Homeoffice-Richtlinie Muster

[Anwendungshinweise (vor Verwendung entfernen): *Dieses Dokument regelt ausschließlich datenschutzrechtliche Aspekte im Rahmen einer Homeoffice-Richtlinie und ist daher nicht als eine Art Anordnung zu Homeoffice verstehen. Dieses Muster ist auf die jeweilige Verarbeitungssituation und die betrieblichen Belange anzupassen. Dieses Dokument geht davon aus, dass die betreffenden Beschäftigten durch den Arbeitgeber mit dienstlichen Endgeräten ausgestattet worden sind/werden und die private Nutzung dienstlicher Endgeräte ausgeschlossen ist. Bitte beachten Sie, dass wir als ds² Sie ausschließlich zum Datenschutz beraten. Zu anderen betroffenen Rechtsbereichen, insbesondere zur betrieblichen Mitbestimmung, dürfen wir Sie nicht beraten.]*

1. Allgemeine Bedingungen

Gegenstand dieser Homeoffice-Richtlinie des [Arbeitgebers] sind ausschließlich Aspekte des Datenschutzes. Sie ergänzen die bei [Arbeitgeber] dazu bereits vorhandenen Regelungen. Im Zweifel und/oder bei Verständnisfragen, ist der jeweilige Vorgesetzte zu konsultieren.

Eine Tätigkeit kann nur im Rahmen des Homeoffice erledigt werden, sofern die jeweilige Tätigkeit des einzelnen Beschäftigten dafür auch geeignet ist, insbesondere aus der Sicht des Datenschutzes.

2. Arbeitsumgebung

Die Homeoffice-Arbeit hat ausschließlich am Wohnsitz des/der Beschäftigten zu erfolgen. Zur Verrichtung der Homeoffice-Arbeit darf nur ein Raum genutzt werden, der abschließbar ist. Sämtliche personenbezogenen Daten, insbesondere betriebliche Daten, Informationen und sonstigen Dokumente, sind unter Verschluss aufzubewahren. Dies gilt auch für etwaige Identifikationstechnik wie Transponder, Chipkarten, o.ä.

Der Arbeitsplatz ist so zu strukturieren, dass keine privaten und dienstlichen Daten miteinander vermischt werden.

Es ist untersagt, Dritten (z.B. Familienmitgliedern, Mitbewohnern, Besuchern) Zugriff auf und/oder Zugang zu der betrieblichen EDV und/oder Unterlagen/Informationen, gleich in welcher Form, zu gewähren. Auch die Weitergabe der Daten an Unbefugte ist untersagt. Die Unterlagen dürfen zudem nicht unbeaufsichtigt gelassen werden.

Der Arbeitsplatz ist so zu wählen, dass andere Personen den Bildschirm nicht einsehen können – auch nicht durch ein Fenster. Ggf. können Sichtschutzfolien unterstützen.

3. Grundsätze für den Umgang mit personenbezogenen Daten

Der/Die Beschäftigte ist verpflichtet, alle seine/ihre oder seine/ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten auch bei der Arbeit im Homeoffice einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen.

Es gelten die Grundsätze zur Verarbeitung personenbezogener Daten gem. Art. 5 DSGVO. Insbesondere dürfen personenbezogenen Daten nicht zu anderen als den betrieblichen Zwecken verwendet werden.

Für dienstliche Telefonate oder ähnliche Gespräche (z.B. Webkonferenzen o.ä.) sind ungestörte Bereiche aufzusuchen, damit die Vertraulichkeit des Gesprächs gewährleistet werden kann.

Dokumente in Papierform dürfen nicht mit ins Homeoffice genommen werden. Diese sind einzuscannen und dann via VPN zu nutzen.

[Alternativ: Jede Mitnahme von betrieblichen/personenbezogenen Daten bedarf der vorherigen Zustimmung des jeweiligen Vorgesetzen. Sofern eine Mitnahme erfolgt, muss ein Transport in verschlossenen Behältnissen erfolgen und die betrieblichen/personenbezogenen Daten dürfen nicht unbeaufsichtigt sein.]

Dokumente sollten grundsätzlich nicht im Homeoffice ausgedruckt werden. Sollte dies für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich sein, dürfen diese nicht im Hausmüll entsorgt werden. Der/Die Beschäftigte hat die ausgedruckten Dokumente ins Büro mitzubringen und nach Erledigung wie üblich dort abzulegen bzw. datenschutzkonform zu vernichten. Dies gilt auch für handschriftliche Notizen o.ä.

Dokumente. Eine dauerhafte Verwahrung im Homeoffice ist unzulässig. Die Vernichtung personenbezogener Daten richtet sich nach der Organisationsanweisung „XY“.

Bei einem Datenschutzvorfall ist unverzüglich gemäß der Organisationsanweisung „Datenschutzvorfälle“ vorzugehen.

Bei Anfragen oder Beschwerden betroffener Personen ist gemäß den Organisationsanweisungen „Betroffenenrechte“ und „Beschwerdemanagement“ vorzugehen.

4. Grundsätze der Nutzung von IT-Systemen im Homeoffice

Zur Verrichtung der Tätigkeit im Homeoffice sind ausschließlich die dienstlichen Geräte (Dienst-Notebook und Dienst-Smartphone) zu nutzen. Die Nutzung von privaten Geräten zu dienstlichen Zwecken ist nicht erlaubt. Die Sicherheitssoftware der Dienstgeräte muss jederzeit aktiviert sein. Die Umgehung oder das Deaktivieren von Sicherheitsmaßnahmen ist untersagt. Datenträger müssen nach dem Stand der Technik verschlüsselt sein, bei Rückfragen melden Sie sich bitte bei der IT-Abteilung. An die dienstlichen Endgeräte darf keine private Hardware (z.B. Festplatten, USB-Sticks) angeschlossen werden.

Die Verbindung der dienstlichen Geräte mit dem privaten Heimnetzwerk ist gestattet. Der Internetzugriff kann alternativ auch über den Hotspot des Dienst-Smartphones erfolgen. Das genutzte Endgerät muss so eingerichtet werden, dass es mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden ist. Das WLAN sollte so eingerichtet sein, dass das Einwählen nur mit einem sicheren Passwort erfolgen kann. Die Nutzung von öffentlich zugänglichen WLAN ist nicht gestattet.

Bei Verlassen des Homeoffice muss sichergestellt werden, dass kein Dritter auf betriebliche Daten zugreifen kann, der Zugang zum System ist auch bei kurzer Unterbrechung zwingend zu sperren. Das Entsperren des Bildschirms hat per Eingabe des Nutzernamens und eines sicheren Passworts zu erfolgen. Bei der Wahl des Passworts sind die Anweisungen aus der „Passwort-Richtlinie“ zu beachten.

Auch betriebliche Endgeräte sind vor Wegnahme besonders zu schützen. Sofern der Beschäftigte die Gerätschaften nicht benutzt, ist etwa der Raum abzuschließen. Fenster des Raumes sind zu verschließen.

Der Zugriff auf die Daten hat per VPN-Verbindung zu erfolgen. Die am PC erstellten und bearbeiteten Dokumente sind über den VPN-Zugang direkt auf dem Firmen-Server und nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern.

Im Hinblick auf die Installation von Software auf den mobilen IT-Systemen oder bei EDV-Auffälligkeiten gilt die Richtlinie „IT-Richtlinie für Nutzer“.

[Ggf.] 5. Sanktionen

Ein Verstoß gegen diese Regelung kann nicht nur eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden, sondern insbesondere auch eine strafrechtliche oder datenschutzrechtliche Pflichtverletzung darstellen, die z.B. mit Geldbuße bedroht ist.]

Unterschrift [Name des/der Beschäftigten]	Unterschrift [Arbeitgeber]