



Richtlinie Datenschutz (alternierende) Telearbeit der Fachhochschule Bielefeld in der Fassung vom 17.12.2019

1. Basis

Das Präsidium hat in der Datenschutz-Leitlinie vom 01.10.2014 in der novellierten Fassung vom 05.07.2018 (Amtliche Bekanntmachungen/Verkündungsblatt 2018-22, S.145-148) den Grundstein für das Datenschutzmanagementsystem (DSMS) der FH Bielefeld gelegt. Auf Basis der Datenschutz-Leitlinie können spezielle Anforderungen an konkrete Verarbeitungsprozesse mit Richtlinien geregelt werden. Das Richtlinie Datenschutz (alternierende) Telearbeit präzisiert die Pflichten der Teilnehmenden an (alternierender) Telearbeit.

2. (alternierende) Telearbeit an der FH Bielefeld

Die Einrichtung von Arbeitsplätzen außerhalb der Dienst- und Arbeitsräume und die Anbindung dieser Arbeitsplätze über das Internet an die Rechner der Hochschule stellen besondere Anforderungen an die Informationssicherheit und den Datenschutz bei der alternierenden Telearbeit. Die räumliche Trennung des (alternierenden) Telearbeitsplatzes von der Dienststelle und die Einbindung in das häusliche Umfeld dürfen weder den Datenschutz noch die Informationssicherheit beeinträchtigen.

Die für die Hochschule geltenden Bestimmungen für die Bereiche Datenschutz und Informationssicherheit gelten uneingeschränkt für die alternierende Telearbeit.

3. Geltungsbereich

Diese Richtlinie gilt für die alternierende Telearbeit in allen Bereichen der Fachhochschule Bielefeld.

4. Arbeitsplatz für die alternierende Telearbeit

Für den häuslichen Arbeitsplatz ist grundsätzlich die Nutzung eines eigenen Zimmers vorgesehen. Im besten Fall soll der häusliche Arbeitsplatz von der übrigen Wohnung durch eine abschließbare Tür abtrennbar sein, damit sich dort befindliche Unterlagen und IT-Systeme außerhalb der Bereiche befinden, in denen sich weitere Bewohner oder Besucher aufhalten. Bei spontanen Besuchen kann der Arbeitsplatz kurzfristig verlassen und vor unbefugtem Zugriff geschützt werden.

5. Anforderungen an den Umgang mit Arbeitsunterlagen und Daten

Die Beschäftigten dürfen notwendige Arbeitsunterlagen unter Berücksichtigung der gebotenen Sicherheitsmaßnahmen von der Dienststelle zum Telearbeitsplatz bringen und dort aufbewahren; dies ist auf das unbedingt erforderliche Maß und den zeitlichen Umfang zu beschränken.

Die Bearbeitung von Daten, die als streng vertraulich eingestuft sind, ist am Telearbeitsplatz nicht zulässig.

Der Transport der Akten erfolgt auf dem direkten Weg zwischen betrieblicher und häuslicher Arbeitsstätte in geschlossenen Behältnissen. Dabei muss stets sichergestellt sein, dass diese nicht abhandenkommen oder beschädigt werden. Dies kann beispielsweise durch eine ausreichend stabile und verschlossene Tasche gewährleistet werden. Transparente Behältnisse sind ungeeignet, weil Unbefugte den Inhalt zur Kenntnis nehmen könnten. Während des Transports dürfen die Behältnisse niemals unbeaufsichtigt abgestellt werden.

Vertrauliche Daten und Informationen sowie Passwörter werden so geschützt, dass unbefugte Dritte diese nicht einsehen, nutzen oder zerstören können.

Hierzu gehört beispielsweise beim Verlassen des Arbeitsplatzes das Sperren oder Herunterfahren des PCs oder das Einschließen mobiler Datenträger und Unterlagen.

Von außen erreichbare Einstiegsmöglichkeiten in die Wohnung sind beim Verlassen des Arbeitsplatzes für alternierende Telearbeit zu verschließen, dies betrifft insbesondere nach außen gehende Türen und Fenster.

Zu vernichtende Daten und sonstige Arbeitsunterlagen werden ausschließlich über den zur Verfügung gestellten Aktenvernichter entsorgt.

Auf den Schutz von Daten und Informationen gegenüber Dritten – hierzu gehören auch Familienangehörige und sonstige im Haushalt lebende Personen sowie jede Person, die sich im Haushalt aufhält – ist bei der häuslichen Arbeitsstätte besonders zu achten. Alle Daten und Informationen sind von der bzw. dem Beschäftigten so zu schützen, dass Dritte keine Einsicht und/oder

keinen Zugriff haben. Die Aufbewahrung der Akten am häuslichen Arbeitsplatz hat deshalb in einem abschließbaren Schrank oder Ähnlichem zu erfolgen.

6. Regeln für den Notfall/Meldeprozess

(1) Unerklärliche Veränderungen an Hard- oder Software sowie alle Vorfälle, die die Vertraulichkeit oder Sicherheit zu schützender Daten beeinträchtigt haben oder gefährden könnten, sind unverzüglich nach dem im Intranet der FH Bielefeld beschriebenen Meldeprozess

<https://www.fh-bielefeld.de/beschaefigte/intern/mitteilungen/dsb/it-sicherheitsvorfaelle-datenschutzverletzung>

an die E-Mail-Adresse

informationssicherheitsvorfall@fh-bielefeld.de

zu melden.

(2) Zudem ist die bzw. der Vorgesetzte unverzüglich zu informieren.

7. Verstöße

Bei Verstößen gegen diese Richtlinien führt der oder die Vorgesetzte ein Gespräch mit der bzw. dem Beschäftigten mit dem Ziel, die Verstöße abzustellen und eine Wiederholung zu vermeiden.

8. Inkrafttreten

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung im Verkündungsblatt/Amtliche Bekanntmachung der FH Bielefeld in Kraft.

Bielefeld, den 22.01.2020

Die Präsidentin

Die Vizepräsidentin für
Wirtschafts- und
Personalverwaltung

gez. I. Schramm-Wölk

gez. G. Schnier

Prof. Dr. Ingeborg Schramm-Wölk

Gehsa Schnier