Anlage 5 zur DV Mobiles Arbeiten

Datenschutz-Richtlinie zur DV Mobiles Arbeiten

1. Gegenstand und Geltungsbereich der Richtlinie

1.1 Ziel dieser Richtlinie ist es, eine datenschutzrechtskonforme Verarbeitung von personenbezogenen Daten, insbesondere deren Vertraulichkeit, Integrität und Verfügbarkeit, an einem mobilen Arbeitsplatz zu gewährleisten.

1.2 Sind Beschäftigte der Universität Greifswald an einem mobilen Arbeitsplatz tätig, so sind die Vorgaben dieser Richtlinie verbindlich einzuhalten.

1.3 Um das Ziel dieser Richtlinie zu erreichen, dürfen Vorgesetzte an die Beschäftigten auch ergänzende Weisungen erteilen, denen ebenso Folge zu leisten ist.

1.4 Alle bereits geltenden allgemeinen dienstlichen Bestimmungen und Anweisungen zu Datenschutz und Datensicherheit gelten auch an einem mobilen Arbeitsplatz. Sollten die allgemeinen Bestimmungen im Widerspruch zu dieser Richtlinie stehen, so gehen die Bestimmungen dieser Richtlinie den allgemeinen Bestimmungen vor.

2. Umgang mit personenbezogenen Daten und Sicherheitsmaßnahmen

2.1 Auch an einem mobilen Arbeitsplatz bleiben vertragliche Weisungsrechte der Universität bestehen und alle dienstlichen Daten, Informationen und Unterlagen, auf die die Beschäftigten von ihrem mobilen Arbeitsplatz aus Zugriff haben, verbleiben im Hoheitsbereich der Universität.

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

2.2.1 Insbesondere dürfen keine Passwörter oder andere Zugangsberechtigungen zur dienstlichen IT zugänglich gemacht werden. Es ist darauf zu achten, dass die Passwörter nicht auf einsehbaren oder zugänglichen Zetteln notiert werden.

2.2.2 Darüber hinaus ist dafür Sorge zu tragen, dass keine unbefugten Personen Zugang oder Zugriff auf die dienstlichen Daten haben. Dies ist auch bei kurzzeitigem Verlassen des Arbeitsplatzes sicherzustellen.

2.2.2.1 Beim Verlassen des Arbeitsplatzes ist in jedem Fall unverzüglich der verwendete Computer zu sperren (z.B. durch Bildschirmsperre), so dass zur Entsperrung ein Passwort eingeben werden muss, welches nur dem*der Beschäftigten bekannt ist.

2.2.2.2 Werden Papier-Akten genutzt, so sind diese grundsätzlich in einem Schrank einzuschließen oder der Raum abzuschließen, es sei denn, der*die Beschäftigte ist allein vor Ort und verlässt den Arbeitsplatz nur kurzzeitig.

2.2.3 Dienstliche Unterlagen dürfen nur für die Zeit des direkten Gebrauchs an den mobilen Arbeitsplatz mitgenommen werden und sind nach Erfüllung des Zwecks unverzüglich zurückzubringen.

2.2.3 Grundsätzlich dürfen keine Dokumente mit vertraulichen Informationen (z.B. personenbezogenen Daten) am mobilen Arbeitsplatz ausgedruckt werden, es sei denn, dies ist für die Erledigung von dienstlichen Aufgaben zwingend erforderlich.

2.2.4 Die Vernichtung vertraulicher Unterlagen und Vorgänge hat ausschließlich innerhalb der Räumlichkeiten der Universität zu erfolgen.

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

3.1 Es ist sicherzustellen, dass die Datenübertragung zwischen dem mobilen Arbeitsplatz und der Universität (auch bei Terminal-Zugriff) verschlüsselt gemäß dem aktuellen Stand der Technik erfolgt. Beschäftigte, die nicht sicher sind, ob die Daten verschlüsselt übertragen werden, haben dies beim Universitätsrechenzentrum Greifswald zu erfragen.

3.2 Die Mitnahme von dienstlichen Daten und Akten erfordert die vorherige Zustimmung des*der Vorgesetzten.

3.3 Bei dem Transport von Unterlagen oder Datenträgern zwischen der Dienststelle und dem mobilen Arbeitsplatz ist sicherzustellen, dass diese zu keinem Zeitpunkt unbeaufsichtigt gelassen werden oder für Dritte zugänglich sind. Der Verbleib von Unterlagen oder Datenträgern in Fahrzeugen ist grundsätzlich untersagt und ausschließlich in zwingend erforderlichen Fällen kurzzeitig zulässig (z.B. Abholung von Kindern aus einer Betreuungseinrichtung). In solchen Fällen dürfen keine Unterlagen oder Datenträger sichtbar im Fahrzeug zurückgelassen werden.

3.4 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

Daten dürfen grundsätzlich nur in den Ordnern und Verzeichnissen der zentralen IT-Systeme bzw. auf den Servern des Universitätsrechenzentrums Greifswald gespeichert werden. Untersagt ist daher grundsätzlich die Speicherung und sonstige Verarbeitung dienstlicher Daten auf privaten PC und Speichermedien (z.B. Laufwerken, Smartphones, USB-Sticks o.ä.) sowie auf externen nicht von der Universität betriebenen Plattformen (Cloud-Computing). Der Empfang und Versand dienstlicher E-Mails unter Nutzung eines privaten E-Mail-Kontos ist unzulässig.

5. Sicherheitsmaßnahmen IT

5.1 Störungen und Auffälligkeiten bei der IT-Nutzung sind unverzüglich dem Universitätsrechenzentrum Greifswald mitzuteilen.

5.2 Es dürfen keine Sicherheitsmaßnahmen umgangen oder deaktiviert werden oder sonstige technische Änderungen an den durch die Universität zur Verfügung gestellten Geräten vorgenommen werden. Insbesondere darf Software nur durch das Universitätsrechenzentrum oder in Absprache mit diesem installiert werden.

6. Verpflichtende Meldung von Datenpannen

Mögliche Datenschutzvorfälle (Datenpannen) sind unverzüglich dem behördlichen Datenschutzbeauftragten zu melden. Ein Datenschutzvorfall ist dann gegeben, wenn Grund zu der Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein könnte. Ebenso liegt ein

Datenschutzvorfall 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 Universität Greifswald Ausnahmen von den zuvor genannten Regelungen dieser Richtlinie genehmigt werden. Anträge sind an das Datenschutzbüro (ref-datenschutz@uni-greifswald.de) zu richten. 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.