Liebe Rechtsanwältinnen und Rechtsanwälte,
liebe Notarinnen und Notare,

COVID-19 oder kurz Corona hat weltweit flächendeckend zu einem Umdenken, auch in der Arbeitsplatzgestaltung, geführt. Homeoffice oder Telearbeit sind in diesen Tagen viel gesuchte Begriffe. Auch in den von uns betreuten Rechtsanwaltskanzleien und Notariaten kommt diese Frage auf; waren die Fragen zunächst eher im Bereich der Notfallplanung und für den Fall der amtlichen Anordnung der Kanzleischließung aufgetreten, stellt sich mit Blick auf die Umsetzung der von Bundes- und Landesregierungen ausgesprochenen Empfehlungen zu Minimierung der Sozialkontakte, vermehrt die Frage, ob und wie Telearbeit unbeschadet einer Standortschließung in den Kanzleibetrieb integriert werden kann.

Neben berufsrechtlichen Fragestellungen, ist die Beantwortung natürlich auch von datenschutzrechtlichen Rahmenbedingungen abhängig. Was gilt also und wie können Sie den Mitarbeiter- und Infektionsschutz mit dem Datenschutzrecht in Einklang bringen? Die wichtigsten Antworten haben wir Ihnen nachfolgend zusammengestellt:

I. Homeoffice – Stellen Sie die Hardware zur Verfügung!

Auch Mitarbeiter, die von zuhause aus tätig werden, stehen unter der Verantwortung der Rechtsanwältin / des Rechtsanwaltes bzw. der Notarin / des Notars, er/sie bleibt damit auch für sämtliche Verarbeitungen im Homeoffice Verantwortliche/r im Sinne des Art. 4 Nr. 7 DSGVO und hat insoweit auch für die Telearbeitsumgebung die Sicherheit der Verarbeitung zu gewährleisten (Art. 25, 32 DSGVO). Zu beachten ist dabei, dass die Arbeit von zuhause aus andere und regelmäßig größere Gefahren für die Datensicherheit, den Datenschutz und die Vertraulichkeit von Daten bedingt; denn anders als in der Kanzlei selbst findet die Arbeit nicht im Kreise von zur Berufsverschwiegenheit verpflichteten Personen, sondern im familiären bzw. privaten Umfeld statt. Die Familienmitglieder des im Homeoffice arbeitenden Mitarbeiters sind indes weder durch gesetzliche Regelungen besonders geschützt, noch nach § 43a Abs. 2 BRAO bzw. § 26 BNotO besonders verpflichtet worden. Die tatsächliche Einflussmöglichkeit auf Maßnahmen der organisatorischen Sicherheit ist in der Wohnung des Mitarbeiters ebenso wesentlich schwieriger zu

kontrollieren und durchzusetzen. Der Aspekt der technischen Maßnahmen gewinnt daher größere Bedeutung.

Daher gilt, soweit Sie beabsichtigen, Ihre Mitarbeiter aus dem Homeoffice heraus tätig werden zu lassen: Stellen Sie die hierfür erforderliche Hardware zur Verfügung und verzichten Sie gänzlich auf den Einsatz von im Mitarbeitereigentum stehenden Computern und sonstiger Hardware. Warum? Nur auf den durch Sie bereitgestellte Hardwaresystemen können Sie die nach dem Stand der Technik geforderten Sicherheitsmaßnahmen etablieren, nur hier haben Sie die Gewissheit, dass die Systeme und Daten in der Kanzlei bestmöglich gegen unberechtigten Zugriff gesichert sind. Nur die technische Trennung von privater und dienstlicher Technik verhindert zudem, dass Sie als Arbeitgeber die Zugriffsmöglichkeit auf dienstliche Dokumente verlieren und vermeidet gleichsam Datenschutzkonflikte, die dadurch entstehen können, dass private Daten auf dienstlicher Hardware gespeichert oder über diese zugänglich werden.

Was sollten Sie in jedem Fall beachten

1. **Installieren Sie sog. Device-Control-Software auf den Homeoffice PCs und Laptops**

   USB-Flash-Laufwerke und andere tragbare USB-Geräte bzw. ihr unkontrollierter Einsatz, stellt eine der Hauptursachen für Sicherheitsvorfälle dar. Über diese Anschlüsse und daran angeschlossene Speichermedien kann Schadsoftware auf den PC geladen oder können Daten vom PC kopiert werden. Auf eine ähnlich simple Art und Weise konnte beispielsweise Edward Snowden vertrauliche Informationen der sicherlich hochgesicherten NSA entwenden. Sog. Device-Locker-Software bietet hier Schutz. Über sie können Zugriffsrichtlinien für USB-Ports und andere Schnittstellen eines Computers festgelegt und kontrolliert werden. So kann sichergestellt werden, dass zwar der USB-Drucker oder auch der Kartenleser weiterhin über USB an den Rechner angeschlossen werden können, externe und unbekannte Festplatten hingegen nicht. Welche Software hier zum Einsatz kommt, kann nicht pauschal gesagt werden. Die Zeitschrift C't testet 2018 beispielsweise das Produkt SafeConsole USB-Device-Management mit recht gutem Ergebnis. Auch die Softwarelösungen DriveLock, ESET oder der Microsoft Defender kommen hier in Betracht.

2. **Nutzen Sie Gruppenrichtlinien**

Setzen Sie Gruppenrichtlinien für externe User in ihrer Serverumgebung. Gestatten Sie beispielsweise nur die rein serverbasierte Datenverarbeitung ohne Speicherung von Daten auf den im Home-Office eingesetzten Endgeräten, indem Sie insbesondere die Einbindung lokaler Ressourcen in eine (Terminal-)Serversitzung (Laufwerke, Drucker usw.) verhindern. Anstatt den Mitarbeiter dazu aufzufordern, den PC beim Verlassen der Räume zu sperren, wäre es ggf. sinnvoll, die Rechner bereits so voreinzustellen, dass eine Sperre bei einer gewissen (kurzen) Zeitspanne der Inaktivität automatisch ausgelöst wird. Mehr zu Möglichkeiten, über Gruppenrichtlinien die Sicherheit zu erhöhen, finden Sie beispielsweise in einem Artikel von Security Insider unter: https://www.security-insider.de/mit-gruppenrichtlinien-die-windows-sicherheit-verbessern-a-555910/.

Auf Verzeichnis- oder Dateiebene sind Zugriffsbeschränkungen auf Grundlage von Benutzerrollen sinnvoll, denn nicht jeder Mitarbeiter, muss auf alle Ressourcen in der Kanzlei zugreifen. Software für so genanntes Information Rights Management (IRM) kann hier Abhilfe schaffen.

Wer hier noch mehr Sicherheit will, der kann auch darüber nachdenken, die Festplatten des extern genutzten Computers zu verschlüsseln. Auch hier bieten verschiedene Anbieter Lösungen am Markt an.

3. VPN und richtige Einstellung der Firewall

Der Zugriff auf die kanzleieigene Hard- und Softwareumgebung von zuhause aus, sollte in jedem Fall nur über sog. VPN-Verbindungen erfolgen. Ein Zugriff über das weitgehend ungesicherte Remotedesktopprotokoll sollte insoweit vermieden werden; wer in der Kürze der Zeit keinen VPN-Tunnel einrichten kann, der sollte jedenfalls nach Möglichkeiten suchen, die RDP-Verbindung weiter zu sichern, beispielsweise über eine 2-Faktor-Authentifizierung, wie sie etwa vom Hersteller ESET angeboten wird. Eine so genannte Zwei-Faktor-Authentifizierung sollte am besten auch zum VPN-Standard gehören. Nicht vergessen werden sollte, die richtige und sichere Einrichtung der kanzleieigenen Firewall, hier ist insbesondere darauf zu achten, dass wirklich nur (!) die erforderlichen Ports nach außen geöffnet und angeboten werden, um Angriffe zu erschweren. Sicherlich ist es ratsam, die Firewall durch den IT-Admin und geeignete Software zusätzlich und dauerhaft zu überwachen.

4. **Keine lokalen Administrationsrechte auf der Hardware**

   Entziehen Sie dem Mitarbeiter soweit möglich die Admin- Rechte auf dem Home-Office-PC, um die Installation von Software und auch die Verbreitung von Schadsoftware zu verhindern. In der Regel erscheint es auch sinnvoll einzelne Internetseiten für den Zugriff über den Home-Office PC zu sperren und so Sicherheitsrisiken zu verringern.

5. **Remotemanagement für die eingesetzte Hardware**

   Schließlich sollte für die im Home-Office eingesetzte Hardware ein Remotemanagement des IT-Administrators ermöglicht werden. Auch hierfür sind verschiedene Softwarelösungen am Markt erhältlich. Über eine solche Lösung können Sie sicherstellen, dass beispielsweise die erforderlichen Updates und Patches für die installierte Software installiert werden; ebenso können Virenscanner und lokale Firewalls aktualisiert und administriert werden**.** Es versteht sich von selbst, dass insbesondere die im Home-Office eingesetzte Hardware mit derartiger Software ausgestattet sein muss.

6. **Blickschutz-Filter für Displays und Monitore**

   Blickschutz-Filter sind flache Kunststoffe, die über einen Bildschirm gelegt werden und den Blickwinkel auf ca. 30° einschränken. Die Filterfolie soll verhindern, dass Unbefugte von der Seite auf den Bildschirm schauen können. Mit dieser einfachen Maßnahme, können Sie das Risiko der unberechtigten Kenntnisnahme Dritter im Vorbeigehen bereits recht wirksam minimieren.

7. **Deutliche und nicht oder nur schwer entfernbare Kennzeichnung der Hardware als Kanzleieigentum**

   Um zu vermeiden, dass bereitgestellte Hardware beim Mitarbeiter durch Dritte (Gerichtsvollzieher, Polizei, Staatsanwaltschaft usw.) beschlagnahmt werden, sollte die Hardware, beispielsweise durch entsprechende Aufkleber oder auch andere Beschriftungen, als Kanzleieigentum gekennzeichnet werden. Zusätzlich ist der Mitarbeiter natürlich zu verpflichten, hierauf bei Gefahr der Beschlagnahme hinzuweisen und die Rechtsanwältin / den Rechtsanwalt bzw. die Notarin / den Notar unverzüglich zu informieren, falls gleichwohl eine Inbesitznahme durch Dritte droht oder erfolgt ist.

II. Telefondienst von zuhause?

Wesentlich vorsichtiger sollte, gerade in der Anwaltskanzlei oder dem Notariat, mit der Umleitung von Telefonaten in das Home-Office umgegangen werden. So zeigt es sich als eher schlechte Idee, wenn die zentrale Kanzlei-Telefonnummer einfach auf einen Privatanschluss eines Mitarbeiters im Sekretariat umgeleitet wird. Insoweit wird – lebt der Mitarbeiter nicht allein – schon nicht ausgeschlossen werden können, dass Familienmitglieder versehentlich Anrufe entgegennehmen und damit das anwaltliche bzw. notarielle Berufsgeheimnis bereits gebrochen und der Datenschutz verletzt wird. Wenn es wirklich nicht anders geht, sollte die Umleitung daher auf ein dem Mitarbeiter zur rein dienstlichen Nutzung überlassenes Mobilfunkgerät erfolgen. Bei IP-Telefonanlagen besteht u.U. auch die Möglichkeit des „direkten Kontakts" mit der Kanzlei-Telefonanlage über das Netz bzw. den an dem Mitarbeiter bereitgestellten PC, über den dann eingehende Telefonanrufe mittels Headset entgegengenommen und ggf. auch weitergeleitet werden können. Was hier im Einzelnen möglich und machbar ist, muss anhand der individuellen Infrastruktur-Umgebung der Kanzlei entschieden werden.

III. Vertragliche Vereinbarung zum Homeoffice

Zusätzlich zu den vorbeschriebenen technischen Maßnahmen, sind auch organisatorische Maßnahmen zu ergreifen. Da die Arbeitsleistung in den Privaträumen des Mitarbeiters abgeleistet wird, ist dieser zur Einhaltung und Ergreifung angemessener Maßnahmen vertraglich zu verpflichten. Auch wenn diese Verpflichtung nicht zwingend der Schriftform bedarf, empfiehlt sich – auch aus Nachweiszwecken (Art. 5 II DSGVO) – der Abschluss einer schriftlichen Vereinbarung.

Zu dem **Mindestinhalten**, die aus Sicht des Datenschutzes und des Berufsrechts zu regeln sind, zählen

- Regelungen betreffend die Einhaltung der beruflichen Verschwiegenheit bei Ausübung der Heimarbeit, wie die Verpflichtung, unberechtigte Dritte vom Zugang zu der bereitgestellten Hardware auszuschließen (bspw. durch Nutzung in abschließbaren Räumen oder über die Verpflichtung die Hardware nach Ende

der Heimarbeitszeit sicher, etwa in einem abgeschlossenen Schrank, zu verwahren);

- das Verbot des Einsatzes der bereitgestellten Hardware außerhalb der eigenen Wohnung ohne Zustimmung des Anwaltes oder Notars;
- das Verbot, Dritten die Einsichtnahme auf die genutzte und in Betrieb befindliche Hardware zu gestatten und/oder zu ermöglichen (auch und insbesondere gegenüber anderen im Haushalt des Mitarbeiters lebenden Personen und durch die Bekanntgabe von Passwörtern, z. B. durch Notieren);
- das Verbot, betriebliche Daten auf privaten Speichermedien zu speichern bzw. eingerichtete Sicherheitsmaßnahmen, die dies verhindern, zu deaktivieren oder zu umgehen oder sonstige technische Veränderungen an den zur Verfügung gestellten Geräten vorzunehmen;
- Regelungen betreffend den Transport der Hardware;
- die Verpflichtung, etwaige eingetretene Verstöße gegen die vorstehenden Verpflichtungen unverzüglich der Rechtsanwältin / dem Rechtsanwalt bzw. der Notarin / dem Notar zu melden.

Regelungen könnten in etwa wie folgt lauten:

„Der Arbeitnehmer ist verpflichtet, auch bei Ausübung der Heimarbeit die beruflichen Verschwiegenheitspflichten der Rechtsanwältin / des Rechtsanwalts bzw. der Notarin / des Notars zu beachten. Die förmliche Verpflichtung nach § 43 a Abs. 2 BRAO bzw. § 26 BNotO findet insoweit auch für die Heimarbeit uneingeschränkt Anwendung. Der Arbeitnehmer ist verpflichtet bei Ausübung der Heimarbeit durch geeignete Maßnahmen sicherzustellen, dass Dritte, hierzu gehören auch Familienangehörige und sonstige in seinem Haushalt lebende und/oder sich dort auch kurzfristig aufhaltende Personen, vom Zugang zu der bereitgestellten Hardware sowie sämtlicher ggf. an den Heimarbeitsplatz verbrachter Datenträger, Akten und oder sonstiger textlicher Informationen auszuschließen. Insbesondere ist sicherzustellen, dass bei Ableistung der Heimarbeit Dritte weder den Bildschirm des Heimarbeitsplatzes, noch den Inhalt textlicher Informationen einsehen können. Akten, die auf der Außenseite Mandantennamen enthalten, sind in jedem Fall bei Anwesenheit Dritter nicht zu bearbeiten, sondern für Dritte nicht sichtbar zu verwahren.

Der Arbeitnehmer verpflichtet sich, die bereitgestellte Hardware sowie sämtliche ggf. an den Heimarbeitsplatz verbrachte Datenträger, Akten und oder sonstige textliche Informationen, von dem unbefugten Zugriff Dritter durch angemessene Maßnahmen zu schützen. Bereitgestellte Laptops sind so zu verwahren, dass sie nicht ohne Überwindung entsprechender Zugangshindernisse in den Besitz Dritter gelangen können. Soweit möglich, ist der Heimarbeitsplatz in einem abschließbaren, anderen Personen im Haushalt des Arbeitnehmers nicht zugänglichen, Raum einzurichten, der außerhalb der Arbeitszeiten abzuschließen ist. Ist dies nicht möglich, sind bereitgestellte Laptops in jedem Fall außerhalb der Arbeitszeiten in abschließbaren Schränken oder sonstigen Behältnissen sicher und für Dritte nicht offen sichtbar zu verstauen.

Der Arbeitnehmer verpflichtet sich, Zugangskennungen, wie Passwörter und Benutzerkennungen, nicht zu notieren. Benutzernamen und Passwörter sind insbesondere nicht mit Klebezetteln oder ähnlichem an der Hardware zu befestigen. Zugangskennungen, wie Passwörter und Benutzerkennungen, dürfen auch sonst keinen Dritten, hierzu gehören auch Familienangehörige und sonstige in seinem Haushalt lebende und/oder sich dort auch kurzfristig aufhaltende Personen, bekanntgegeben werden.

In keinem Fall ist der Arbeitnehmer – ohne ausdrückliche Zustimmung der Rechtsanwältin / des Rechtsanwaltes bzw. der Notarin / des Notars – berechtigt, die bereitgestellte Hardware sowie sämtliche ggf. an den Heimarbeitsplatz verbrachte Datenträger, Akten und oder sonstige textliche Informationen, an einen anderen Ort als den genehmigten Heimarbeitsplatz zu verbringen und/oder sie an einem anderen Ort einzusetzen und/oder zu bearbeiten. Die bereitgestellte Hardware ist bei Verbringung in den Heimarbeitsplatz und/oder zurück in die Kanzlei sicher zu verpacken; die Hardware darf – auch kurzzeitig – nicht offen in Kraftfahrzeugen zwischengelagert werden. Kurzfristige Zwischenlagerungen von nicht länger als einer Stunde, sind nur im abgeschlossenen Kofferraum zulässig. Bei längerer Abwesenheit ist die Hardware in jedem Fall aus Kraftfahrzeugen zu entfernen.

Dem Arbeitnehmer ist es untersagt, betriebliche Daten und Informationen auf privaten Medien zu speichern. Ihm ist weiterhin untersagt, durch die Rechtsanwältin / den Rechtsanwalt bzw. die Notarin / den Notar auf der bereitgestellten Hardware eingerichtete Sicherheitsmaßnahmen zu

deaktivieren und/oder zu umgehen und/oder sonstige technische Veränderungen an den durch zur Verfügung gestellten Geräten vorzunehmen.

Der Arbeitnehmer verpflichtet sich, die Rechtsanwältin / den Rechtsanwalt bzw. die Notarin / den Notar über etwaige eingetretene Verstöße gegen die vorstehenden Verpflichtungen unverzüglich zu informieren. Dies gilt auch, wenn und soweit der Eintritt eines Verstoßes nicht sicher festgestellt werden kann."

Es empfiehlt sich, auch wenn die Wirksamkeit derartiger Regelungen im Einzelnen arbeitsrechtlich umstritten ist, auch eine Regelung betreffend **Kontrollmöglichkeiten der Rechtsanwältin / des Rechtsanwaltes bzw. der Notarin / des Notars vor Ort** zu treffen. Eine Regelung könnte etwa wie folgt lauten:

„Der Rechtsanwalt / die Rechtsanwältin bzw. der Notar / die Notarin ist berechtigt, vor Aufnahme der Home-Office-Tätigkeit, den Heimarbeitsplatz aufzusuchen und zu besichtigen, um sicherzustellen, dass die Einhaltung des Datenschutzes sowie der weiteren berufsrechtlichen Verpflichtungen eingehalten werden können. Der Rechtsanwalt / die Rechtsanwältin bzw. der Notar / die Notarin kann sich hierzu auch der Unterstützung des betrieblichen Datenschutzbeauftragten bedienen. Dem Arbeitnehmer ist bekannt, dass der Rechtsanwalt / die Rechtsanwältin bzw. der Notar / die Notarin auch während der Durchführung der Heimarbeit auf die Kontrolle der Einhaltung der vertraglichen Pflichten durch den Arbeitnehmer angewiesen sein kann. Dies insbesondere dann, wenn konkrete Anhaltspunkte dafür vorliegen, dass der Arbeitsplatz im Home-Office nicht mehr den Anforderungen genügt oder konkrete Verstöße gegen die Verpflichtungen drohen. Der Arbeitnehmer kann insoweit verpflichtet sein, der Rechtsanwältin / dem Rechtsanwalt bzw. der Notarin / dem Notar aus dem allgemeinen Rücksichtnahmegebot (§§ 241, 242 BGB) Zutritt zum Home-Office-Arbeitsplatz auch während der Arbeitszeit zu gewähren. Etwaige Kontrollen werden mindestens 24 Stunden vorher angekündigt; der Arbeitnehmer erklärt sich grundsätzlich mit derartigen Kontrollen einverstanden und verpflichtet sich insoweit auch die mit ihm zusammen wohnenden Personen von der Möglichkeit etwaiger Kontrollen und damit einhergehender Betretungen seiner

Wohnung zu unterrichten. Kontrollmaßnahmen haben sich in jedem Fall auf den konkreten Heimarbeitsplatz zu beschränken. Soweit der Arbeitnehmer Kontrollen verweigert, kann dies die sofortige Beendigung der Heimarbeitsgenehmigung zur Folge haben. Der Rechtsanwalt / die Rechtsanwältin bzw. der Notar / die Notarin weist in diesem Zusammenhang darauf hin, dass er / sie in diesem Fall auch verpflichtet sein kann, insbesondere bei Gefahr im Verzug, staatliche Organe, wie etwa die Landesdatenschutzbehörde, die Polizei oder die Staatsanwaltschaft darum ersuchen kann, etwaige Betretungen zur Sicherstellung der Vertraulichkeit und/oder der Berufspflichten des Rechtsanwaltes / der Rechtsanwältin bzw. des Notars / der Notarin durchzuführen oder anzuordnen."

Weiterhin können – außerhalb des Datenschutzes – natürlich arbeitsrechtliche Regelungen erforderlich werden, beispielsweise im Zusammenhang mit der Arbeitsstättenverordnung und/oder sonstigen Verpflichtungen des Rechtsanwaltes / der Rechtsanwältin bzw. des Notars / der Notarin als Arbeitgeber.

Wir hoffen, Ihnen mit diesen Informationen weitergeholfen zu haben. Sollten gleichwohl Rückfragen verbleiben, melden Sie sich gerne!

Ihre

Juliane Kazemi und Dr. Robert Kazemi