Insbesondere die folgenden Punkte sind bei der Einführung von Homeoffice aus datenschutzrechtlicher Sicht zu berücksichtigen[1]:

Allgemeines	
☐	Zunächst ist zu prüfen, welche Tätigkeiten generell im Rahmen des Homeoffice erbracht werden können.
☐	Es ist zu prüfen, ob der Mitarbeiter für die Homeoffice-Arbeit geeignet ist (entscheidende Kriterien sind beispielsweise: Vertrauen, Kompetenz, ausreichende Sensibilität, Datenschutz-Awareness des Mitarbeiters).
☐	Ein den personenbezogenen Daten angemessenes Schutzniveau muss getroffen werden (Art. 32 DSGVO).
Umgebung	
☐	Es ist festzulegen, in welcher Umgebung die Arbeit stattfinden darf (z.B. „Die Homeoffice-Arbeit hat ausschließlich am Wohnsitz des/der Beschäftigten zu erfolgen.“)
☐	Als Homeoffice sollte nur ein Raum genutzt werden dürfen, der abschließbar ist. Unterlagen mit personenbezogenen Daten müssen unter Verschluss aufbewahrt werden. Generell sollte untersagt werden, die Unterlagen unbeaufsichtigt zu lassen.
☐	Es sollte untersagt werden, Dritten (z.B. Familienmitgliedern, Mitbewohnern, Besuchern) den Zugriff/Zugang auf die betriebliche EDV und/oder Unterlagen/Informationen zu gewähren. Der Arbeitsplatz sollte so gewählt werden, dass andere Personen den Bildschirm nicht einsehen können – auch nicht durch ein Fenster.
Technisches	
☐	Festlegung, welche Geräte genutzt werden dürfen (z.B. „Zur Verrichtung der Tätigkeit im Homeoffice sind ausschließlich die dienstlichen Geräte (Dienst-Notebook und Dienst-Smartphone) und die vom Arbeitgeber freigegebene/genehmigte Software zu nutzen.“)
☐	Alle Datenträger in den mobilen und, sofern vorhanden, festen Geräten sollten verschlüsselt werden.
☐	Festlegung, welche Netzwerke genutzt werden dürfen (z.B. „Die Verbindung der dienstlichen Geräte mit dem privaten Heimnetzwerk ist gestattet. Die Nutzung von öffentlich zugänglichen WLAN ist nicht gestattet.“)

[1] Bitte beachten Sie, dass diese Checkliste nicht abschließend ist und dass weitere Regelungen zum Arbeiten im außerbetrieblichen Bereich, insbesondere Arbeits-/ und/oder Organisationsanweisungen (beispielsweise im Falle von Bring Your Own Device), entsprechend berücksichtigt werden müssen.

	Sofern die Nutzung des privaten Internet-Anschluss erlaubt wird, sollte das genutzte Endgerät so eingerichtet werden, dass es mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden ist. Das WLAN sollte so eingerichtet sein, dass das Einwählen nur mit einem sicheren Passwort erfolgen kann.
☐	Die Sicherheitssoftware der Dienstgeräte sollte jederzeit aktiviert sein. (Auf Updates, Sicherheitspatches sowie aktiven Virenschutz und Firewall sollte geachtet werden).
☐	Es sollte dafür gesorgt werden, dass alle Geräte mit einem sicheren Passwort geschützt sind.
☐	Bei Verlassen des Homeoffice sollte sichergestellt werden, dass kein Dritter auf betriebliche/personenbezogene Daten zugreifen bzw. Kenntnis nehmen kann; der Zugang zum System ist auch bei kurzer Unterbrechung zwingend zu sperren (Anmeldung hat per Eingabe des Nutzernamens und Passwort zu erfolgen).
☐	Eine VPN-Verbindung sollte für jeden Mitarbeiter, der im Homeoffice arbeiten soll, eingerichtet worden sein.
☐	Die Funktionsfähigkeit der lokalen Backups sollte sichergestellt und regelmäßig überprüft werden.
Umgang mit personenbezogenen Daten	
☐	Regelung wie mit Papierdokumenten umzugehen ist (z.B. „Dokumente in Papierform dürfen nicht mit ins Homeoffice genommen werden. Diese sind einzuscannen und dann via VPN zu nutzen.“) Regelung, dass dienstliche Papierdokumente nicht in den privaten Hausmüll geworfen werden sollen. Ggf. kann ein Verweis auf bereits vorhandene Organisationsanweisungen zur datenschutzkonformen Entsorgung erfolgen.)
☐	Regelung, dass die Beschäftigten darauf achten, ihren Arbeitsplatz so zu strukturieren, dass keine privaten und dienstlichen Daten miteinander vermischt werden.

☐	Regelung, ob und inwiefern die Nutzung von Druckern im Homeoffice erlaubt ist (z.B. „Falls im Homeoffice Ausdrucke angefertigt werden, sind diese anschließend mitzubringen und nach Erledigung wie üblich abzulegen bzw. zu entsorgen. Eine dauerhafte Verwahrung im Homeoffice ist unzulässig.“)
☐	Sofern dienstliche Endgeräte genutzt werden, Regelung, dass an diesem keine private Hardware (z.B. Festplatten, USB-Sticks) angeschlossen werden dürfen.
☐	Festlegung des Speicherorts der Daten (z.B. „Die am PC erstellten und bearbeiteten kundenbezogenen Dokumente sind über den VPN-Zugang direkt auf dem Firmen-Server zu speichern.“)
☐	Regelung, dass insbesondere für dienstliche Telefonate oder ähnliche Gespräche ungestörte Bereiche aufzusuchen sind, damit die Vertraulichkeit des Gesprächs gewährleistet werden kann.
☐	Regelung, dass die personenbezogenen Daten nicht zu anderen als den betrieblichen Zwecken verwendet werden dürfen.
☐	Sicherstellen, dass jeder Mitarbeiter weiß, wie bei Datenschutzvorfällen vorzugehen ist (z.B. kann diesbezüglich auf eine andere Organisationsanweisung verwiesen werden).
☐	Sicherstellen, dass jeder Mitarbeiter weiß, wie bei einer Anfrage einer Person bezüglich ihrer Betroffenenrechte auch vom Homeoffice vorzugehen ist.
☐	Die Mitarbeiter sollten zur Vertraulichkeit verpflichtet worden sein.
Verarbeitung von personenbezogenen Daten im Auftrag	
☐	Sofern Sie im Auftrag eines Kunden mit personenbezogenen Daten arbeiten, sollten Sie prüfen, ob die Arbeit im Homeoffice nicht durch entsprechende Vereinbarungen, insbesondere einer Auftragsverarbeitungsvereinbarung ausgeschlossen wird.

Quellen und weitergehende/zusätzliche Informationen zum Thema Homeoffice finden Sie hier:

„Telearbeit und Mobiles Arbeiten“, Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Stand: Januar 2019, https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

„Top Tips for Cybersecurity when Working Remotely“, Artikel der European Union Agency for Cybersecurity (ENISA) Stand: März 2020, https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely

„Home-Office? –Aber sicher!“ Information des Bundesamts für Sicherheit in der Informationstechnik (BSI), Stand: März 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html

„Datenschutz: Plötzlich im Homeoffice – was nun?“, Information des ULD Schleswig-Holstein, Stand: März 2020, https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf