Not-Home-Office
Hinweise und Hilfestellungen zum Datenschutz

Die Corona-Pandemie verändert das Alltagsleben. Auch der Arbeitsplatz hat sich für viele Beschäftigte der UPB momentan zumindest teilweise in den häuslichen Bereich verlagert. Dies ermöglicht uns, auch in dieser Zeit die Arbeitsfähigkeit der Universität Paderborn zu erhalten.

Ein großes Dankeschön an alle, die dies spontan und oftmals ohne große Vorbereitungen möglich gemacht haben.

Der Datenschutz stellt uns alle unter diesen Bedingungen vor besondere Herausforderungen. Sie finden daher im Folgenden Hinweise und Hilfestellungen, wie der Datenschutz und die Datensicherheit auch im Not-home-office berücksichtigt werden kann.

Physischer Transport von Papierdokumenten und mobilen Geräten

Dienstliche Papierdokumente und mobile Geräte, auf denen sich personenbezogene Daten und/oder vertrauliche Informationen befinden, müssen zwischen Dienststelle und dem häuslichen Arbeitsplatz und umgekehrt gesichert transportiert werden. Bitte finden Sie eine Möglichkeit, diese abgeschlossen zu transportieren und wählen Sie den direkten Weg zwischen dem häuslichen und dienstlichen Büro und umgekehrt.

Zutritts- und Zugriffsschutz

Mögliche Maßnahmen sind:

Wenn möglich, sollte der häusliche Arbeitsplatz nur von Ihnen genutzt werden. Bitte arbeiten Sie nicht in der Öffentlichkeit (bspw. in Cafés).

Personenbezogene Daten und vertrauliche Informationen, die Rahmen der dienstlichen Aufgabenerfüllung verarbeitet werden oder wurden, dürfen **nicht mit privaten Daten vermischt** werden. Vorzugsweise ist ein dienstlicher Rechner zu verwenden (Notebook). Für den Fall, dass **private Geräte** genutzt werden, sind dienstliche Inhalte mit personenbezogenen Daten sowie vertraulichen Informationen gegen den Zugriff durch andere Personen zu schützen. In diesem Fall richten Sie bitte für den dienstlichen Gebrauch ein eigenes Konto ein und schützen Sie dieses Konto durch ein Passwort. Bitte nutzen Sie möglichst aktuelle Betriebssysteme mit Sicherheitsupdates. Aktuelle Virenscanner schützen Sie gegen schädliche Software.

Die Daten sollten möglichst **verschlüsselt gespeichert werden** und nach **Übertragung** in das dienstliche Netz, sicher **gelöscht werden.** (Vergessen Sie nicht, auch den Papierkorb zu leeren. Alle Daten sollten nach Ende der Heimarbeitsphase sicher gelöscht werden. Die dienstlich zur Verfügung gestellte **IT-Ausrüstung** kann **nicht für private Zwecke** genutzt werden.

Die **Verbindung** zur UPB muss über gesicherte Verbindungen erfolgen. Die meisten Anwendungen (E-Mail, PAUL, PANDA, …) lassen sich nur verschlüsselt nutzen (HTTPS). Zusätzlich schützt eine **VPN-Verbindung** die Daten. Einige Dienste lassen sich von außerhalb der Uni auch nur mit VPN-Verbindung nutzen.

Stellen Sie bitte sicher, dass sämtliche dienstliche sowie für diese Zwecke genutzten Geräte und Speichermedien vor dem **unbefugtem Zugriff und Zugang** zu den darauf befindlichen personenbezogenen Daten sowie vertraulichen Informationen geschützt sind. In diesem Zusammenhang ist es auch wichtig, den **Bildschirm** so einzustellen, dass Haushaltsangehörige und weitere Dritte (bspw. durch Fenster im Erdgeschoss) die Daten und Informationen nicht einsehen können.

Wenn Sie Ihren Arbeitsplatz verlassen, aktivieren Sie bitte eine **Bildschirmsperre,** die nur mit einem Passwort aufgehoben werden kann, das nur Ihnen bekannt ist. Hilfreich ist auch, zusätzlich eine automatische Bildschirmsperre einzurichten, die das Sperren spätestens nach 5 Minuten aktiviert

Die **Installation von neuer Software** auf den dienstlichen Geräten darf nur in Rücksprache mit der Dienststelle erfolgen.

Um Datenverlust durch unbefugten Zugriff sicherzustellen, sollen externe Datenträger (externe Festplatten, USB-Sticks) mit denen Daten transportiert werden, ebenfalls verschlüsselt werden.

E-Mails aus der ZV und vom IMT heraus und umgekehrt, also auch zwischen IMT und ZV können problemlos versandt werden.

Andere dienstliche E-Mails, deren Inhalt personenbezogene Daten und/oder vertrauliche Informationen aufweisen, sind möglichst mit **Verschlüsselungstechnik** nach dem Stand der Technik zu versenden, wenn sie den Bereich des E-Mail-Servers verlassen.

Bitte leiten Sie dienstliche E-Mails niemals auf **private E-Mail-Postfächer** weiter (d.h. keine Nutzung von gmail, gmx etc. für dienstliche Mails).

Ein Austausch über personenbezogene Daten sowie vertrauliche Informationen mit dienstlichem Inhalt darf ebenfalls nicht über **Messenger-Dienste** (bspw. WhatsApp) oder andere externe Dienste stattfinden.

Drucken Sie Dokumente, die dienstlichen Inhalt mit personenbezogenen Daten sowie vertraulichen Informationen, aufweisen, möglichst nicht an Ihrem **häuslichen Arbeitsplatz aus.** Sollte dies für die Erledigung von dienstlichen Aufgaben zwingend erforderlich sein, ist dafür Sorge dafür zu tragen, dass die Ausdrucke sofort entnommen und direkt vor Ort geeignet abgelegt oder vernichtet werden. Bitte trennen Sie in diesen Fällen den Drucker vom Internet.

Aufbewahrung von Papierdokumenten und mobilen Geräten

Dienstliche Papierdokumente und mobile Geräte, auf denen sich personenbezogene Daten sowie vertrauliche Informationen befinden müssen **geschützt aufbewahrt** werden. Dies bedeutet, dass andere Haushaltsangehörige oder Dritte keinen Zugang haben können.

Speicherung

Die Speicherung von personenbezogenen Daten sowie weiteren vertraulichen Informationen, die im Rahmen der dienstlichen Aufgabenerfüllung verarbeitet werden oder wurden, muss grundsätzlich in den **Verzeichnissen/Ordnern von Servern bzw. in den zentralen IT-Systemen der UPB** erfolgen, die für den Benutzer freigegeben sind.

Sollte eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen temporär nicht möglich ist, kann eine Ausnahme gemacht werden: In diesen Fällen darf eine **lokale Speicherung** der Daten und Informationen auf den am häuslichen Arbeitsplatz verwendeten Geräten, stattfinden, wenn sichergestellt ist, dass diese Daten auf den verwendeten Datenträgern **verschlüsselt** gespeichert werden. Bitte übertragen Sie die Daten dann bei nächstmöglicher Gelegenheit.

Vernichtung von Papierdokumenten

Müssen Papierdokumente, die dienstlichen Inhalt mit personenbezogenen Daten sowie vertraulichen Informationen aufweisen vernichtet werden, wählen Sie bitte **nicht Ihren Papierkorb**. Eine datenschutzgerechte Vernichtung muss sich an die Anforderungen der DIN 66399-2 orientieren (bspw. Aktenvernichter mit der Mindestsicherheitsstufe 3). Stehen solche Möglichkeiten am häuslichen Arbeitsplatz nicht zur Verfügung, bewahren Sie die Dokumente bitte verschlossen auf und entsorgen Sie sie bei nächster Möglichkeit datenschutzgerecht am dienstlichen Arbeitsplatz.

Telefonie

Sind Sie auf ein privates Telefon angewiesen, dann richten Sie nach Möglichkeit eine Weiterleitung der dienstlichen Rufnummer ein.

Werden die Rufnummern der eingehenden Anrufe übertragen, löschen Sie bitte diese regelmäßig auf Ihrem Endgerät.

Telefonieren Sie mit Ihrem eigenen privaten Endgerät, raten wir Ihnen, die Nummer bei **ausgehenden Anrufen zu unterdrücken.**

Meldepflicht bei Datenschutzvorfall

Mögliche Datenschutzvorfälle sind unverzüglich nach Bekanntwerden der Dienststelle und der Datenschutzbeauftragten zu melden. Eine **Kontaktaufnahme** sollte insbesondere bereits dann erfolgen, wenn die Annahme besteht, dass die Vertraulichkeit von Daten, gefährdet sein kann und/oder das Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten und/oder vertraulichen Informationen haben oder hatten (bspw. ein verlorenes oder im Zug vergessenes Notebook, eine gestohlene/verlorene Tasche mit Datenträgern und/oder dienstlichen Papierdokumenten, gestohlenes/verlorenes Notebook etc.) Festgestellte Sicherheitslücken sind der Dienststelle ebenfalls sofort anzuzeigen Die Meldung eines (Informationssicherheits-)Vorfalls erfolgt über das **Ticketsystem der UPB** unter https://www.uni-paderborn.de/universitaet/informationssicherheit/informationssicherheitsvorfall/.

Wir hoffen, Ihnen damit wertvolle Hinweise gegeben zu haben. Passen Sie gut auf sich auf und bleiben Sie gesund.

Als Ansprechpartnerin steht Ihnen die Datenschutzbeauftragte Eva-Maria Wicker zur Verfügung.

Paderborn, 5.6.2020