Arbeiten im Home-Office

Basic-To-Do´s

Durch die Corona-Pandemie sind Arbeitgeber gehalten, ihren Beschäftigten flächendeckend das Arbeiten von zu Hause aus zu ermöglichen. Diese Umstellung muss aufgrund der dringlichen Situation ohne die Möglichkeit einer umfangreichen Vorbereitung zur Einhaltung rechtlicher Vorgaben erfolgen.

Folgende Hinweise sind allerdings bei der Umstellung auf Home-Office zumindest als Basic-To-Do´s zu beachten:

• Gesetzlicher Rahmen

Gesetzlich wird zwischen Telearbeit und mobilem Arbeiten unterschieden. Telearbeit ist in der Arbeitsstättenverordnung (ArbStättV) als einen durch den Arbeitgeber fest eingerichteten Bildschirmarbeitsplatz im Privatbereich des Beschäftigten definiert und formuliert arbeitsrechtliche und arbeitssicherheitstechnische Mindeststandards. Voraussetzung für die Telearbeit ist insofern die Lieferung der Ausstattung, Installation sowie die arbeitsrechtliche Vereinbarung. Mobiles Arbeiten wird gesetzlich nicht definiert, baut jedoch ebenso auf einer Verbindung zum Betrieb per Informations- und Kommunikationstechnik (IuK) auf, verlangt aber im Gegensatz zur Telearbeit keine Bindung an den häuslichen Arbeitsplatz. Von beliebigen Orten aus kann so die Arbeit mithilfe mobiler Endgeräte erledigt werden. Der Arbeitgeber ist dennoch weiter als Verantwortlicher für die datenschutzkonforme Verarbeitung personenbezogener Daten zuständig und verantwortlich. Bei Auftragsverarbeitungen ist sicherzustellen, dass die Arbeiten im Home-Office nicht im Vertrag über die Auftragsvereinbarung ausgeschlossen ist.

• Einsatz von mobilen Endgeräten

Beim Einsatz von mobilen Endgeräten ist die Nutzung dienstlicher Endgeräte gegenüber privaten Endgeräten stets zu empfehlen. Der Vorteil besteht darin, dass der Verantwortliche die dienstlichen Endgeräte selbst konfiguriert hat und so den Datenschutz und die Datensicherheit effektiver gewährleisten kann. Ansprechpersonen für technische Probleme und die nötigen Sicherheitsmaßnahmen wie eine Aktualisierung des Systems und des Virenschutzes sind darüber hinaus von Unternehmensseite in aller Regel gegeben.

Falls eine Nutzung privater Endgeräte (*„Bring your own device“*) unabdingbar ist, müssen dienstliche Daten in einem verschlüsselten Bereich verarbeitet und gespeichert werden. Die Daten sind nach der Übertragung in das dienstliche Netz auf ihrem privaten Gerät unwiederbringlich zu löschen, soweit Daten lokal ab- und zwischengespeichert wurden. Zum sicheren Löschen werden unter Umständen besondere Tools benötigt, ein Verschieben in den Papierkorb mit dem entsprechenden „Leeren“ des Papierkorbs reicht nicht immer aus.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

• Dokumente

Dokumente sollten möglichst auf Datenträgern im Netz des Unternehmens bzw. der Einrichtung (Intranet) gespeichert werden, um ein regelmäßiges Backup zu ermöglichen. Damit wird das von Art. 32 Datenschutz-Grundverordnung (DS-GVO) ausgehende Schutzziel der Verfügbarkeit am besten gewährleistet. Die Einwahl in das Netzwerk des Unternehmens bzw. der Einrichtung sollte im Sinne der Datensicherheit immer über ein Virtuelles Privates Netzwerk (VPN) erfolgen. Bei lokaler Ablage, die nie gänzlich verhindert werden kann, sollten die Daten auf verschlüsselten Festplatten gespeichert werden. Private Hardware sollte auch deswegen nach Möglichkeit nicht verwendet werden, um sich effektiv vor möglicher Schadsoftware zu schützen. Auf Unternehmensware darf von einem funktionierenden Virenschutz ausgegangenen werden, was für den privaten Bereich nicht pauschal unterstellt werden kann.

• Verhinderung des Zugriffs durch Dritte

Eine Nutzung der Endgeräte durch andere Personen als dem Beschäftigten, etwa Familie, Kinder oder Freunde ist durch arbeitsrechtliche Anweisung pauschal zu untersagen. Beim Verlassen des Arbeitsplatzes sollte so ein Kennwortschutz aktiviert werden. Diese Bildschirmsperre sollte nach einer bestimmten inaktiven Zeit (z.B. 5 Minuten) automatisch aktiviert werden.

• Vermeidung von Papier

Bei der Gestaltung der Arbeit im Home-Office sollten möglichst keine Ausdrucke durch den Arbeitnehmer nötig werden und auch keine schriftlichen Unterlagen von diesem benutzt oder angefertigt werden. Stattdessen sollten die notwendigen Daten über (verschlüsselte) E-Mails oder über das Intranet verfügbar gemacht werden. Sofern schriftliche Unterlagen tatsächlich notwendig und erforderlich sind, sollten diese bei Transport und Aufbewahrung durch verschließbare Behälter geschützt werden. Die Entsorgung sollte nicht über den Papiermüll geschehen, sondern durch einen Aktenvernichter oder bei nächster Möglichkeit im Büro des Betriebes, wo eine zertifizierte Datenvernichtung gewährleistet ist.

• Telefon- und Videokonferenzen

Sofern Konferenzdienste in Anspruch genommen werden, ist deren Zugriff auf Inhalts- oder Metadaten kritisch zu überprüfen. Entgeltfreie Dienste werden häufig indirekt „mit Daten bezahlt“, kostenpflichtige Dienste dagegen wahren also häufiger den notwendigen Datenschutz, worauf man sich jedoch auch nicht verlassen kann. Während der Konferenzen sollten Zusatzangebote wie eine Sprach- und/oder Videoaufzeichnung oder eine Auswertung des gesprochenen Wortes, um dieses z.B. in andere Sprache zu übersetzen, immer deaktiviert bzw. ungenutzt bleiben.

Zu diesem Thema finden Sie ausführliche Informationen in der GDD-Praxishilfe DS-GVO XVI unter: https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_xvi-videokonferenzen-und-datenschutz.

Eine Übersicht über Videokonferenzsysteme, Messenger und Fernwartungssoftware finden Sie unter: https://www.gdd.de/aktuelles/startseite/neue-praxishilfe-videokonferenzen-und-datenschutz-erschienen.

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Seminartipps zum Arbeitspapier

Online-Kompaktkurs: IT-Sicherheit und Home-Office

Um die IT-Sicherheit im Home-Office zu gewährleisten sind geeignete Maßnahmen zu treffen. Soweit ein dienstlicher Rechner genutzt werden kann, sind die Maßnahmen noch relativ einfach zu beherrschen. Soll oder muss jedoch ein privater Rechner (Stichwort „Familien-PC“) genutzt werden, wird es komplizierter. Der Bayerische Landesbeauftragte für den Datenschutz hat Empfehlungen für den Einsatz von privaten Rechnern im Home-Office von Behörden-Beschäftigten gegeben.
Welche Probleme tun sich vor dem Hintergrund der Netzstrukturen in Deutschland und der privaten IT-Infrastruktur der Beschäftigen auf? Wie geht man damit um?
Im Online-Kompaktkurs werden Vorschläge zur Umsetzung dieser Regelungen gemacht und die Vor- und Nachteile diskutiert. Welche begleitenden organisatorischen Regelungen (Anleitungen und Merkblätter) sind erforderlich? Welche ersten Erfahrungen haben Unternehmen mit dem Betrieb des Home-Office gemacht?

Weitere Infos finden Sie hier.

Online-Schulung: Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden

Die DS-GVO hat einige Neuerungen für Verantwortliche gebracht, die deutliche Reichweite haben. So ist mit dem Prinzip der Rechenschaftspflicht eine »Beweislastumkehr« vorhanden, die dann besonders zum Tragen kommen wird, wenn die zuständige Datenschutzaufsichtsbehörde zur Prüfung »vorbeischaut«. Dann wird auch der Datenschutzbeauftragte gefragt, vielleicht auch gefordert sein. Seine Rolle hat sich mit der DS-GVO mitunter grundlegend geändert – vom »Einzelkämpfer«, der sich um den Datenschutz irgendwie kümmern soll, zu einer Instanz, dessen Aufgaben in der Beratung und Kontrolle liegt und dem Verantwortlichen für den Datenschutz, der Geschäftsleitung, kompetent zur Seite steht. Auch werden sicher erhebliche Bußgelder auf diejenigen Stellen zukommen, die sich nicht mit der Umsetzung der DS-GVO in ihren Prozessen befasst haben. Gut für die Institution, die weiß, wie die Datenschutzaufsichtsbehörden so »ticken«, wie diese die Umsetzung der DS-GVO kontrollieren und welche Anforderungen diese an interne Kontrollmechanismen haben.
Machen auch Sie sich in dieser Online-Schulung mit der aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden vertraut und minimieren Sie das Bußgeldrisiko durch interne Audits.

Weitere Infos finden Sie hier.

DataAgenda
ist das Informationsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

Datakontext
ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.

Autoren

Prof. Dr. Rolf Schwartmann
Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V (GDD), Leiter der Kölner Forschungsstelle für Medienrecht (TH Köln) und Mitglied der Datenethikkommission.

Dr. Tobias Jacquemain, LL.M.
Wissenschaftlicher Referent bei der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

DATAKONTEXT GmbH • Augustinusstraße 9d • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com