Empfehlung zum Datenschutz bei vorübergehendem Home-Office

Die folgenden Hinweise sollen Ihnen helfen, Aspekte des Datenschutzes und der Datensicherheit zu berücksichtigen, wenn in Ihrem Betrieb in größerem Umfang Tätigkeiten ins Home-Office verlagert werden. Die Hinweise richten sich in ihrem Aufbau nach den Empfehlungen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (Handbuch Betriebliche Pandemieplanung). Sie unterscheiden daher die Phasen vor, während und nach einer Pandemie.

Die Maßnahmen sind allgemein zu berücksichtigende Empfehlungen und an die konkreten Gegebenheiten und Risiken anzupassen.

Planung, Information und Einweisung der betroffenen Mitarbeiter

- Eine Auslagerung von Datenbeständen oder Datenverarbeitungen ist immer mit Risiken verbunden. Diese können im Verhältnis zu den überwiegenden Interessen des Gemeinwohls und der Gesundheit gerechtfertigt werden, sollten aber auf das erforderliche Maß begrenzt werden. Konkret bedeutet dies zum Beispiel, dass nur die Fernzugriffsrechte eingeräumt werden und die Unterlagen (Originale oder Kopien) mitgenommen werden, die für die Tätigkeiten im Home-Office notwendig sind.
- Informieren Sie insbesondere Mitarbeiter, die bisher nicht von zu Hause gearbeitet haben, über die **bestehenden Betriebsvereinbarungen, Richtlinien und Arbeitsanweisungen** zum Home-Office.
- Weisen Sie erneut auf die **Meldepflichten für Datenpannen und Sicherheitsvorfälle** hin und stellen Sie sicher, dass die Meldewege funktionsfähig sind.
- Soweit Ihren Mitarbeitern Arbeitsgerät (Laptops etc.) zur Verfügung gestellt wird oder es erforderlich ist, erweiterte Zugriffsrechte einzuräumen, informieren Sie diese auch über die hiermit verbundenen **Risiken** und weisen Sie sie in einen sicheren Umgang ein.
- Stellen Sie sicher, dass ausreichend **Ansprechpartner** für Rückfragen zur Verfügung stehen.
- Protokollieren und dokumentieren Sie nach Möglichkeit die Auslagerung und Anpassungen von Datenverarbeitungen (Dokumente, Hardware, Prozesse).

Risiken und Maßnahmen während der Auslagerung

- Sorgen Sie für einen sicheren **Transport von Daten und Datenträgern** (verschlossene Behältnisse, verschlüsselte Festplatten, nicht unbeaufsichtigt lassen…).
- Grundsätzlich sind nur vom Arbeitgeber zur Verfügung gestellte oder genehmigte **Hard- und Software z**u verwenden. Bezüglich der Nutzung privater Rechner sollte eine gesonderte Regelung („Bring-your-own-device“) getroffen werden.
- Eine sichere **Verbindung** zur Unternehmens-IT-Infrastruktur ist zu gewährleisten (z.B. VPN).
- Die Zugriffe sollten nur nach individueller **Anmeldung** erfolgen und systemseitig protokolliert werden. Nutzen Sie nach Möglichkeit eine Mehr-Faktor-Authentifzierung.
- Soweit für Emails und Anhänge eine **verschlüsselte Übertragung** vorgesehen ist, ist dies auch im Homeoffice umzusetzen.

- Personenbezogene und vertrauliche Daten sind grundsätzlich **verschlüsselt zu speichern**.
- Es ist sicherzustellen, dass Dritte (Familienmitglieder, Besucher) keinen **Zugang** zu den vertraulichen Informationen haben (passwortgesicherte Bildschirmsperre, abschließbarer Schrank/Raum...). Besonders schutzwürdige Informationen dürfen nur verarbeitet werden, wenn der Bildschirm von Dritten nicht einsehbar ist.
- Dokumente sollten nur lokal **gespeichert oder ausgedruck**t werden, wenn dies für die Erledigung betriebsbedingter Aufgaben zwingend erforderlich ist. Ausdrucke mit vertraulichen Informationen dürfen nicht im Hausmüll entsorgt werden. Wenn eine sichere Vernichtung nicht möglich ist, sind die Dokumente sicher zu verwahren bis sie im Betrieb entsorgt werden können.

Maßnahmen bei Rückkehr zum Normalbetrieb

- Daten, die auf externen Geräten gespeichert wurden, werden bei nächster Gelegenheit auf die üblichen **Datenspeicher** übertragen.
- Nicht mehr erforderliche Kopien sind gemäß der betrieblichen Vorgaben zu **vernichten** (z.B. Datentonne).
- Dokumente, Prozesse, Inventar und Rechtekonzepte sind in den **Normalbetrieb** zurückzuführen. Auch dieser Prozess ist zu dokumentieren.