Home – Office – Richtlinie der [Organisation]

Diese Entwurfsvorlage ggf. individuell anpassen und in Folge bitte juristisch prüfen lassen

§ 1. Gegenstand und Geltungsbereich der Richtlinie

Ziel dieser Home – Office - Richtlinie ist es, eine datenschutzrechtskonforme Verarbeitung von personenbezogenen Daten, insbesondere deren Vertraulichkeit, Integrität und Verfügbarkeit im Home - Office zu gewährleisten.

(1) Wenn Beschäftigte der **[Organisation]**, sofern dies erlaubt oder angeordnet wurde (z.B. auch im Rahmen der sog. „Corona-Krise“), an einem Telearbeitsplatz („Home - Office“) arbeiten, so gelten die Vorgaben dieser „Home – Office - Richtlinie“, die verbindlich einzuhalten sind.

(2) Diese Home – Office - Richtlinie gilt für alle Beschäftigten und alle Standorte der **[Organisation]**, wenn und soweit personenbezogene Daten im Home - Office verarbeitet werden.

(3) Um das Ziel der Home – Office - Richtlinie zu erreichen, dürfen Vorgesetzte an die Beschäftigten auch ergänzende Weisungen erteilen, denen ebenso Folge zu leisten ist.

(4) Alle bereits geltenden allgemeinen betrieblichen Bestimmungen und Anweisungen zu Datenschutz und Datensicherheit gelten auch im Home - Office und sind einzuhalten. Sollte diese Bestimmungen im Widerspruch zu dieser Richtlinie stehen, so gehen die Bestimmungen dieser Home – Office - Richtlinie den allgemeinen Bestimmungen vor.

§ 2. Umgang mit personenbezogenen Daten und Sicherheitsmaßnahmen

(1) Auch im Home-Office bleiben vertragliche Weisungsrechte der **[Organisation]** bestehen und alle betrieblichen Daten, Informationen und Unterlagen, auf die die Beschäftigten von ihrem Home - Office aus Zugriff haben, verbleiben im Hoheitsbereich der **[Organisation]**.

(2) Es dürfen keine betrieblichen Daten oder Unterlagen, insbesondere personenbezogene und andere vertrauliche Daten an Dritte weitergegeben, Dritten bekannt werden (bspw. durch Ausdrucke oder Einsichtnahme am Monitor), unbefugt kopiert oder zu anderen, als betrieblichen Zwecken, verwendet werden.

(a) Insbesondere dürfen keine Passwörter oder andere Zugangsberechtigungen zur betrieblichen IT (z.B. Chipkarten) zugänglich gemacht werden. Es ist darauf zu achten, dass die Passwörter nicht einsehbar oder zugänglich (z. B. auf Zetteln) notiert sind oder Chipkarten im Lesegerät verbleiben.

(b) Insbesondere ist darauf zu achten, dass Personen, die im selben Haushalt leben (Familienmitglieder, sonstige Mitbewohner) und Besucher (Gäste, Handwerker) keinen Zugang oder Zugriff auf die betrieblichen Daten haben.

(c) Wird der Home – Office - Arbeitsplatz verlassen (auch bei nur kurzem Verlassen), so muss sichergestellt sein, dass keine unbefugte Person auf die Daten zugreifen kann.

- Grundsätzlich sollte daher der als Home - Office genutzte Raum abschließbar sein und bei Nichtnutzung durch den Beschäftigen abgeschlossen werden.
- Beim Verlassen des Home – Office - Arbeitsplatzes ist in jedem Fall unverzüglich der verwendete Computer so zu sperren (z.B. durch Bildschirmsperre), so dass zur Entsperrung ein Passwort eingeben werden muss, das nur dem Beschäftigen bekannt ist.
- Werden Papier-Akten genutzt, so sind diese grundsätzlich in einem Schrank einzuschließen oder der Home – Office - Raum abzuschließen, es sei denn der Beschäftigte ist allein zu Hause und verlässt seinen Home – Office - Arbeitsplatz nur kurzzeitig.

(d) Grundsätzlich dürfen keine Dokumente mit vertraulichen Informationen (z.B. personenbezogene Daten) im Home - Office ausgedruckt werden, es sei denn, dies ist für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich. In diesem Fall ist

dafür Sorge zu tragen, dass die Dokumente direkt vor Ort auf geeignete Art und Weise vernichtet werden können (Aktenvernichter) und vernichtet werden, sobald diese nicht mehr benötigt werden.

§ 3. Sicherheitsmaßnahmen bei der Übertragung von Daten und Transport von Akten und Datenträgern

(1) Es ist sicherzustellen, dass die Datenübertragung zwischen dem Home – Office - Arbeitsplatz und der **[Organisation]** (auch bei Terminal-Zugriff) verschlüsselt gemäß dem aktuellen Stand der Technik erfolgt. Beschäftigte, die nicht sicher sind, ob die Daten verschlüsselt übertragen werden, müssen dies bei der IT-Abteilung erfragen.

(2) Die Mitnahme von betrieblichen Daten und Akten erfordert die vorherige Zustimmung des Vorgesetzten.

(3) Unterlagen, Datenträger, Dokumente und Akten, die mitgenommen werden, dürfen nur in verschlossenen Behältnissen transportiert (z.B. verschlossener Aktenkoffer oder Kiste) und zu keinem Zeitpunkt unbeaufsichtigt gelassen werden. Es dürfen auch keine Datenträger oder Unterlagen im Fahrzeug zurückgelassen werden.

(4) Bei der Mitnahme von Daten muss sichergestellt sein, dass die Daten auf den verwendeten Datenträgern nach dem aktuellen Stand der Technik verschlüsselt sind.

§ 4. Verarbeiten und Speichern von Daten

(1) Daten dürfen grundsätzlich nur auf von betrieblichen Laufwerken oder Datenspeichern von Endgeräten oder Ordnern/Verzeichnissen von zentralen IT-Systemen bzw. Servern gespeichert werden, die im Eigentum oder Besitz der **[Organisation]** stehen oder durch sie zugelassen bzw. freigegeben sind. Untersagt ist daher grundsätzlich die Speicherung und sonstige Verarbeitung betrieblicher Daten auf privaten Speichermedien (z.B. Laufwerken, Smartphones, USB-Sticks o.ä.).

(2) Die Daten dürfen grundsätzlich nicht auf lokalen Festplatten, sondern nur in den Ordnern/ Verzeichnissen der betrieblich freigegebenen IT-Systemen bzw. Servern gespeichert werden. Hintergrund ist, dass andernfalls bei Auskunftsrechten von betroffenen Personen über die bei der **[Organisation]** verarbeiteten personenbezogenen Daten dieses nicht vollständig nachvollzogen werden kann, da die Daten überall noch lokal gespeichert sind. Hiervon darf nur ausnahmsweise in dem Fall abgewichen werden, wenn die Internet-Anbindung an die Server bzw. zentralen IT-Systeme nicht möglich ist. In diesen Ausnahmefällen ist es gestattet, die Daten auf den im Home - Office genutzten Geräten lokal zu speichern, wenn sichergestellt ist, dass die Daten verschlüsselt gespeichert werden. Sind Beschäftigte sich nicht sicher, ob die Daten auf den von ihnen genutzten Datenträgern verschlüsselt gespeichert werden, so können sie sich an den IT-Support wenden. Werden Daten ausschließlich lokal gespeichert, so müssen diese bei nächster Gelegenheit auf die üblicherweise dafür vorgesehenen zentralen IT-Systeme bzw. Server der **[Organisation]** übertragen, sowie die lokale Speicherung anschließend sicher gelöscht werden.

§ 5. Sicherheitsmaßnahmen IT

(1) Störungen und Auffälligen bei der IT-Nutzung sind unverzüglich der IT-Abteilung mitzuteilen.

(2) Es dürfen keine Sicherheitsmaßnahmen umgangen oder deaktiviert werden oder sonstige technische Änderungen an den, durch die **[Organisation]** zur Verfügung gestellten Geräten vorgenommen werden. Insbesondere darf Software nur durch die IT-Abteilung oder in Absprache mit der IT-Abteilung installiert und genutzt werden.

§ 6. Verpflichtende Meldung von Datenpannen

Mögliche Datenschutzvorfälle (Datenpannen) sind unverzüglich dem betrieblichen Datenschutzbeauftragten und/oder dem Verantwortlichen zu melden. Insbesondere ist ein Datenschutz

vorfall dann gegeben, wenn Grund zu der Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein könnte. Ein Datenschutzvorfall liegt auch vor, wenn Grund zu der Annahme besteht, dass Dritte unbefugt Zugang oder Zugriff zu personenbezogenen Daten haben oder hatten.

§ 7. Ausnahmen

In begründeten Einzelfällen können durch die **[Organisation]** Ausnahmen von den zuvor genannten Regelungen dieser Richtlinie genehmigt werden. Die genehmigten Ausnahmen sind mit den entsprechenden Gründen zu dokumentieren.

§ 8. Hinweis auf Sanktionen bei Verstößen gegen diese Richtlinie

Verstöße gegen diese Richtlinie können arbeitsrechtliche Folgen haben (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung). Zudem können Verstöße gegen diese Richtlinie Unterlassungs- und Schadenersatzansprüche nach sich ziehen.

Dokument erstellt/veröffentlicht [Datum] / [ORT]

ALTERNATIV:

[Beschäftigte]	**[Organisation]**
Ort, Datum, Unterschrift	**Ort, Datum, Unterschrift**