügung zu stellen.

Zudem sollten Sie Ihre Mitarbeiter dazu anhalten, die Ausdrucke sofort an sich zu nehmen und nicht im Drucker liegenzulassen.

Sensibilisierung der Mitarbeiter ist das A und O

Es ist also unerlässlich, die Mitarbeiter vorab durch geeignete Maßnahmen zu sensibilisieren und ihnen die Risiken aufzuzeigen, die sich durch einen sorglosen Umgang mit Unternehmensdaten im heimischen Umfeld ergeben können. Meist liegt die Gefahr darin, dass der Mitarbeiter sich in privater und gut vertrauter Umgebung nicht dem Risiko eines unbeobachteten Datenabgriffs ausgesetzt sieht. Diese Arglosigkeit kann, anders als im Büroumfeld, dazu führen, dass er sorgloser mit den Informationen umgeht.

Einsatz privater Geräte im Homeoffice

Der Einsatz von privater Hard- und Software (z.B. Notebooks, USB-Sticks, Speicherkarten, mobile Laufwerke) für betriebliche Zwecke und die Verwendung privater Datenträger (z.B. Disketten, CDs, Speichersticks) darf nur nach gesonderter Genehmigung durch Ihren IT-Verantwortlichen und für festgelegte Zwecke erlaubt werden.

Sie wünschen mehr Informationen oder eine persönliche Beratung?

+49 0711 40070720

info@barth-datenschutz.de

Nutzung betrieblicher Geräte für private Zwecke

Die Nutzung von betrieblicher Hard- und Software für private Zwecke und die Nutzung von betrieblichen mobilen Datenträgern an privaten Geräten sollten Sie untersagen. Gleiches gilt für die Überlassung an betriebsfremde Personen, also auch an Familienangehörige.

Ausnahmen bedürfen der Genehmigung durch den Vorgesetzten und der Freigabe durch die IT-Verantwortlichen.

1 Wechseldatenträger

Durch einen unvorsichtigen Umgang mit Wechseldatenträgern besteht auch die Gefahr, dass Schad- oder Spionagesoftware eingeschleppt wird. Wechseldatenträger können zudem bei einem Anschluss an Fremdsysteme ausspioniert werden und so die Vertraulichkeit von Unternehmensdaten gefährden. Deshalb muss der vertrauliche und sichere Umgang mit mobilen Datenträgern eindeutig geregelt werden.

2 Firewall und Internetschutz

Zusätzlich zu den zentralen Vorkehrungen werden alle PCs und Notebooks auch durch eine lokal installierte Firewall und den Internetschutz geschützt. Eine entsprechende Anleitung und Benutzerhinweise stehen zur Verfügung. Die Geräte sind damit auch bei einem Zugang zum Internet von externen Standorten aus entsprechend geschützt.

Um einen ständigen Schutz der Geräte zu gewährleisten, darf nur die von der IT-Abteilung freigegebene und installierte Sicherheitssoftware installiert und betrieben werden. Ferner darf die Konfiguration der Schutzsoftware nicht verändert, deaktiviert oder deinstalliert werden. Insbesondere dürfen die automatische Aktualisierung der Schutzsoftware nicht deaktiviert oder verändert und die Geräte nicht ohne aktuellen Schutz am Internet betrieben werden.

Die Konfiguration der Firewall und deren Funktionsfähigkeit sind von der IT-Abteilung in angemessenen Abständen zu überprüfen.

3 Diebstahl und Verlust von Datenträgern

Um Diebstählen vorzubeugen, sind Notebooks und Dockingstations beim mobilen Betrieb nach Möglichkeit zu sichern, z. B. mit einem Kabelschloss.

Jeder Diebstahl oder sonstiger Verlust von mobilen Geräten oder Datenträgern ist sofort dem Vorgesetzten und der zuständigen IT-Abteilung zu melden. Von diesen Stellen werden dann die weiteren Schritte eingeleitet.

4 Verhalten auf Reisen

Notebooks und sonstige mobile Datenträger dürfen auf Reisen, beispielsweise in Zügen, aber auch während der Sicherheitskontrollen auf Flughäfen und an sonstigen öffentlichen Plätzen nicht unbeaufsichtigt gelassen werden.

Notebooks dürfen nicht als Fluggepäck aufgegeben werden.

Notebooks sind auf Reisen als Handgepäck mitzuführen und möglichst verborgen zu tragen.

Notebooks dürfen nicht sichtbar in Fahrzeugen abgelegt werden. Bei

einer Verwahrung des Notebooks im Auto ist das Notebook nach Möglichkeit im Kofferraum mit einem Kabelschloss an der Karosserie zu befestigen.

Im Hotel müssen Notebooks oder sonstige mobile Datenträger möglichst mitgeführt oder im Hoteltresor verwahrt werden. Die Zimmertresore sind häufig nicht ausreichend sicher.

Bei der Nutzung von Taxi oder Mietwagen ist darauf zu achten, keine Datenträger im Fahrzeug zu vergessen.

Bei Auslandsreisen sind die jeweils geltenden besonderen Risiken, Vorkehrungen und Auflagen zu beachten.

Beim Arbeiten mit dem Notebook in Zügen oder in sonstigen einsehbaren Umgebungen ist auf einen ausreichenden Sichtschutz zu achten, z. B. durch Sichtschutzfolien, um ein Mitlesen durch unbefugte Personen zu verhindern. In öffentlichen Verkehrsmitteln dürfen keine personenbezogenen oder sonstigen sensiblen Daten verarbeitet werden.

Auf Reisen erfasste Daten und erstellte Verarbeitungsergebnisse sind laufend über eine sichere Verbindung auf den zentralen Systemen oder auf mobilen Datenträgern zu sichern. Die Sicherungsdatenträger sind zu verschlüsseln und getrennt vom Notebook zu verwahren.

FAZIT:

Homeoffice ist im heutigen Büroalltag ein fester Bestandteil. Aber insbesondere Sorglosigkeit im privaten Umfeld kann Ihre Mitarbeiter dazu verleiten, unachtsam mit den Unternehmensdaten umzugehen. Verantwortliche Stelle für diese Daten ist und bleibt der Arbeitgeber. Geeignete Awareness-Maßnahmen können Ihre Mitarbeiter auf die Gefahren hinweisen und einen sachgerechten Umgang mit den schutzwürdigen Informationen sicherstellen.

Entscheidende Bedeutung kommt beim Homeoffice der technischen Ausstattung zu. Die Verbindung vom Unternehmens-Laptop zum Server des Arbeitsgebers muss hinreichend abgesichert sein. Dabei ist stets die Verhältnismäßigkeit zu beachten.

Wenn Sie als Verantwortlicher diese Maßnahmen ernst nehmen und umsetzen, steht aus Sicht des Datenschutzes, der Informationssicherheit und der IT-Sicherheit einem mobilen Arbeitsplatz nichts im Wege.

Als Nutzer von Datenschutz365 erhalten Sie auf der Plattform alle notwendigen Hilfsmittel, um sämtliche hier beschriebenen Vorgaben und Hinweise umzusetzen.

Sie wünschen mehr Informationen oder eine persönliche Beratung?

+49 0711 40070720
info@barth-datenschutz.de

CHECKLISTE →
Homeoffice

CHECKLISTE Homeoffice

Bereich	Maßnahme	Inhalt
1. Datenschutz-Management	Regelwerk für die Arbeit im Homeoffice bzw. im mobilen Büro und Sicherstellung, dass alle betroffenen Mitarbeiter unterwiesen werden	• Kommunikationsarten (E-Mail, Internet, Fax, Mobiltelefon) • Datenklassifizierung: Welche Daten dürfen wie das Unternehmen verlassen? • Sicherheitsanforderungen (z. B. Regelungen zu Datensicherung, Virenschutz, Firewall, Verschlüsselungsoptionen, in jedem Fall bei sensiblen Daten) • Möglichkeiten für die Datenübermittlung: VPN, E-Mail, mobile Datenträger (USB), Ausdrucke • Vernichtung von Papier und elektronischen Datenträgern • Ggf. Regelungen zur Fernwartung • Aushändigung der Richtlinien an die betroffenen Mitarbeiter
	Erstellen einer Richtlinie für sicheres Arbeiten im Homeoffice	• Benennung von Sicherheitszielen • Schutzbedarf der bearbeiteten Informationen und diesbezügliche Risiken
2. Schulung / Unterweisung	Unterweisung aller betroffenen Mitarbeiter	• Einweisung der Mitarbeiter • Mitarbeiterschulungen, z. B. über den Umgang mit ausgedruckten Dokumenten
3. Dokumentation	Dokumentation der Ausgabe und Rücknahme von unternehmenseigener Soft- und Hardware (z. B. Laptop, Drucker) an und vom jeweiligen Mitarbeiter	
	Ggf. Vereinbarung eines Zutrittsrechts zum Heimarbeitsplatz zur Durchführung von Kontrollen und für den Zugriff auf Dokumente	

CHECKLISTE Homeoffice

Bereich	Maßnahme	Inhalt
4. Zugriffskontrolle	Identifizierungs- und Authentisierungsmechanismus	
	Protokollierung	• Authentisierungen • Zugriffe • Veränderungen • Administratortätigkeiten • Fehler
	Administrationsrechte	• Regelungen und Kontrolle • Einschränkung der Benutzerumgebung für den Mitarbeiter
5. Kryptographie	Verschlüsselung	• Mobile Endgeräte • Mobile Datenträger • E-Mails
6. Physische und Umgebungssicherheit	Arbeitsplatz-Sicherungsmaßnahmen	• Wer ist zutrittsberechtigt? • Welche Sicherungsmaßnahmen gibt es?
	Clean-Desk-Policy	• Gedruckte Dokumente vor Einsicht Unbefugter schützen
	Bildschirm	• Passwortgeschützter automatischer Bildschirmschoner • Bildschirm-Blickschutz-Folie
7. Betriebssicherheit	Updates	• Installiert und aktuell
	Virenschutz	• Installiert und aktuell
	Firewall	• Aktiviert
	Boot-Schutz	• Aktivierung empfehlenswert
	Datensicherung	• Regelungen und Kontrolle
8. Kommunikationssicherheit	Trennung von Daten	• Trennung privater Daten von unternehmenseigenen Daten
7. Rechtssicherheit	Beauftragung von freien Mitarbeitern	• Ggf. Verpflichtung auf die Vertraulichkeit der Daten