Regeln zum Datenschutz bei dezentraler Arbeit

Präambel
Diese Regeln sollen gewährleisten, dass die Bestimmungen zum Schutz von personenbezogenen Daten bei einer dezentralen Arbeit (im Weiteren „Telearbeit") eingehalten werden. Dazu gehört insbesondere die Gewährleistung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten.

Sofern Beschäftigten der Katholischen Hochschule für Sozialwesen Berlin (KHSB) die Telearbeit erlaubt wird, sind diese Regeln von den betreffenden Beschäftigten einzuhalten.

§ 1 Geltungsbereich
(1) Diese Regeln gelten für die Verarbeitung personenbezogener Daten durch Beschäftigte der KHSB in Telearbeit.

(2) Diese Regeln verpflichten alle Beschäftigten der KHSB zur Einhaltung der hier festgelegten Vorgaben, soweit eine Verarbeitung personenbezogener Daten in Telearbeit erfolgt.

§ 2 Umgang mit personenbezogenen Daten in der Telearbeit
(1) Beschäftigte sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Vorgaben oder Anweisungen im Umgang mit personenbezogenen Daten auch bei der Telearbeit einzuhalten.

(2) Beschäftigten ist es untersagt, personenbezogene Daten oder sonst vertrauliche Daten an Dritte (im Sinne von Außenstehenden oder unbeteiligten Personen, s. § 4 Nr. 12 des Gesetzes über den Kirchlichen Datenschutz, KDG) weiterzugeben, sie Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken), sie auf eigenen Speichermedien abzuspeichern, unbefugt zu kopieren oder zu anderen als dienstlichen Zwecken zu verwenden.

(3) Beschäftigte sind verpflichtet, Verletzungen des Schutzes von personenbezogenen Daten („Datenpannen") unverzüglich an den Kanzler Martin Wrzesinski (E-Mail: kanzler@khsb-berlin.de) oder den betrieblichen Datenschutzbeauftragten (Oliver Stutz, datenschutz nord GmbH, E-Mail: office@datenschutz-nord.de) zu melden. Eine Datenpanne liegt insbesondere vor, wenn Grund zu der Annahme besteht, dass Dritte unbefugt Zugriff auf personenbezogene Daten haben oder hatten.

§ 3 Technische und organisatorische Sicherheitsvorkehrungen in der Telearbeit
(1) Telearbeit birgt Risiken für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten. Zur Minimierung dieser Risiken sind die nachfolgenden Grundsätze bei der Verarbeitung von personenbezogenen Daten in der Telearbeit einzuhalten.

(2) Beschäftigte dürfen in der Telearbeit ausschließlich die von der KHSB bereitgestellte oder genehmigte Hard- und Software verwenden oder müssen den Zugang zum virtuellen Arbeitsplatz in der Hochschule nutzen. Private Geräte, die Beschäftigte für diesen Zugang verwenden, müssen über mindestens diese Sicherheitsmaßnahmen verfügen: aktuelle System- und Anwendungssoftware, Schutz vor Schadsoftware, aktivierte Firewall sowie ein wirksamer Zugangsschutz (Passwort, Fingerabdruck oder Gesichtserkennung).

(3) Die Speicherung von Daten hat grundsätzlich auf den Servern bzw. zentralen IT-Systemen der KHSB zu erfolgen. Bei der Verwendung von Hardware, die die Hochschule bereitgestellt hat, dürfen personenbezogene Daten auf den in der Telearbeit verwendeten Geräten gespeichert werden, wenn eine Verschlüsselung der Daten gegeben ist (z.B. Festplattenverschlüsselung BitLocker).

(4) Bei der Nutzung des privaten Internetanschlusses müssen die von den Beschäftigten verwendeten mobilen Geräte entweder durch ein Kabel oder ein verschlüsseltes WLAN (WPA2 oder WPA3) mit dem privaten Netzwerk verbunden werden. Jede Datenübertragung zwischen dem Arbeitsplatz in der Telearbeit und den Servern bzw. zentralen IT-Systemen der KHSB muss nach dem Stand der Technik verschlüsselt sein (VPN, Verschlüsselung der Verbindung, möglichst Verwendung einer Zwei-Faktor Authentifizierung über Passwort und Zertifikat/ SMS-PIN/ OTP/ Token).

(5) Bei der Telearbeit ist sicherzustellen, dass unbefugte Personen keinen Zugang zu den im Zusammenhang mit der Beschäftigung verarbeiteten Daten erhalten. Dies gilt insbesondere für Personen, die mit den Beschäftigten in einem Haushalt leben. Nach Arbeitsende sollten alle vertraulichen Unterlagen, mobile Geräte und Datenträger verschlossen aufbewahrt werden.

(6) Der Telearbeitsplatz sollte so gewählt werden, dass unbefugte Personen den Bildschirm nicht einsehen können. Beschäftigte müssen bei Verlassen des Telearbeitsplatzes ihren Bildschirm sperren. Die Bildschirmsperre muss mit einem Passwort gesichert sein.

(7) Befinden sich in der Wohnung der Beschäftigten Sprachassistenten wie z. B. Amazon Alexa, Google Home, Microsoft Cortana, Apple Siri oder Samsung Bixby, sind bei diesen während der Telearbeit die Mikrofone zu deaktivieren.

(8) Die Telearbeit mit Akten oder sonstigen Papierdokumenten sowie ein Ausdruck von Dokumenten mit personenbezogenen Daten sollte grundsätzlich nicht erfolgen. Sollte dies zur Aufgabenerfüllung gleichwohl erforderlich sein (z. B. bei der Korrektur von Hausarbeiten oder Klausuren), haben die Beschäftigten für die Telearbeit für eine angemessene Sicherung der Akten und sonstigen Papierdokumente Sorge zu tragen (z. B. Transport in verschlossenen Behältnissen, Aufbewahrung in einem verschlossenen Schrank). Private und dienstliche Papierdokumente dürfen nicht miteinander vermischt werden. Nicht mehr benötigte Papierdokumente sind datenschutzgerecht zu vernichten.

§ 4 Folgen bei Verstößen

Ein Verstoß gegen diese Regeln kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Martin Wrzesinski, 14.04.2020