Das Homeoffice aus datenschutzrechtlicher Perspektive in Zeiten des Corona-Virus

RECHTLICHE UND PRAKTISCHE ANFORDERUNGEN UND MAßNAHMEN RICHTIG UMSETZEN

Themenübersicht

- Schutz personenbezogener Daten im Homeoffice
- Grundregeln fürs Homeoffice
- Anforderungen an den physischen und digitalen Arbeitsplatz zu Hause

Das Arbeiten im Homeoffice wird begleitet von großen Herausforderungen. Es müssen in Organisation und IT zügig gangbare Lösungen gefunden und umgesetzt werden, um den Geschäftsbetrieb stabil und effizient aufrechtzuerhalten. Gleichzeitig sollen aber auch die Mehrkosten für Ausweichlösungen, insbesondere im IT-Bereich, möglichst gering gehalten werden. Arbeitgeber müssen jetzt darauf achten, dass nicht auf „Notlösungen" zurückgegriffen wird, die datenschutzrechtlich negative Konsequenzen haben können.

Wer trägt die Verantwortung im Homeoffice?

Der Arbeitgeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO und ist im Homeoffice, genauso wie am regulären Arbeitsplatz, gemäß Art. 24 DSGVO dafür verantwortlich, dass bei der Datenverarbeitung der gesetzliche Datenschutz im vollen Umfang eingehalten wird. Für Datenschutzverstöße im Homeoffice haftet er also gleichermaßen, wie in den unternehmenseigenen Räumlichkeiten, auch wenn hier oft Haushaltsmitglieder des Arbeitnehmers und damit unternehmensfremde Personen in unmittelbarer Nähe sind. Diese sieht der Arbeitnehmer selbst oft nicht als Dritte an, auch wenn die rechtliche Bewertung eindeutig anders ausfällt. Mitarbeiter müssen daher oft erst für diese Thematik sensibilisiert und darüber aufgeklärt werden, dass der Datenschutz im Homeoffice sogar anspruchsvoller ist als im Unternehmen. Erhalten Dritte im Homeoffice Kenntnis von personenbezogenen Daten, so ist dies u.U. gemäß Art. 33, 34 DSGVO als Datenschutzverletzung gleichermaßen den Behörden und ggf. den Betroffenen zu melden, wie eine Datenschutzverletzung am regulären Arbeitsplatz oder online. Der Arbeitgeber muss den Datenschutz daher auch im Homeoffice gewährleisten und überwachen.

Arbeitsrecht beachten: Homeoffice kann nur im gegenseitigen Einvernehmen zwischen Arbeitgeber und Arbeitnehmer vereinbart werden. Arbeitgeber müssen aktuell daher unbedingt darauf achten, dass die Absprachen, die jetzt mit Mitarbeitern zum Homeoffice getroffen werden, ausdrücklich auf die aktuelle Ausnahmesituation der Corona-Pandemie begrenzt sind. Es besteht sonst die Gefahr, dass ein Anspruch auf Homeoffice begründet wird, der später nur schwer wieder rückgängig zu machen ist. Das GSK-Update zu den aktuellen arbeitsrechtlichen Themen kann hier heruntergeladen werden.

Für welche Daten gelten im Homeoffice besondere Anforderungen?

Auch im Homeoffice werden regelmäßig personenbezogene Daten verarbeitet. Anders als am regulären Arbeitsplatz sind hier jedoch höhere Risiken gegeben, dass unbefugte Dritte von diesen Kenntnis erlangen. Mitarbeiter müssen daher darauf achten, wie sie sich bei der Arbeit im Homeoffice verantwortungsbewusst verhalten. Unternehmensinterne Informationen ohne Personenbezug unterfallen zwar nicht den gesetzlichen Daten-

schutzbestimmungen, sind jedoch aus Unternehmenssicht gleichsam schutzwürdig. Ratsam ist für Arbeitgeber die Erstellung einer speziellen Homeoffice-Richtlinie für alle Mitarbeiter, in der Datenschutz und die Verschwiegenheit gleichsam geregelt sind. Sollte eine solche Homeoffice-Richtlinie im Unternehmen noch nicht vorhanden sein, so kann die aktuelle Situation einen guten Anlass bieten, dies unter Einbeziehung des Datenschutzbeauftragten und Betriebsrates nachzuholen.

Welche Grundregeln sind zu beachten?

Insbesondere die Grundregeln für betriebliche Daten und Kommunikation müssen auch in einer Ausnahmesituation wie dem aktuellen Pandemiefall eingehalten werden. Personenbezogene Daten sollten niemals in den privaten E-Mail-Accounts, den Apps von privaten Messengerdiensten oder auf dem privaten PC von Mitarbeitern gespeichert oder verarbeitet werden. Neben den generellen Sicherheitsbedenken bei diesen Anwendungen hat der Arbeitgeber keine Möglichkeit zu überprüfen, wofür die Mitarbeiter den Diensten weitere Rechte eingeräumt haben. Viele Personen nutzen kostenfreie E-Mail-Anbieter oder Messenger, die in erheblichem Umfang Daten für Werbe- und andere Zwecke nutzen und verarbeiten. Auch die E-Mail-Adressen und Telefonnummern von Kontaktpersonen werden von diesen Diensten oft automatisch ins Adressbuch des Accounts übernommen. Ist dieses Adressbuch wiederum mit anderen Diensten verknüpft, werden die Daten großflächig verteilt. Oft wissen Mitarbeiter noch nicht einmal, wie weitreichend sie ihre private Kommunikation freigegeben haben. Arbeitgeber müssen eine solche unkontrollierte Ausbreitung verhindern, indem sie eine Nutzung der privaten Accounts für unternehmensbezogene Aufgaben grundsätzlich untersagen. Dies ist auch im Hinblick auf die Zeit nach der aktuellen Pandemie ratsam, denn alle, die unter Verstoß gegen datenschutzrechtliche Bestimmungen verarbeitet werden, sicher gelöscht werden müssen. Diese Löschung zu überwachen, wird außerhalb des unternehmenseigenen Systems kaum gelingen und letztendlich besteht neben den datenschutzrechtlichen Bedenken auch immer die Gefahr, dass Mitarbeiter, die ein Unternehmen verlassen, sensible Unternehmensdaten wie Kundenkontakte mitnehmen, weil sie nicht gelöscht wurden.

Was gilt für den physischen Arbeitsplatz?

Die größte Herausforderung im Homeoffice stellen die Familien- und Haushaltsmitglieder der Arbeitnehmer dar. Mitarbeiter sollten dazu angewiesen werden, Vertrauliches auch im Homeoffice vertraulich zu behandeln. Bestenfalls sollten Papierunterlagen nicht vom regulären Arbeitsplatz mit ins Homeoffice genommen werden. Auch sollten Mitarbeiter im Homeoffice keine Unterlagen, die personenbezogene Daten beinhalten, ausdrucken. Kann die Verwendung von Papierunterlagen im Homeoffice nicht ganz ausgeschlossen werden, sollten Unterlagen mit personenbezogenen Daten nicht offen für andere einsehbar sein und am Ende des Arbeitstages sicher und abgeschlossen verwahrt, statt beispielsweise auf dem Küchentisch ausgebreitet liegen gelassen werden. Ebenso sollte der Bildschirm vor der Sicht Dritter abgeschirmt werden. Telefonate sollten auch zu Hause nicht im Beisein Dritter geführt werden. Ist eine räumliche Trennung für Telefonate bei einem Mitarbeiter zu Hause nicht möglich, besteht aber das Erfordernis Telefonate zu führen, bei denen insbesondere über besonders sensible personenbezogene Daten gesprochen wird, sollten Mitarbeiter mit einer geeigneten Wohnsituation identifiziert werden, bei denen das Beisein Dritter ausgeschlossen werden kann. Genauso wie am regulären Arbeitsplatz kann auch im Homeoffice Papiermüll anfallen, der personenbezogene Daten enthält. Mitarbeiter sollten diesen separat zu Hause sammeln, verschlossen verwahren und später am regulären Arbeitsplatz sicher entsorgen. Ein bloßes Zerreißen in kleinere Stücke reicht i.d.R. nicht zur sicheren Entsorgung aus.

Was gilt für den digitalen Arbeitsplatz?

Für den digitalen Arbeitsplatz sind eine Verschlüsselung der Datenträger und ein Passwortschutz auch im Homeoffice wichtig. Alle Geräte mit Daten darauf, die außerhalb der des regulären Arbeitsplatzes bewegt werden, können abhandenkommen und damit ggf. zu einer meldepflichtigen Datenschutzverletzung werden. Greifen Mitarbeiter von zu Hause aus auch auf das System im

Unternehmen zu, sollte dies über eine sichere VPN-Verbindung erfolgen, um Datensicherheit herzustellen und um die Erstellung von Datenkopien auf private Notebooks zu vermeiden. Um den unbefugten Zugriff auf Daten auch im Homeoffice zu verhindern, sollte das Notebook, auch bei nur kurzzeitiger Arbeitsunterbrechung, gesperrt werden. Mitarbeiter sollten gerade jetzt noch einmal dafür sensibilisiert werden, dass auch in der aktuellen Sondersituation Familienmitglieder keinen Zugriff auf das betriebliche Notebook haben dürfen. Die unternehmenseigene IT-Ausstattung sollte ausschließlich zu beruflichen Zwecken verwendet werden, um Risiken zu minimieren. Nutzen beispielsweise Kinder ein Betriebsnotebook für Hausaufgaben oder Spiele, so besteht eine höhere Gefahr, dass diese unwissentlich Schadsoftware installieren, weil sie häufig Gefahren im Internet noch nicht einschätzen können. Es ist auch zu erwarten, dass Hacker die aktuelle Situation gezielt missbrauchen werden, um Schutzlücken auszunutzen. Ebenso besteht die Möglichkeit, dass es vermehrt zu Phishing-Versuchen kommen wird.

Was ist bei der Nutzung privater Endgeräte zu beachten?

Grundsätzlich sollte vermieden werden, dass Daten auf Geräten gespeichert werden, die nicht im Unternehmenseigentum stehen. Private USB-Sticks sollten ebenfalls nicht verwendet werden. Einerseits werden diese häufig unverschlüsselt verwendet und es besteht zudem das hohe Risiko, dass diese verloren gehen, andererseits könnte die Benutzung privater USB-Sticks später in Vergessenheit geraten und nur auf einem Notebook gelöschte Daten von Dritten später wiederhergestellt werden. Nutzen Mitarbeiter private Smartphones zum Telefonieren, sollten personenbezogene Daten wie z.B. Kontakte nicht im Adressbuch gespeichert werden, da diese häufig mit Anwendungen wie WhatsApp verknüpft sind, die das Adressbuch auslesen und speichern. Bei privaten Druckern sollte regelmäßig der interne Speicher gelöscht werden. Nutzen Mitarbeiter dennoch einen privaten PC, was vermieden werden sollte, um beispielsweise über WebAccess auf Anwendungen zuzugreifen, sollte sichergestellt werden, dass in den Browsern des privaten PC möglichst keine spezifischen Plug-Ins installiert sind, da diese häufig die gesamte Eingabe im Browser mitlesen.

Wie kann zusätzliche Software zur Arbeitserleichterung eingesetzt werden?

Bei allen Softwarelösungen, die im Rahmen der aktuellen Situation eingeführt werden, wie Online-Meeting- und Messenger-Anwendungen, muss darauf geachtet werden, dass auch jetzt und unter Zeitdruck der nach den datenschutzrechtlichen Bestimmungen geforderte Prüfungs- und Dokumentationsprozess eingehalten wird. Insbesondere sind Fragen zur Auftragsdatenbearbeitung nach Art. 28 DSGVO sowie zum Datentransfer im Falle von Anwendungen, die Anbieter aus Ländern, die nicht dem Europäischen Wirtschaftsraum angehören, zu klären und insoweit die erforderlichen Maßnahmen zu ergreifen. Welche Besonderheiten bei der Nutzung externer Software zu beachten ist, werden wir in einem unserer nächsten GSK-Updates genauer beleuchten.

Dr. Katy Ritzmann
Rechtsanwältin, Partnerin
Standort Berlin
katy.ritzmann@gsk.de

Dr. Jörg Kahler
Rechtsanwalt, Partner
Standort Berlin
joerg.kahler@gsk.de

Ira Mießler, LL.M.
Rechtsanwältin, Associate
Standort Berlin
ira.miessler@gsk.de

Anne Bettina Nonnaß
Rechtsanwältin, Associate
Standort Berlin
anne.nonnass@gsk.de

Jörg Wünschel
Rechtsanwalt, Associate
Standort Berlin
joerg.wuenschel@gsk.de

GSK
STOCKMANN

Haftungsausschluss
Diese Mandanteninformation enthält ausschließlich allgemeine Informationen, die nicht geeignet sind, den besonderen Umständen eines Einzelfalles gerecht zu werden. Sie hat nicht den Sinn, Grundlage für wirtschaftliche oder sonstige Entscheidungen jedweder Art zu sein. Sie stellt keine Beratung, Auskunft oder ein rechtsverbindliches Angebot auf Beratung oder Auskunft dar und ist auch nicht geeignet, eine persönliche Beratung zu ersetzen. Sollte jemand Entscheidungen jedweder Art auf Inhalte dieser Mandanteninformation oder Teile davon stützen, handelt dieser ausschließlich auf eigenes Risiko.

GSK Stockmann und auch die in dieser Mandanteninformation namentlich genannten Partner oder Mitarbeiter übernehmen keinerlei Garantie oder Gewährleistung, noch haftet GSK Stockmann und einzelne Partner oder Mitarbeiter in irgendeiner anderen Weise für den Inhalt dieser Mandanteninformation. Aus diesem Grund empfehlen wir, in jedem Fall eine persönliche Beratung einzuholen.

www.gsk.de

GSK Stockmann

BERLIN
Mohrenstrasse 42
10117 Berlin
T +49 30 203907-0
F +49 30 203907-44
berlin@gsk.de

HEIDELBERG
Mittermaierstrasse 31
69115 Heidelberg
T +49 6221 4566-0
F +49 6221 4566-44
heidelberg@gsk.de

FRANKFURT / M.
Taunusanlage 21
60325 Frankfurt am Main
T +49 69 710003-0
F +49 69 710003-144
frankfurt@gsk.de

MÜNCHEN
Karl-Scharnagl-Ring 8
80539 München
T +49 89 288174-0
F +49 89 288174-44
muenchen@gsk.de

HAMBURG
Neuer Wall 69
20354 Hamburg
T +49 40 369703-0
F +49 40 369703-44
hamburg@gsk.de

LUXEMBURG
GSK Stockmann SA
44, Avenue John F. Kennedy
L-1855 Luxemburg
T +352 271802-00
F +352 271802-11
luxembourg@gsk-lux.com