Hinweise zur datenschutzrechtlichen Verantwortung des Arbeitgebers im Kontext von Home-Office und Telearbeit

Projekt Rechtsinformationsstelle Digitale Hochschule NRW, Leitung Prof. Thomas Hoeren

Bearbeiter: wissenschaftliche MitarbeiterInnen Maximilian Wellmann (DFN), Malin Fischer (RiDH), Julian Albrecht (RiDH)

Veröffentlicht am 28. Mai 2020

A. Fragestellung

Was müssen Hochschulen als Arbeitgeber aus datenschutzrechtlicher Perspektive bei der Einrichtung professioneller HomeOffice-Strukturen/Telearbeitsmöglichkeiten beachten?

B. Hintergrund

Die Corona-Krise erfordert ein in weiten Teilen „digitales Sommersemester“, welches die Hochschulen in NRW ad hoc organisieren müssen, teilweise ohne sich zuvor stark mit der Digitalisierung der Lehre beschäftigt zu haben. Zugleich müssen auch die vielen Beschäftigten der Hochschulen zumindest zeitweise ins Homeoffice geschickt werden. Besonders mit Blick auf eine zweite Ansteckungswelle ist es ratsam – soweit noch nicht geschehen – sich mit der Schaffung professioneller Homeoffice/Telearbeitsmöglichkeiten zu beschäftigen. Dazu gehört auch der Datenschutz.

C. Inhaltsverzeichnis

D. Zusammenfassung

Auch im Homeoffice/bei der Telearbeit verarbeitet der Arbeitnehmer personenbezogene Daten. Zudem ergeben sich gegenüber der Arbeit vor Ort beim Arbeitgeber zusätzliche Gefährdungslagen. Währenddessen bleibt der Arbeitgeber Verantwortlicher im Sinne der Datenschutzgrundverordnung. Daher muss er Vorkehrungen im Hinblick auf ein ausreichendes Datenschutzniveau treffen. Unterlässt er dies, haftet er für Datenschutzverstöße durch seine Arbeitnehmer.

Solche Vorkehrungen können rechtlich gut in einer Homeoffice-Richtlinie als Zusatzvereinbarung zum Arbeitsvertrag oder in einer Betriebsvereinbarung getroffen werden. Eine Auswahl der empfehlenswerten Maßnahmen:

- Sensibilisierung der Mitarbeiter für Gefahren und gute Verhaltensweisen
- Schulungen
- Bereitstellung der Endgeräte mit entsprechenden Voreinstellungen
- Virtual Private Network-Zugänge
- Bereitstellung von Bildschirmschutzfolie
- Container Apps bei Nutzung privater Geräte für dienstliche Zwecke

E. Ausarbeitung

Die folgenden Hinweise sollen der datenschutzkonformen Remote-Arbeit von zuhause dienen. Zur effektiven Durchsetzung bietet es sich an, diese Hinweise in der gesamten betroffenen Betriebsstruktur zu kommunizieren.

I. Begriff und Abgrenzung

Der Begriff des Homeoffice kann synonym mit dem der Telearbeit behandelt werden. Die Arbeitsleistung wird dabei in den Räumlichkeiten des Arbeitnehmers an einem festen Telearbeitsplatz erbracht, der durch feste Informationsverarbeitungs- und Kommunikationsmittel mit der IT-Infrastruktur des Arbeitgebers verbunden ist. Vereinzelt wird hiervon das mobile Arbeiten, das ein ortsunabhängiges Arbeiten von unterwegs ermöglicht, abgegrenzt.[1] Für die nachfolgende Einordnung wird der Begriff der Telearbeit umfassend sowohl für alle Arbeiten

[1] Vgl. BfDI abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.pdf?__blob=publicationFile (zuletzt abgerufen: 26.5.2020).

von zu Hause als auch unterwegs verstanden (so auch BSI, Tipps für sicheres mobiles Arbeiten[2]).

II. Problemstellung

Im Gegensatz zum Arbeiten im Unternehmen ergeben sich bei der Telearbeit verschiedene tatsächliche Probleme, die eine datenschutzrechtliche Implikation aufweisen können. Anders als am Arbeitsplatz im Unternehmen wird infrastrukturell oftmals nicht das gleiche Sicherheitsniveau am Telearbeitsplatz herrschen können. Aufgabe des Verantwortlichen ist es aber, ein angemessenes Schutzniveau im Hinblick auf die Rechte und Freiheiten der Arbeitnehmer und den Schutz ihrer personenbezogenen Informationen zu gewährleisten. Problemstellungen sind dabei in Zugangsmöglichkeiten sensitiver (personenbezogener) Daten durch Familienangehörige und Dritte angelegt. Ein klassischer Fall ist z.B. das mobile Arbeiten im Zug, bei dem der unmittelbare Sitznachbar in vielen Fällen einen freien Blick auf den Bildschirm hat und so vertrauliche Daten Dritten bekannt werden können (Shoulder Surfing). Bei der Verwendung mobiler IT-Systeme besteht zudem im Vergleich zu stationären Arbeitsplätzen eine erhöhte Gefahr des Verlustes personenbezogener Daten durch Zerstörung, Diebstahl oder eine klimatisch falsche Aufbewahrung. Bei all diesen Herausforderungen bleibt das Unternehmen in der datenschutzrechtlichen Verantwortung. Auch bei einer Verarbeitung der Daten in der Sphäre des Arbeitnehmers ändert sich am Status des Arbeitgebers als Verantwortlicher i.S.d. Art. 4 Nr. 7 DS-GVO nichts, da die Verarbeitung im betrieblichen Kontext auf „Weisung“ des Arbeitgebers gem. Art. 29 DS-GVO erfolgt. Konkret ergibt sich hieraus für den Verantwortlichen die Pflicht für sämtliche Verarbeitungsvorgänge die im Zusammenhang mit dem Arbeitsprozess stehen, Vorkehrungen im Hinblick auf die Datensicherheit zu treffen. Dies entspringt nicht zuletzt einer haftungsrechtlichen Motivation, da im Außenverhältnis der einzelne Arbeitnehmer als Beschäftigter i.S.v. § 26 Abs. 8 BDSG als Teil des Unternehmens zu behandeln ist, sodass der Arbeitgeber für datenschutzrechtliche Verstöße seiner Angestellten einzustehen hat.

III. Datenschutzrechtliche Vorgaben des Art. 32 DS-GVO

Um den datenschutzrechtlichen Anforderungen adäquat zu begegnen, ist es die Aufgabe des Verantwortlichen, die Vorgaben aus Art. 32 DS-GVO zu beachten und durch konkrete Schutzmaßnahmen umzusetzen. Im Fokus des Art. 32 DS-GVO steht für den Verantwortlichen zunächst abstrakt die Sicherstellung eines dem Risiko angemessenen Schutzniveaus der Datensicherheit während der Verarbeitung. Welche Schutzmaßnahmen im Einzelfall durch den Verantwortlichen ergriffen werden müssen, ist das das Ergebnis einer Einzelfallabwägung nach

---

[2] Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf;jsessionid=AD0EB8E3DA5185A87AAFF9EAEA83BF21.2_cid503?__blob=publicationFile&v=9 (zuletzt abgerufen: 26.5.2020).

den Kriterien des Art. 32 Abs. 1 DS-GVO. Dabei sieht Art. 32 Abs. 1 lit. a) – d) DS-GVO einen nicht abschließenden Regelbeispielskatalog vor, der folgende Maßnahmen auflistet:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die zu ergreifenden Schutzmaßnahmen unterliegen einem Verhältnismäßigkeitsvorbehalt, wodurch die Pflicht zur Implementierung angemessener Schutzmaßnahmen für den Verantwortlichen auf ein wirtschaftlich zumutbares Maß begrenzt wird.

IV. Implementierung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO

Überträgt man die normativen Anforderungen des Art. 32 DS-GVO auf den Sachverhalt der Telearbeit, kommen eine Vielzahl technischer und organisatorischer Maßnahmen in Betracht. Zu empfehlen ist die Implementierung einer unternehmensweit einheitlichen Regelung zur Telearbeit, z.B. in Form einer Homeoffice-Richtlinie. In der Umsetzung bietet sich hier je nach Größe und Struktur des Unternehmens eine Betriebsvereinbarung oder ein Zusatz zum Arbeitsvertrag an. Für den Arbeitgeber bewirkt dies den Vorteil, dass er hierdurch einerseits seinen Rechenschaftspflichten gegenüber der zuständigen Aufsichtsbehörde aus Art. 5 Abs. 2 DS-GVO nachkommen kann und er sich andererseits vertraglich gegenüber dem Arbeitnehmer auf die Einhaltung der statuierten Pflichten berufen kann. Im Rahmen einer Homeoffice-Richtlinie können eine Vielzahl von technisch organisatorischen Maßnahmen seitens des Verantwortlichen ins Werk gesetzt werden (eingehend BSI, Tipps für sicheres mobiles Arbeiten). Adressat des Art. 32 Abs. 1 DS-GVO ist ausschließlich der Verantwortliche und nicht der Nutzer selbst. Für den Verantwortlichen bietet es sich an, die Maßnahmen in zwei Kategorien aufzuteilen. In der ersten Kategorie können organisatorische Maßnahmen getroffen werden, die den Telearbeiter sensibilisieren und zu einem eigenen datensicheren Handeln veranlassen. In der zweiten Kategorie sind technische Maßnahmen durch den Verantwortlichen selbst zu treffen. In dieser Kategorie wird auch der Unterschied virulent, ob dem Telearbeiter Endgeräte seitens des Arbeitgebers zur Verfügung gestellt werden oder ob es sich um eine Bring Your Own Device (BYOD) Lösung handelt.

1. Organisatorische Maßnahmen

Als organisatorische Maßnahme kann die Sensibilisierung der Telearbeiter im Hinblick auf die Gefahren, die durch den unangemessenen Umgang mit personenbezogenen Daten, die unsachgemäße Vernichtung von Daten oder eine unsichere Kommunikation entstehen können, eingeordnet werden. Wird eine Homeoffice-Richtlinie verabschiedet, kann diese in Verbindung mit Schulungen dafür sorgen, dass kritische Anwendungskontexte adressiert werden und Arbeitnehmern durch datenschutzkonformes Handeln ein angemessenes Datenschutzniveau i.S.d. Art. 32 DS-GVO sichern. Spezifisch sind Telearbeiter deshalb dahingehend zu sensibilisieren, dass ein unbefugter Dritter zu keinem Zeitpunkt Zugriff auf dienstliche Unterlagen erlangen darf, was u.a. durch ein regelmäßiges Sperren der Hardware auch bei nur kurzfristiger Abwesenheit und eine entsprechend verschließbare Einrichtung am Ort der Telearbeit (z.B. Rollcontainer, in den ein Laptop eingeschlossen werden kann; Safe im Hotel) zu gewährleisten ist. Auch ist ein Mithören der dienstlichen Kommunikation zu unterbinden. In diesem Kontext sollten auch Sprachassistenten auf privaten mobilen Endgeräten o.ä., die möglicherweise Daten aufzeichnen, ausgeschaltet werden. Der Arbeitnehmer ist zudem darauf hinzuweisen, regelmäßig Datensicherungen vorzunehmen, um einem Verlust von Daten vorzubeugen. Ideal ist hier die fortlaufende Speicherung im Netz der Institution, sodass auf eine lokale Speicherung nicht zurückgegriffen werden muss. Ist es notwendig, Daten lokal zu speichern, empfiehlt sich nur eine verschlüsselte Speicherung z.B. über VeraCrypt. In der Homeoffice-Richtlinie sollte auch geklärt werden, ob und wie Telearbeiter institutionsfremde IT-Systeme/Netze nutzen dürfen. Geht es darum, analog vorliegende Kopien zu entsorgen, ist darauf hinzuwirken, dass sensitive Informationen nicht achtlos im Hausmüll, sondern nach der Rückkehr ins Büro im betriebsinternen Müll entsorgt werden. Sämtliche dieser skizzierten Maßnahmen liegen dabei in der Handlungssphäre des Telearbeiters und können dementsprechend nur durch diesen umgesetzt werden. Kommt der Telearbeiter diesen Maßnahmen nicht nach, kann sich der Verantwortliche dennoch exkulpieren, wenn er über das Inkraftsetzen der Homeoffice-Richtlinie nachweisen kann, dass er die Mitarbeiter entsprechend sensibilisiert hat.

2. Technische Maßnahmen im Überblick

Werden die zu nutzenden Endgeräte durch den Arbeitgeber zur Verfügung gestellt, bestehen im Vergleich zu BYOD Lösungen weitreichendere Möglichkeiten des Verantwortlichen in Bezug auf die Implementierung technischer Maßnahmen. Zu seinem Pflichtenkreis zählen aber generell die „Härtung“ des organisationseigenen IT-Systems, z.B. durch das Einspielen aktueller Software-Patches und AV-Signaturen sowie dem Einsatz einer Firewall. Auch eine Reduzierung der Zugangsmöglichkeiten auf die Server der Institution auf ein Minimum gehört hierzu.

a) Bereitstellung der Endgeräte durch den Arbeitgeber

Der Verantwortliche kann durch entsprechende (Vor-) Einstellungen wie einer Verschlüsselung der Geräte schon a priori ein hohes Datensicherheitsniveau sichern. Dies ist zwingend, weil die Gefahr des Verlustes, insbesondere durch Diebstahl oder Zerstörung höher ist, als im direkten Vergleich zum Arbeitsplatz im Büro. Zu den weiteren Maßnahmen zählen ferner die Errichtung eines sicheren Fernzugriffs auf das Netz der Institution, z.B. über Virtual Private Networks (VPN). Die Einrichtung eines Support und Reporting Systems, das den Telearbeiter bei technischen Problemen unterstützt und bei einem Verlust von Geräten hilft, sollte vorgesehen werden. Diese Maßnahme steht im direkten Zusammenhang mit einem vorzusehenden Fernzugriff, der es ermöglicht auf das Gerät zuzugreifen und einen Datenabfluss an unberechtigte Dritte zu verhindern.

Sinnvoll kann es zudem sein, dem Arbeitnehmer Bildschirmschutzfolien zur Verfügung zu stellen, die dieser beim öffentlichen Arbeiten in Zügen oder Flugzeugen aber auch in den eigenen Räumlichkeiten einsetzen kann. Im Zusammenspiel mit den Maßnahmen, die in der Sphäre des Arbeitnehmers liegen (siehe 1.) kann hierdurch ein angemessenes Schutzniveau erreicht werden.

b) Bring Your Own Device

Besondere Anforderungen ergeben sich bei BYOD Lösungen. Diese werden im Hinblick auf ihre Vereinbarkeit mit dem Datenschutzrecht teilweise sehr kritisch gesehen (vgl. ZD-Aktuell 2020, 04405). Der Verantwortliche verliert beim Einsatz privater Geräte eine Vielzahl der skizzierten technischen Einflussmöglichkeiten. Technisch gesehen ist ein Zugang zum Netz der Institution über einen VPN-Zugang zwingend zu ermöglichen. Müssen personenbezogene Daten lokal gespeichert werden, sind diese zu verschlüsseln. Auch die Möglichkeit zur Fernlöschung ist einzuräumen. Voraussetzung all dieser Maßnahmen ist eine Trennung der privaten und technischen Daten, da ansonsten sämtliche Maßnahmen auch die privaten Inhalte des Arbeitnehmers betreffen würden. Dies käme aber einer gesteigerten Eingriffsintensität in die Rechte und Freiheiten der betroffenen Person gleich, was mit den Zwecken der Verarbeitung (betriebliche Erfordernisse) nicht mehr zu rechtfertigen ist. Technisch lässt sich dieses Trennungsgebot durch Container Apps umsetzen, mit denen die Daten so sortiert werden, dass der Zugriff auf den jeweiligen Bereich beschränkt wird. Die dienstlichen Daten werden dabei wie in einem Container eingeschlossen und können verschlüsselt über einen Web-Dienst, durch den Arbeitgeber administriert werden (*Hoppe*, in: Kramer, IT-Arbeitsrecht, 2. Aufl. 2019, Rn. 691).

3. Zusammenfassung technischer und organisatorischer Maßnahmen

In Bezug auf die Datensicherheit sind danach exemplarisch folgende technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO zu treffen, die bestenfalls vertraglich in einer

Homeoffice Richtlinie zu formalisieren sind (vgl. *Hoppe*, in: Kramer, IT-Arbeitsrecht, 2. Aufl. 2019, Rn. 689):

- Zugangskontrolle (u.a. Passwortschutz zum Ausschluss einer Nutzung durch unbefugte Dritte; am Stand der Technik ausgerichtet, Zwei-Faktor Authentifizierung)
- Weitergabekontrolle (Uploadverbot dienstlicher Daten auf unternehmensfremde Server; Fernlöschungsrecht)
- Eingabekontrolle (Protokollierung vorgenommener Datenveränderungen)
- Auftrags- und Verfügbarkeitskontrolle (regelmäßige Backups)
- Strukturierte und verschlüsselte Verwaltung von Passwörtern durch den Nutzer
- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Verschlüsselungsfunktionen von E-Mail Programmen nutzen
- Trennungsgebot für BYOD (technisch bewirkte physische Trennung des Speicherorts von dienstlichen und privaten Daten)

4. Einrichten eines DSGVO-konformen Videokonferenzdienstes

Zur reibungslosen Kommunikation der Beschäftigten ist das Angebot eines hochschuleigenen Videokonferenzsystems unerlässlich. Dabei sind verschiedene DSGVO-Vorgaben zu beachten.

Hierzu können wir auf unseren kürzlich veröffentlichten (18.05.20) datenschutzrechtlichen Leitfaden verweisen, indem wir am Beispiel des Dienstes Zoom zeigen, wie unter Beachtung bestimmter Schritte und Vorkehrungen, ein DSGVO-konformes Angebot geschaffen werden kann. Beachten Sie jedoch, dass das Datenschutzniveau und die relevanten Vertragsunterlagen jedes Dienstes individuell zu prüfen ist. Andere Dienste konnte wir bisher aus Kapazitätsgründen nicht prüfen.

Die Datei des Leitfadens heißt: Rechtsinformationsstelle DigitaleHochschule_Datenschutzrechtlicher Leitfaden Zoom Angebot durch Hochschulen NRW_18-05-20.doc und wurde per Newsletter versandt. Auf Anfrage können wir sie Ihnen nochmals zusenden.