# Editorial – Grußwort des Forschungsprojektleiters von «BayWiDI» Prof. Dr. Dirk Heckmann

Sehr geehrte Leserinnen und Leser,

das Jahr schreitet voran und seit Monaten müssen wir uns – teilweise von einem Tag zum nächsten – auf neue Regeln und Vorsichtsmaßnahmen einstellen. Bei den meisten mittel- bis langfristigen Planungen – Urlaube, Hochzeiten, Umzüge – muss ein großes Fragezeichen vermerkt werden. Neben Portemonnaie und Handy muss vor dem Verlassen des Hauses jetzt auch kontrolliert werden, ob eine frische Maske dabei ist.

So ungewöhnlich die Umstände und so sehr sie sich dennoch allmählich normalisieren: das Leben geht weiter. Aus diesem Grund hat die Forschungsstelle für IT-Recht und Netzpolitik (For..Net), an welcher auch das Projekt BayWiDI angesiedelt ist, beschlossen, nicht länger mit der Verleihung des ersten For..Net Media Awards zu warten. Zwar sind persönliche Kontakte besonders im Rahmen größerer Veranstaltungen nach wie vor zu meiden. Umso wichtiger ist nun die Vernetzung im digitalen Raum. Der Media Award wurde deshalb bei einem Online-Event mit Live-Abstimmung durch die Zuschauerinnen und Zuschauer an Ann Cathrin Riedel verliehen, die mit ihrem Newsletter „Ann Cathrin's Digital Digest" das Publikum überzeugte. Durch ihren Newsletter bringt sie ihren Abonnentinnen und Abonnenten komplexe Sachverhalte in einer konstruktiven, verständlichen Form näher und trägt so zu einer gemeinwohlorientierten Digitalisierung bei.

Genau diesem Gedanken möchten wir auch mit dieser Ausgabe des BayWiDI-Magazins Rechnung tragen: Zunächst wird Lukas Schmidt sich näher mit datenschutzrechtlichen Anforderungen und Problemen rund um das Thema Home-Office auseinandersetzen. Anschließend erwartet Sie ein Beitrag zu

möglichen neuen Perspektiven durch Pharma 4.0 von Luisa Lorenz. Felix Sobala gibt Ihnen 20 Schritte zu mehr Cybersicherheit im Home-Office an die Hand. Zuletzt ist Priska Katharina Büttel mit einem Überblick über vertrauenswürdige Informationsangebote rund um Covid-19 vertreten.

Ich wünsche Ihnen eine unterhaltsame Lektüre

Ihr Prof. Dr. Dirk Heckmann

*Leiter des Forschungsprojekts «BayWiDI»*

## Inhalt


- Home-Office – Datenschutz zwischen Couch und Kinderbetreuung / 2
- Digitalisierung und Vernetzung – Pharma 4.0 als (Corona-)Krisenlösung? / 5
- *My home(office) is my castle* – Ein „Crashkurs IT-Sicherheit" für zuhause in 20 einfachen Schritten. / 10
- Covid-19: Wegweiser für Informationsangebote / 13
- Leiter des Forschungsprojekts und AutorInnen / 16
- Impressum / 17

# Home-Office – Datenschutz zwischen Couch und Kinderbetreuung

Die Covid-19 Pandemie zwingt sowohl national als auch international vielerorts Millionen Menschen dazu, von ihrem angestammten Arbeitsplatz innerhalb der Betriebe in das Home-Office zu wechseln. Der wöchentliche Jour fixe verwandelt sich von einer mehr oder minder spannenden Präsenzveranstaltung in einen digitalen Video-Call auf den Plattformen dritter Anbieter wie beispielsweise Zoom, Skype oder Google Hangouts, die Aktenbearbeitung und Kundenbetreuung erfolgt, statt rein über die Server des Arbeitgebers, auch aus dem eigenen Wohnzimmer. Zwischen der berechtigten Sorge über das gesundheitliche Wohlergehen und den Erhalt des Arbeitsplatzes kann blinder Aktionismus vor allem den Bereich des Datenschutzes und damit einhergehende Haftungs- und Bußgeldgefahren ausblenden. Längst zeigen sich bei den verwendeten Drittprodukten sowohl datenschutzrechtliche als auch IT-sicherheitsbezogene Risiken, um deren Behebung die Betreiber bemüht sind.[1] Dieser Beitrag soll sowohl betroffenen Arbeitnehmern als auch Entscheidungsträgern eine erste Handreichung bieten, wie mit den sich verändernden Arbeitsbedingungen aus (datenschutz-) rechtlicher Sicht zu verfahren ist.

## I. Besteht eine generelle Pflicht zur Bereithaltung der Möglichkeit des Home-Office?

Das deutsche Recht sieht, im Gegensatz zu anderen Rechtsordnungen (exemplarisch sei auf das Gesetz der Arbeitsflexibilisierung der Niederlande verwiesen[2]), grundsätzlich keinen Anspruch des Arbeitnehmers auf Heimarbeit bzw. Telearbeit vor.[3] Vielmehr obliegt dem Arbeitgeber nach § 106 S. 1 GewO das Weisungsrecht, den Arbeitsort des Arbeitnehmers nach billigem Ermessen näher zu bestimmen. Ein Recht des Arbeitnehmers auf die Entsendung ins Home-Office besteht mithin gerade nicht. Anders als die Entsendung, Anordnung einer Dienstreise oder Versetzung bedarf die Entsendung ins Home-Office (als Unterkategorie der Telearbeit[4]) neben der Entschließung des Arbeitgebers wohl auch der Zustimmung des Arbeitnehmers.[5] Einseitig ist eine Anordnung nur in Ausnahmefällen denkbar, etwa wenn seitens des Betriebsrates einer dementsprechenden Betriebsvereinbarung zugestimmt wurde.[6] Bleibt der Arbeitnehmer eigenmächtig – aus Angst vor Ansteckung – dem bestimmten Arbeitsplatz fern, so kann dies im Zweifelsfall ein Grund für eine fristlose Kündigung nach § 626 Abs. 1 BGB darstellen, auch wenn *Hollo* es zumindest moralisch fraglich findet, dass in Zeiten einer grassierenden Pandemie die Ausnahme des Arbeitsweges aus den Ausgangsbeschränkungen und die Erledigung der Arbeit am betrieblichen Arbeitsplatz als sozialadäquat und mithin dem billigen Ermessen des § 106 S. 1 GewO entsprechend angesehen wird.[7] Erst wenn der Arbeitgeber in besonders grobem Maße seine arbeitsschutzrechtlichen Pflichten, resultierend aus § 618 BGB i.V.m. öffentlich rechtlichen Schutznormen, verletzt, könnte eine eigenmächtige Verlagerung der Arbeit in das Home-Office seitens des Arbeitnehmers angedacht werden.[8] Da das Vorliegen solcher Begebenheiten für den juristischen Laien jedoch schwerlich zu beurteilen sein dürfte, wird von der nicht anwaltlich begleiteten Wahrnehmung dieser Ausnahme abgeraten.

## II. Hardware- und Software-Anforderungen an die häuslichen Einrichtungen

Die DS-GVO stellt, sofern es sich um die professionelle Verarbeitung personenbezogener Daten handelt, grundsätzlich strenge Anforderungen an die zu verwendenden Hardware- und Software-Komponenten. Art. 32 DS-GVO sieht vor, dass der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese sogenannten technischen und organisatorischen Maßnahmen (TOMs) werden in der Regel auf heimischen IT-Systemen nicht zwangsläufig zu finden sein, da sie auch aus datenschutzrechtlicher Perspektive grundsätzlich für die Verarbeitung zu rein persönlichen und familiären Zwecken auch nicht nötig sind.[9]

Arbeitet der Arbeitnehmer von seinem Heimarbeitsplatz aus, so verbleibt der Arbeitgeber dennoch auch für diesen Bereich datenschutzrechtlich Verantwortlicher; der Arbeitnehmer hingegen ist in einer solchen Situation mit einem Auftragsverarbeiter i.S.d. Art. 28

**1** Vgl. Zoom schließt Sicherheitslücken, ZEIT Online vom 02.04.2020 (zuletzt abgerufen am 17.04.2020).

**2** *Schwiering/Zurel*, Das Homeoffice in der Arbeitswelt 2.0 – Rechtliche Rahmenbedingungen für Telearbeit, ZD 2016, 17 (18).

**3** *Imping* in Kilian/Heussen, Computerrechts-Handbuch, 34. EL Mai 2018, Abschnitt 70.11, Rn. 17.

**4** Grundsätzlich sind unter einem Telearbeitsplatz aus rechtlicher Perspektive ein vom Arbeitgeber fest eingerichteter Bildschirmarbeitsplatz im Privatbereich des Beschäftigten, für die der Arbeitgeber eine mit dem Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat, zu verstehen, § 2 Abs. 7 ArbStättV. Das derzeit vielfach praktizierte Home-Office wird jedoch in vielen Fällen unter Zuhilfenahme privater Telekommunikations- und IT-Einrichtungen stattfinden.

**5** *Maschmann* in BeckOGK, Stand 01.09.2018, § 106 GewO, Rn. 1.

**6** *Fuhlrott*, Arbeitsrechtliche Fragestellungen im Zusammenhang der Coronavirus-Epidemie, GWR 2020, 107 (108).

**7** *Hollo*, Kein Recht auf Homeoffice, LTO.de vom 15.04.2020 (zuletzt abgerufen am 17.04.2020).

**8** *Günther/Böglmüller*, COVID-19-Pandemie und Home-Office, ArbRAktuell 2020, 186 (187).

**9** *Etteldorf*, COVID-19 Special - EU Member State Data Protection Authorities Deal with COVID-19:
An Overview, EDPL 2020, 1 (8).

DS-GVO zu vergleichen.[10] Konkrete Hinweise der nationalen Datenschutzbehörden, welche Anforderungen dieser Wandel für die privaten Endgeräte der Arbeitnehmer aus datenschutzrechtlicher Sicht fordert, lassen derzeit auf sich warten. Lediglich der Bayerische Landesbeauftragte für den Datenschutz hat bezüglich der Nutzung von privaten Geräten bei der Verwendung für Videokonferenzen und Messengerdiensten bekannt gegeben, dass der Einsatz dann erlaubt sein soll, wenn keine Speicherung von sensiblen Daten auf dem Privatgerät erfolgt, die Kommunikation datensparsam erfolgt, das Gerät durch eine PIN oder ein Passwort geschützt werden kann und die personenbezogenen Daten mit Wegfall der Nutzung zu löschen sind.[11] Berechtigt kritisieren *Schröter/Zöllner* daher das Vorgehen der deutschen Datenschutzbehörden als ungenügend und bemängeln insbesondere, dass die gegebenen Handreichungen überwiegend eine bloße Umformulierung der Anforderungen der DS-GVO darstellen und wenig hinreichende praktische Umsetzungsbeispiele bieten.[12] Ein Blick auf die europäischen Nachbarländer lässt ein etwas besseres Bild der dortigen Datenschutzbehörden erkennen. Der polnische Datenschutzbeauftragte empfiehlt in Bezug auf die für das Home-Office genutzten Geräte:[13]

- Nur seitens des Arbeitgebers bereitgestellte Software auf den Geräten zu verwenden
- Aktualisierung der verwendeten Software, insbesondere der Antivirenapplikationen
- Bereithaltung eines gesonderten Arbeitsbereiches, welcher dem Zugriff Dritter entzogen ist
- Sperrung des Gerätes, sofern dieses unbeaufsichtigt bleibt
- Verwendung starker Passwörter und mehrstufiger Authentifizierung
- Bei Verlust oder Diebstahl sollte die Möglichkeit gegeben sein, aus der Ferne eine Datenvernichtung zu initiieren

Die österreichische Datenschutzbehörde empfiehlt überdies, eine geschützte Internetverbindung für die Kommunikation zu verwenden, keine beruflichen Daten auf privaten Geräten bzw. Cloud-Anwendungen zu speichern und auf den häuslichen Ausdruck von Dokumenten weitgehend zu verzichten bzw. angefallene Dokumente bei Notwendigkeit angemessen zu vernichten und nicht im Hausmüll zu entsorgen.[14] Für die Arbeit an heimischen Computereinrichtungen empfiehlt die niederländische Datenschutzbehörde, dass die Möglichkeit eingerichtet wird, dass sich der Arbeitnehmer über seinen privaten Computer auf dem Server des Arbeitgebers anmelden können sollte, um in der gleichen Software- und Serverumgebung wie am betrieblichen Arbeitsplatz zu arbeiten; sofern der Einsatz von Diensten Dritter nötig wird, z.B. für Videounterhaltungen, sind solche Anbieter zu verwenden, die ein hohes Datenschutzniveau aufweisen – empfohlen werden seitens der niederländischen Behörde Signal und FaceTime – und so wenig sensible Inhalte zu besprechen wie möglich.[15] Sofern auf private E-Mail-Provider zurückgegriffen werden muss (dies sollte in der Regel

**10** *Schwiering/Zurel*, Das Homeoffice in der Arbeitswelt 2.0 – Rechtliche Rahmenbedingungen für Telearbeit, ZD 2016, 17 (20).

**11** Vgl. *BayLfD*, Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie (zuletzt abgerufen am 17.04.2020).

**12** *Schröter/Zöllner*, Denn sie wollen wissen, was sie tun (dürfen) (zuletzt abgerufen am 17.04.2020).

**13** *Polnischer Datenschutzbeauftragter*, Schutz personenbezogener Daten während der Arbeit aus der Ferne (zuletzt abgerufen am 17.04.2020).

**14** *Österreichische Datenschutzbehörde*, Datensicherheit und Home-Office (zuletzt abgerufen am 17.04.2020).

**15** *Niederländische Datenschutzbehörde*, Während der Coronakrise sicher von zu Hause aus arbeiten (zuletzt abgerufen am 17.04.2020).

nicht der Fall sein), rät die irische Datenschutzbehörde dazu, Inhalte und Attachements verschlüsselt zu übermitteln und insbesondere keine personenbezogenen Daten in der Betreffzeile zu offenbaren.[16]

## III. Vertragliche Vereinbarung

Da der Arbeitgeber auch in Zeiten des Home-Office Verantwortlicher i.S.d. Datenschutzrechts nach Art. 7 Nr. 4 DS-GVO bleibt, ist es sinnvoll, die mit dem Arbeitgeber vereinbarten Vorgaben bezüglich des einzuhaltenden Datenschutzniveaus und der zu ergreifenden Schutzmaßnahmen vertraglich festzuhalten. Hiernach hat der Arbeitgeber den von der Verarbeitung Betroffenen auch weiterhin Auskunft gem. Art. 12 ff. DS-GVO zu geben. Der Arbeitgeber hat hierfür geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln, Art. 12 Abs. 1 S. 1 DS-GVO. Aus diesem Grund sollte der Arbeitnehmer vertraglich verpflichtet werden, Daten nur auf den Servern des Arbeitgebers zu speichern und nicht zu Hause, gleich ob in digitaler oder analoger Form, aufzubewahren; lokale Speicherungen und Aufbewahrungen sollten nur in sehr eng umgrenzten und genau definierten Fällen zugelassen werden, welche ihrerseits in einem Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO aufgeführt werden müssen.[17]

Um die Einhaltung der nach Art. 32 DS-GVO zu fordernden technischen und organisatorischen Maßnahmen (siehe Ausführungen unter Punkt II.) überprüfen zu können, sollte sich der Arbeitgeber überdies ein vertragliches Betretungsrecht der privaten Räumlichkeiten des Arbeitnehmers einräumen lassen. Um hierbei einen verhältnismäßigen Ausgleich zwischen den widerstreitenden Interessen zu finden, sollte dieses Recht nicht unbedingt eingeräumt, sondern an feste zeitliche Überprüfungszeitpunkte gebunden werden; außerplanmäßige Überprüfungen sollten nur in besonderen Verdachtsfällen und unter vorheriger Ankündigung (z.B. 24h im Voraus) zulässig sein.[18]

*Bergt* empfiehlt überdies, dass zur Vermeidung von Unsicherheiten ein vertragliches Zutrittsrecht der Datenschutzbehörden gem. Art. 58 Abs. 1 lit. f) DS-GVO für die Privatwohnungen der Arbeitnehmer vereinbart wird.[19] Dieses Recht ermöglicht den Aufsichtsbehörden, in ihren gesetzlichen Grenzen Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten. Dies ist sinnvoll, da die DS-GVO zwar grundsätzlich nicht das Betreten von reinen Privatwohnungen vorsieht, wohl aber von gemischt genutzten Räumlichkeiten[20]; eine explizite vertragliche Regelung macht die Unsicherheiten obsolet, ob es sich bei den für das Home-Office genutzten Privaträumlichkeiten um derartige gemischt genutzte Räume handelt, die dem Arbeitgeber als Verantwortlichen zugerechnet werden können. Ebenso ist eine Vereinbarung unter dem Gedanken des Arbeitnehmers als potentiellem Auftragsverarbeiter im Home-Office ratsam, da ein fehlendes Zutrittsrecht der Aufsichtsbehörden eine Auftragsverarbeitung verhindern würde.[21]

## IV. Fazit

Die Arbeit im Home-Office stellt aus datenschutzrechtlicher Perspektive sowohl Arbeitnehmer als auch Arbeitgeber vor Herausforderungen. Insbesondere darf sich der Arbeitgeber nicht darauf zurückziehen, dass der Datenschutz und die Vorhaltung geeigneter Maßnahmen nunmehr im Verantwortungsbereich des Arbeitnehmers lägen. Er hat vielmehr die Einhaltung zu überwachen und diese vertraglich zu regeln. Die Wirksamkeit eines ausreichenden Datenschutzrechts als elementare Verwirklichung des Rechts auf informationelle Selbstbestimmung muss sich insbesondere in Krisenzeiten beweisen. Umso verwunderlicher mutet es daher an, dass die Leopoldina, wenn auch in Bezug auf die Nutzung von Daten für sog. „Corona-Apps“, fordert, dass angesichts „der Erfahrung der derzeitigen Pandemie […] auf europäischer Ebene die Datenschutzregelungen für Ausnahmesituationen überprüft und ggfs. mittelfristig angepasst werden“ sollen. Die Ausnahmesituation einer gesundheitlichen Notlage darf nicht dazu führen, dass die informationellen Freiheitsrechte der Bürger sowohl seitens staatlicher Stellen als auch privater Unternehmen unverhältnismäßig beeinträchtigt werden.

*Lukas Schmidt*

**16** *Irische Datenschutzbehörde*, Protecting Personal Data When Working Remotely (zuletzt abgerufen am 17.04.2020).

**17** *Bergt* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, S. 357 f.

**18** Vgl. *Hoppe* in Kramer, IT-Arbeitsrecht, 2. Aufl. 2019, Rn. 676.

**19** *Bergt* in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, S. 360.

**20** *Polenz* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 58 Rn. 23.

**21** *Leopoldina*, Ad-hoc-Stellungnahmen zur Coronavirus-Pandemie (PDF), S. 7 (zuletzt abgerufen am 17.04.2020).

# Digitalisierung und Vernetzung – Pharma 4.0 als (Corona-)Krisenlösung?

**Pharma 4.0**: ein Schlagwort, das verglichen mit Begrifflichkeiten wie *Industrie 4.0, Big Data, Internet der Dinge* (Internet of Things, IoT) oder – thematisch differenzierter – *mHealth* bzw. *eHealth* innerhalb der rechtswissenschaftlichen Diskussion möglicherweise zwar seltener fällt, seinem Gehalt nach gleichwohl nicht minder bedeutsam ist. Denn die fortschreitende Digitalisierung nahezu aller rechtsrelevanter Bereiche erfasst ebenso den Gesundheitssektor, namentlich die Pharmaindustrie.

Zu nennen sind hierbei beispielsweise die Bereiche der sog. *Patient Centricity* („Patientenorientiertheit") oder die Individualisierung von Medikamenten. Bei ersterem handelt es sich um einen „Trend" im Gesundheitssektor, innerhalb dessen der Fokus im Rahmen entsprechender Leistungserbringungsprozesse nahezu gänzlich auf den Patienten verlagert wird: Ein Konzept, dessen Ziel es ist, in Abkehr zur reinen, gerade nicht individualisierten Gesundheitsleistung, den Erwartungen, Bedürfnissen und Wünschen von Patienten Raum zu geben, um mit den im Wege der Korrespondenz gewonnen Daten die Personalisierung von (Medizin-)Produkten und Leistungsangeboten zu gewährleisten.[1] In anderen Branchen, etwa dem Einzelhandel, ist die sog. *Customer Centricity* bereits integraler Bestandteil diverser Vertriebs- und Marketingstrategien.[2]

## I. Aktueller Bezug: Sars-CoV-2 stellt Deutschland vor Herausforderungen

Insbesondere dieser Tage, in denen das global zu medizinischen Herausforderungen führende Corona-Virus[3] respektive seine Auswirkungen schon bzw. noch sehr präsent sind, stellt sich die Frage, wie Vernetzung und Digitalisierung in Zeiten internationaler Betroffenheit einen schnellen, effektiven und gleichermaßen nachhaltigen, idealerweise gemeinsamen, Ausweg aus einer Pandemie[4] bewirken können.

So startete etwa das Netzwerk für Pharma Solutions (NetPhaSol), eine seit 2017 bestehende bundesweite Plattform für die Erforschung, Entwicklung und Vermarktung neuer Produkte, Technologien und Dienstleistungen mit 30 Unternehmen und 20 Forschungseinrichtungen aus Wirtschaft und Wissenschaft, im März 2020 die Kampagne „Find your Partner". Ein durch das Bundesministerium für Wirtschaft und Energie gefördertes Projekt, das Vernetzung und Kooperation forciert und damit beispielhaft für zahlreiche Initiativen, die kooperative Impf- und/oder Wirkstoffentwicklung – in diesem Falle primär hinsichtlich des Corona-Virus – voranzutreiben erstreben, steht. Denn bislang forsch(t)en Pharmaunternehmen weltweit oftmals isoliert an Impfstoffen und antiviralen Mitteln (d.h. solchen zur Behandlung bereits infizierter Patienten).

Als weiteres Projekt zu erwähnen ist der an einem Wochenende Ende März 2020 seitens der Bundesregierung und sieben sozialer Initiativen ausgerichtete Hackathon gegen Corona und für Digitalisierung (#WirVsVirus). Ziel dieses Hackathons war und ist es, die mit dem Corona-Virus einhergehende Herausforderung als Gesellschaft zu bewältigen, indem gemeinsam Lösungen entwickelt und zugleich Wege etabliert werden, erfolgsversprechende Lösungen sodann im digitalen Raum zu vernetzen und ausbauen zu können. Der auf Kontinuität ausgerichtete digitale Beteiligungsprozess brachte insoweit innerhalb von 48 Stunden 28.361 Menschen zusammen, die gemeinsam an über 1.500 Lösungen arbeiteten. Diesem vielversprechenden Startschuss schließt sich nun die eigentliche Projektarbeit in Form der Lösungs-Erprobung und nutzerzentrierten Umsetzung an. Die besten 20 Projekte erhielten direkt einen Platz im sog. *Solution Enabler Programm*. Dieses beinhaltet unter anderem programmatisch Begleitung und individuelles Coaching, unkomplizierte und bedarfsgerechte Versorgung mit Ressourcen, die schnelle Vermittlung von Expertise sowie Know-how, eine systematische Vernetzung, Clustering und (inter-)nationalen Austausch, um Synergieeffekte weiter nutzen zu können, Unterstützung bei der Pilotierung und Implementierung der Lösungen sowie finanzielle Förderung.[5] Neben den bereits qualifizierten 20 Teams konnten sich im Rahmen des dreistufigen Förderungsprozesses weitere Teams für das *Solutions Enabler Programm* bewerben. Auch standen Plätze für Teams und ggf. Einzelpersonen zur Verfügung, die zwar nicht am Hackathon teilnahmen, deren Lösungsansätze aber besonders relevant sind.

Während folglich drohende bzw. bereits akute Engpässe innerhalb pharmazeu-

1 *Niestroj*, Patient Centricity, Health&Care Magazin vom 19.06.2019, zuletzt abgerufen am 14.05.2020.

2 *Niestroj*, Health&Care Magazin vom 19.06.2019 (vgl. Fn. 1).

3 Offizieller Name des Virus laut WHO: Sars-CoV-2; Name der aus dem Virus resultierenden Lungenkrankheit: COVID-19.

4 Am 11.03.2020 stufte die Weltgesundheitsorganisation (WHO) COVID-19 offiziell als Pandemie ein, *WHO* vom 11.03.2020, zuletzt abgerufen am 14.05.2020.

5 Unterstützung nach dem #WirVsVirus Hackathon, zuletzt abgerufen am 14.05.2020.

tischer Lieferketten bevölkerungsübergreifend für Unruhe, Besorgnis und Angst sorgen, werden die längst nicht erschöpften Potentiale im Bereich der Digitalisierung/Vernetzung von Entwicklung- und Produktionsprozessen bzw. -ketten als den zentralen Entwicklungskonzepten des modernen medizinischen und pharmazeutischen Bereichs gerade in schweren Zeiten zu zukunftweisenden Hoffnungsträgern.

## II. Neue Perspektiven in der Pharmaindustrie dank Pharma 4.0

Das Phänomen Pharma 4.0 verlagert den Schwerpunkt von ehemals an festen Vorgaben ausgerichteten Produktionsprozessen hin zu intelligenten sowie vernetzen Systemen zur Echtzeitüberwachung, Simulation und Steuerung von Fertigungsprozessen.[6] Insoweit repräsentiert Pharma 4.0 jenen Teil des *Internet of Things*, der die Pharmaindustrie in all ihren Facetten beeinflusst. Konzeptionell handelt es sich um die Idee adaptiver und agiler Unternehmen, die sich neue – nach Möglichkeit individuell adaptierte – Technologien zu Nutzen machen, um Unternehmens- und Entscheidungsprozesse zu beschleunigen sowie in ihrer Flexibilität zu erhöhen. So ermöglichen leistungsstarke Systeme zur Gewinnung und Auswertung von Prozess- sowie Produktdaten die Verfügbarkeit wichtiger Informationen in Echtzeit, die sodann zur Optimierung nutzbar gemacht werden können.[7] Überdies erleichtern die entsprechenden Systeme die Einhaltung regulatorischer Anforderungen, welche etwa aus der sog. *Good Manufacturing Practice* (GMP), national verbindlichen Vorgaben oder einschlägigen EU-Richtlinien folgen.[8] Insgesamt verspricht die Produktion im Sinne von Pharma 4.0 dem zunehmend an Gewicht gewinnenden Bereich der personalisierten Medizin wegbereitend zu sein. Lösungen für Pharma 4.0 sind unter anderem *Smart Devices*, *Software as a Service* (SaaS), *Enterprise Manufacturing Intelligence* (EMI) oder *Big Data*. Im Ergebnis umfasst das Schlagwort Pharma 4.0 eine Fülle von Aspekten, die in Kombination für die Rettung weltweit akut bedrohter Menschenleben ein sehr hoffnungsvoller Lösungsweg zu sein scheinen. Und zwar ganz gleich, welcher Krankheitsauslöser im Einzelfall zu „bekämpfen" ist.

- ***Big Data*** als integraler Bestandteil der Digitalwirtschaft[9] meint den Umgang mit sehr großen Datenmengen, d.h. mit der Fülle an strukturierten und unstrukturierten Daten, die tagtäglich in Unternehmen anfallen und deren gezielte Auswertung und weitergehende Verarbeitung zusätzliche Erkenntnisgewinne und Prozessverbesserungen bringen kann.
- ***Enterprise Manufacturing Intelligence-Systeme*** (EMI-Systeme) sorgen für die Sicherstellung und intelligente Informationsdurchdringung in der unternehmensweiten Verfügbarkeit von Betriebsdaten und Leistungskennzahlen.[10]
- ***Software as a Service*** (SaaS) ist ein Teilbereich des Cloud Computings. Als Bereitstellungsmodell für Anwendungssoftware über das Internet und andere elektronische Netzwerke ist SaaS der technologische Nachfolger des A*pplication Service Providing* (ASP).[11] Folglich handelt es sich bei SaaS-Lösungen um das (entgeltliche) Angebot zur Nutzung von (regelmäßig Standard-)Software für einen vertraglich vereinbarten Zeitraum.[12]
- Bei ***Smart Devices***[13] handelt es sich um eigenständige, mit künstlicher Intelligenz ausgestattete Kleinstsysteme, die über das *Internet of Things* (IoT) vernetzt sind und mit anderen Smart Devices über WiFi, Bluetooth, Mobilfunk oder Nahfeldkommunikation (*Near Field Communication*, NFC) kommunizieren (können).[14] Als Beispiel zu nennen sind *Smart Watches*, digitale Sprachassistenten, *Smart Wearables*, Fitness-Tracker oder Hörgeräte. Zusammenfassend alle über die entsprechenden Sensoren verfügenden Alltagsgegenstände, die eigens erhobene Daten selbstständig verarbeiten können. *Smart Devices* werden sowohl im privaten Bereich als auch im Rahmen logistischer, industrieller oder produktionstechnischer Abläufe eingesetzt.
- ***Good Manufacturing Practice*** (GMP) („Gute Herstellungspraxis") bezeichnet als Oberbegriff die Gesamtheit der umfangreichen und differenzierten Vorgaben, die bei der Herstellung von Arzneimitteln zu beachten sind, mithin Grundsätze, die den hohen Standard der Qualität sowie Konformität von Arzneimitteln sichern sollen.[15]

Das **Corona-Virus** verdeutlichte unmittelbar, dass die Entwicklung neuer Impf- bzw. Wirkstoffe vor allem in Fällen unvorhergesehener Krankheitsszenarien nicht selten ein Wettlauf mit dem jeweiligen Erreger ist. Bereits am 25.03.2020 – d.h. rund zwei Wochen nach Einstufung des Corona-Virus als Pandemie – forschten nach Zählung des Verbands Forschender Arzneimittelhersteller 55 Unternehmen an Impfstoffen gegen Sars-CoV-2; daneben testen zahllose weitere Konzerne wenigstens den Krankheitsverlauf bzw. die Symptome

**6** Vgl. Handelsblatt-online vom 28.02.2020, Pharma 4.0 – die neuen Wege in der digitalen Pharma- und Biotechproduktion, zuletzt abgerufen am 14.05.2020.

**7** Fraunhofer-Institut für Produktionstechnologie IPT, Pharma 4.0, zuletzt abgerufen am 14.05.2020.

**8** Vgl. Fraunhofer-Institut für Produktionstechnologie IPT, Pharma 4.0 (vgl. Fn. 8).

**9** Weiterführend *Paal/Hennemann*, Big Data im Recht, Wettbewerbs- und daten(schutz)rechtliche Herausforderungen, NJW 2017, 1697.

**10** *Heinz/Krämer/Riemenschneider/Seeger*: Auf dem Weg zur allwissenden Fabrik – Vertikale Integration auf Basis kontinuierlicher Datenverarbeitung, Philipps-Universität Marburg, 2007, zuletzt abgerufen am 14.05.2020.

**11** *Stiemerling/Hirschmeier*, Software as a Service in der Praxis, Typische Konfliktfelder und Regelungsbedarf, ITRB 2010, 146.

**12** *Gennen/Laue* in Redeker, Handbuch der IT-Verträge, 40. Lieferung 02.2020, 1.17 Software as a Service (SaaS), Rn. 2.

**13** Weiterführend *Kremer*, Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, CR 2012, 438.

**14** ITWissen.info, Smart Device, zuletzt abgerufen am 14.05.2020.

**15** *Prinz*, Die Good Manufacturing Practice (GMP) und ihre fehlende Verbindlichkeit für Apotheken, PharmR 2012, 16, 17.

mildernde Medikamente.[16] Im Zuge dessen wurden ehemals für andere Krankheitsbilder entwickelte Arzneimittel, die derzeit noch erprobt werden oder bereits zugelassen sind, auf ihre Wirksamkeit im Kampf gegen das Corona-Virus getestet. Doch diese Forschungs- und Entwicklungsarbeit war und ist, das wurde schnell offenkundig, kein nationaler, stiller Alleingang. Vielmehr stehen die Zeichen auf weltweite Kooperation. Insbesondere die in den betroffenen Ländern oftmals zeitversetzt auftretenden, in Form und Intensität variierenden medizinischen Auswirkungen und Folgen einer Pandemie zeigen unverkennbar, dass in der Branche der Medikamentenentwicklung eine enge, kooperative Vorgehensweise angezeigt ist. Plötzlich arbeiten kleine Biotechfirmen mit großen Pharmakonzernen zusammen, staatliche Forschungsinstitute und private Organisationen stehen in regem Austausch. Auch die Weltgesundheitsorganisation (WHO) partizipiert. Die Gesundheitsforschung fördernde Stiftungen und Organisationen (wie etwa die Gates-Stiftung oder der britische Wellcome Trust) leisten Unterstützung finanzieller Art. Gemeinsames grenz- und institutionsübergreifendes (Inter-)Agieren scheint der Grundtenor der Pharmaindustrie in Zeiten pandemischer Zustände zu sein.

Deutlich wird, eine Krise wie die des Corona-Virus setzt gewaltige Ressourcen frei. Zeitgleich möchte ein jeder, der an der Forschung und Entwicklung beteiligt ist, freilich dennoch als erster Erfolge verzeichnen. Immerhin ist der Wettlauf mit dem Erreger auch ein solcher um viel Ruhm und Geld. Und letzteres vermag einer (mutmaßlich lediglich) pandemiebedingten Harmonie am ehesten gefährlich werden. Daher bleibt abzuwarten, ob und in welcher Form sich die in der Pandemie herausgebildeten Allianzen auf Dauer halten werden.

## III. Digitale Technologien im Gesundheitswesen: eHealth und mHealth

Neben den Potentialen von Pharma 4.0 sind langfristig bzw. mit Blick auf zukünftige, noch ungewisse Gesundheitsszenarien ferner die Phänomene des *eHealth* und des *mHealth* von zentraler Bedeutung. Denn beispielsweise sog. *Wearables* (direkt am Körper getragene Mini-Computer[17]), mittels derer Patientendaten nicht nur in Echtzeit überwachbar sind, sondern zugleich On-Demand-Analysen ermöglicht werden, versprechen gerade im Bereich der präventiven Krisenvermeidung oder zumindest -eindämmung, wertvolle Daten liefern zu können. Insgesamt aber sind sämtliche Medizinprodukte[18] geeignet, durch *eHealth* bzw. *mHealth* modifiziert und damit zu sog. smarten Produkten zu werden.

*Electronic Health*, kurz *eHealth*, meint (zusammenfassend) alle elektronisch unterstützten Aktivitäten und Systeme des Gesundheitswesens, wodurch Patientendaten sowie weitere medizinische Informationen über Entfernungen hinweg erhoben, verfügbar gemacht oder ausgewertet werden können.[19] Innerhalb der Autorenschaft wird *eHealth* tendenziell als Oberbegriff für die Summe elektronischer Anwendungen zur medizinischen Versorgung verwendet, wobei jedoch die definitorische Abgrenzung bzw. das teilweise synonyme Verständnis zu(r) „Telemedizin“ nicht einheitlich ist. Die Basis von *eHealth*-Anwendungen bilden moderne Informations- und Kommunikationstechnologien (IKT).

Demgegenüber steht *mHealth* verkürzend für „mobile Health“, mithin englisch für mobile Gesundheit. Als Untergruppe von *eHealth*-Aktivitäten

**16** *Bahnsen/Buchter/Malcher/Tatje*, Die Weltenretter, ZEIT Online vom 25.03.2020, zuletzt abgerufen am 14.05.2020.

**17** Hierzu im Detail *BSI*, Wearables – direkt am Körper getragene Mini-Computer, zuletzt abgerufen am 14.05.2020.

**18** Gemäß § 2 Abs. 1 Medizinproduktgesetz (MPG, in der konsolidierten Fassung vom 04.04.2020, BGBl. I Nr. 23/2020) sind **Medizinprodukte** insoweit alle Instrumente, Apparate, Vorrichtungen, Software, Stoffe oder anderen Gegenstände, einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinprodukts eingesetzten Software, die vom Hersteller zur Anwendung für Menschen für die in Nr. 1 bis 4 normierten Zwecke verwendet werden und deren bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann; Hinsichtlich der Gesetzeslage auf **europäischer Ebene** vgl. (noch) Art. 1 Abs. 2 lit. a) Medizinprodukte-RL (RL 93/42/EWG). Diese Richtlinie wird jedoch ab dem 26.05.2020 von der am 25.05.2017 beschlossenen Medizinprodukte-VO (EU 2017/745) abgelöst. Die entsprechend dieser Verordnung geltende Definition der Medizinprodukte normiert dann Art. 2 Nr. 1 Medizinprodukte-VO.

**19** *Matusiewicz/Thielscher*, Electronic Health (E-Health) und Mobile Health (mHealth) – Ein Definitionsversuch, in: Die Digitale Transformation im Gesundheitswesen, MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, 2017, S. 3.

und -Systemen vereint der Begriff hierbei all jene medizinischen Angebote, die auf mobilen Geräten (etwa Computern, Smartphones, Tablets und ähnlichen Endgeräten) verfügbar sind, wobei im Rahmen der entsprechenden Kommunikationsprozesse Mobilfunktechniken sowie mobile und drahtlose Technologien zum Einsatz kommen.[20] Ziel dieser Innovation ist es, mittels der Verbindung von IT und mobilen Technologien die medizinische Versorgung flächendeckend nachhaltig auszubauen (insbesondere in ländlichen und strukturschwachen Regionen) sowie zu verbessern. Damit einher geht der Gedanke, vor allem Personen/Patienten, die zu privaten Zwecken auf *mHealth*-Software zurückgreifen, zu mehr Verantwortung im Umgang mit der eigenen Gesundheit zu verhelfen, mithin die allgemeine Gesundheitskompetenz zu schulen. Dies ist allem voran mit Blick auf den demographischen Wandel angezeigt.

Die Einsatzbereiche von *mHealth*-Lösungen sind derzeit thematisch bzw. qualitativ vielschichtig und variieren daher stark in ihren Adressatengruppen. Professionelle Angebote, die nicht etwa nur dem Fitness-Tracking dienen oder (breiten-)sportliche Thematiken zum Inhalt haben (sog. „Gesundheits-Apps“[21]), umfassen sämtliche Versorgungsbereiche, namentlich die der Prävention, Diagnostik, Therapie und Nachsorge, das Monitoring von Patienten sowie im Einzelfall Wellnessthemen; überdies versprechen *mHealth*-Angebote den administrativen Bereich (beispielsweise das Praxis- oder Klinikmanagement) zu unterstützen.[22]

- Von **Medizin-Apps** (*Medical Apps*) fokussierte Nutzer sind insbesondere Patienten und/oder deren Angehörige sowie (berufsbedingt) Angehörige von Heilberufen.[23] Ziel ist es vor allem, die Nutzer im Rahmen ihres Genesungs- und Behandlungsprozesses zu unterstützen.
- Reine **Gesundheits-Apps** (*Health Apps*) hingegen richten sich vordergründig an gesunde Nutzer und sollen – mit Blick auf einen gesunden Lebensstil – der Selbstvermessung sowie Selbstoptimierung dienen.[24]
- **Lifestyle-Apps** als Unterfall der Gesundheits-Apps dienen ihrer Konzeption nach der Lebenserleichterung und Unterstützung gesunder und aktiver Menschen.[25] Ausweislich Erwägungsgrund 19 der europäischen Medizinprodukte-VO[26] handelt es sich bei Apps dieser Art jedoch ausdrücklich nicht um Medizinprodukte.

Potentielle Adressaten des jeweiligen Medizinproduktes sind infolge dessen sowohl Krankenkassen und Leistungserbringer als auch (schlicht) anderweitig Interessierte sowie Patienten bzw. Versicherte. Nachdem die Rechtslage nach wie vor unsicher ist, besteht der Markt für *mHealth*-Angebote derzeit (noch) überwiegend aus privaten Anbietern (sog. zweiter Gesundheitsmarkt). Der sukzessive Einstieg von Krankenkassen, Körperschaften und anderen Kostenträgern wird das Marktpotential entsprechender Produkte jedoch zukünftig gewiss beeinflussen, nachdem die wirtschaftliche Bedeutung dieses Industriezweiges bereits jetzt enorm ist.

Deutlich wird, dass anlässlich des Einsatzes von *eHealth* und/oder *mHealth* aufgrund der produkttypischen Konzeption denknotwenig zahlreiche, größtenteils (höchst) sensible personenbezogene (Gesundheits-)Daten verarbeitet werden. Neben den Disziplinen der Medizin bzw. der medizinischen Informatik, der Versorgungsforschung, der Kommunikationswissenschaft sowie Betriebs- und Volkswirtschaftslehre spielt demzufolge auch die Rechtswissenschaft, namentlich die Bereiche der IT-Sicherheit und des Datenschutzes, eine entscheidende Rolle. Und die Regelungsprämissen dieser Bereiche variieren zum Teil stark.

## IV. Datenschutzrechtliche Aspekte: Gesundheitsdaten und Ortungsdaten im Fokus

Sensible Gesundheitsdaten werden spontan oftmals mit Informationen über individuelle Krankheitsparameter assoziiert. Dabei ist bereits die bloße Auskunft oder Diagnose, dass der „Patient“ hinsichtlich einzelner Bereiche bzw. insgesamt als „gesund“ gilt, ein wertvolles Datum. Der Verlauf und die Dauer der Behandlung, die zum Einsatz kommende Medikation sowie eine (anhaltende) Genesung bzw. Immunisierung sind gleichwohl nicht selten im zentralen Blickfeld der diese Angaben abfragenden Stellen.[27]

Die Erfahrungen mit **Sars-CoV-2** zeigen, dass Digitalisierung und Gesundheit aus datenschutzrechtlicher Sicht nicht denknotwendig nur klassische Gesundheitsdaten wie beispielsweise Symptome oder Diagnosen als Schnittmenge haben. Vielmehr erhalten im

**20** Vgl. *Matusiewicz/Thielscher*, MWV 2017, S. 5 (vgl. Fn. 19).

**21** Vertiefend hierzu, insbesondere hinsichtlich der regulatorischen und wettbewerbsrechtlichen Einordnung von Apps und anderer *mHealth*-Software: *Dietel/Lewalter*, mHealth-Anwendungen als Medizinprodukte – Vereinbarkeit mit dem HWG und Ausblick auf die neue EU-Medizinprodukteverordnung, PharmR 2017, 53.

**22** *Matusiewicz/Thielscher*, MWV 2017, S. 5 (vgl. Fn. 19).

**23** *Klemperer/Schott/Aly/Lieb*, Medizinische Apps: Vorsicht vor dem Einfluss kommerzieller Interessen der Hersteller in Arzneiverordnung der Praxis, 2018, S. 5, zuletzt abgerufen am 14.05.2020.

**24** Vgl. *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Gesundheits-Apps (PDF), 2019, zuletzt abgerufen am 14.05.2020.

**25** Weiterführend zu den Lifestyle-Apps vgl. etwa *Jandt/Hohmann*, Life-Style-, Fitness- und Gesundheits-Apps - Laufen Datenschutz und Vertraulichkeit hinterher?, DSRITB 2015, 17.

**26** ErwGr. 19 der Medizinprodukte-VO: „Es muss eindeutig festgelegt werden, dass Software als solche, wenn sie vom Hersteller speziell für einen oder mehrere der in der Definition von Medizinprodukten genannten medizinischen Zwecke bestimmt ist, als Medizinprodukt gilt, während **Software für allgemeine Zwecke**, auch wenn sie in Einrichtungen des Gesundheitswesens eingesetzt wird, sowie **Software, die für Zwecke in den Bereichen Lebensstil und Wohlbefinden** eingesetzt wird, **kein Medizinprodukt** ist. Die Einstufung der Software entweder als Produkt oder als Zubehör ist unabhängig vom Ort der Software und von der Art der Verbindung zwischen der Software und einem Produkt.“

**27** Zu den datenschutzrechtlichen Aspekten von Medizinprodukten *Ortner/Daubenbüchel*, Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918.

Kontext der Covid-19-Ausbreitung auch weitere personenbezogene Daten, namentlich Ortungsdaten und Bewegungsmuster, nun einen Aussagewert mit Gesundheitsbezug.

Denn ein bislang erstmals sowie einzig anlässlich der **Corona-Pandemie** gleichermaßen umfassend wie kontrovers diskutiertes Thema war das der **Handyortung**, wodurch Infizierte und Kontaktpersonen ermittelt werden sollten, um die Ausbreitung des Virus einzudämmen. Bereits zuvor hatten andere Länder ähnliche Wege eingeschlagen, etwa das israelische Gesundheitsministerium, das eine App entwickeln ließ, die Nutzer hinsichtlich des Kontaktes mit nachweislich Corona-Infizierten informieren sollte; dabei gestattete Israel dem Geheimdienst, Überwachungstechnologien einzusetzen, die eigentlich der Terrorbekämpfung vorbehalten waren.[28]

Während sich Singapur und Österreich für Apps, die Bluetooth-Handshakes auswerten, entschieden, setzte China auf Kontrolle primär in Form von Gesichtserkennung.[29] Hingegen wurde hierzulande unter anderem diskutiert, ob und in welcher Form freiwillig[30] zur Verfügung gestellte Bewegungsdaten nutzbar gemacht werden können.

Seit dem 07.04.2020 ist die sog. Corona-Datenspende-App des Robert Koch Instituts für iOS und Android-Geräte verfügbar. Nach Aussage ihrer Initiatoren soll die auf freiwilliger Basis zu nutzende App – die in Kombination mit Fitnessarmbändern und Smartwatches verschiedener Hersteller funktioniert – ergänzende Informationen dazu liefern, wo und wie schnell sich das Corona-Virus national ausbreitet.[31] Auch die Corona-Warn-App der Bundesregierung, die von der Deutschen Telekom und SAP in Zusammenarbeit mit dem Robert-Koch-Institut entwickelt wurde, ist inzwischen verfügbar und wurde bereits 15,6 Mio. Mal heruntergeladen.[32] Wenngleich seitens der Bundesregierung derzeit **kein spezifisches Gesetz für die App** geplant ist, könnte ein solches im Hinblick auf eine möglicherweise drohende (rechtswidrige) Diskriminierung von Nicht-Nutzern in Form eines faktischen Nutzungszwangs künftig noch folgen.[33] Eine Gruppe renommierter Datenschützer veröffentlichte jedenfalls schon jetzt einen entsprechenden Gesetzesentwurf.[34]

Aus datenschutzrechtlicher Sicht ist insbesondere an die durch Art. 35 Abs. 1 Satz 1 DS-GVO vorgeschriebene Datenschutz-Folgenabschätzung zu denken, die immer dann durchzuführen ist, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies wäre bei der Corona-App zweifellos der Fall. Bisher erfolgte von offizieller Seite zwar eine derartige Folgenabschätzung, diese wird jedoch heftig kritisiert.[35]

## V. Fazit und Ausblick

Zweifelsfrei eignet sich Pharma 4.0 neben der Verbesserung der medizinischen Versorgungsleistung auch dazu, Wettbewerbsvorteile zu generieren. Allerdings nicht nur. Denn Pharma 4.0 ist gemeinsam mit den anderen Erscheinungsformen der Digitalisierung und Vernetzung Teil einer komplexen Gemengelage diverser Interessen(gruppen), deren Belange – trotz oder gerade wegen der wirtschaftlichen Potentiale von Digitalisierung und Vernetzung – umfassend zu berücksichtigen und zu würdigen sind.

Die Corona-Krise hat die Welt zusammenrücken lassen – und zwar gerade nicht physisch-persönlich, sondern mitmenschlich helfend und auf digitalem Weg. Die digitalen Netze Europas sind gefragter denn je, die Digitalisierung und Vernetzung zahlreicher Gesellschaftsbereiche in pandemischen Zeiten nahezu überlebensnotwendig. Gleichwohl dürfen selbst (medizinische) Extremsituationen nicht dazu verleiten, gewichtige Prinzipien zu missachten und (grund-)rechtliche Vorgaben zu ignorieren. Die unzähligen Potentiale der Digitalisierung repräsentieren spiegelbildlich zugleich die Fülle an in (mindestens) ebenso großer Zahl vorhandenen Missbrauchspotentialen.

*Luisa Lorenz*

**28** tagesschau.de, Hilft das Handy im Kampf gegen Corona?, 29.03.2020, zuletzt abgerufen am 14.05.2020.

**29** tagesschau.de vom 29.03.2020 (vgl. Fn. 28).

**30** Zu der Frage, ob Bürger zur Nutzung entsprechender Apps verpflichtet werden könnten, *Theurer*, Zugriff auf Handydaten in der Corona-Krise?, DRiZ 2020, 172.

**31** Pressemitteilung des Robert Koch-Instituts vom 07.04.2020, Mit Daten von Fitnessarmbändern und Smartwatches mehr über die Verbreitung des Coronavirus erfahren, zuletzt abgerufen am 14.05.2020.

**32** Statista, Anzahl der Downloads der Corona-Warn-App über den Apple App Store und den Google Play Store in Deutschland im Juli 2020, 13.07.2020 (zuletzt abgerufen am 16.07.2020).

**33** *Greis*, Corona-App soll Mitte Juni starten, golem.de vom 07.05.2020, zuletzt abgerufen am 14.05.2020.

**34** *Engeler/Marnau/Bendrath/Geuter*, Vorschlag für ein Gesetz zur Einführung und zum Betrieb einer App-basierten Nachverfolgung von Infektionsrisiken mit dem SARS-CoV-2 (Corona) Virus (PDF), Version 1.0, 03. Mai 2020, zuletzt abgerufen am 14.05.2020.

**35** *Bock et al.*, Kritik an Datenschutzfolgenabschätzung für die Corona-Warn-App, Netzpolitik.org, 29.06.2020; *FIfF Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.*, Pressemitteilung vom 29.06.2020, jeweils zuletzt abgerufen am 15.07.2020.

# *My home(office) is my castle* – Ein „Crashkurs IT-Sicherheit" für zuhause in 20 einfachen Schritten.

## A. Corona-bedingte Entwicklungen

Aufgrund der Schutzmaßnahmen zur Verlangsamung der weiteren Ausbreitung des Corona-Virus (SARS-Cov-2) verlagern viele Menschen ihre Arbeit ‚ins Home-Office'. Für manche Menschen war das im Rahmen von Telearbeit oder mobilem Arbeiten[1] schon Alltag; für andere ist das Neuland[2] – eine Situation, auf die es kurzfristig und dennoch angemessen zu reagieren gilt. Die unbeliebtesten Ratschläge in derlei akuten Situationen sind solche, die einem mit dem Seitenhieb, man habe schon immer auf den Vorbereitungsbedarf hingewiesen und vor den Gefahren gewarnt, gegeben werden, obwohl ‚das Kind jetzt in den Brunnen gefallen ist': Wer kennt nicht den Ratschlag der regelmäßigen Backups, wenn wichtige Daten erst unwiederbringlich verloren sind. Hilfe sieht in solchen Momenten anders aus. Umso komfortabler und ergreifenswerter ist doch eigentlich die Chance, die sich in der gegenwärtige Situation bietet: Eine Vielzahl von Unternehmen und Angestellten sind nun erstmalig und teils unvorbereitet mit der Home-Office-Gegebenheit konfrontiert und müssen nun mit der Situation umgehen.[3] Das bietet die Möglichkeit, *mit* den anderen ebenfalls Betroffenen zu lernen und – sollte einmal etwas nicht direkt perfekt umgesetzt werden – verständnisvoller behandelt zu werden, aber auch selber *mit anderen* nachsichtig in dieser Ausnahmesituation umzugehen. Und schließlich spricht nichts dagegen, im Anschluss an diese Ausnahmesituation auch langfristig den entsprechenden Rahmen in Form von Leitlinien, Maßnahmen, Strategien und Anweisungen für das Home-Office (unternehmensseitig) zu etablieren und in die Form von Dienst-/Betriebs- oder individualvertraglichen Vereinbarungen zu „gießen". Bis dahin kann dieser Crashkurs in 20 Schritten Ihnen kurzfristig helfen.

## B. Maßnahmeempfehlungen

Eben aufgrund dieser Breitenwirkung des Home-Office-Phänomens haben eine Vielzahl von Institutionen Handreichungen herausgebracht, mit Hilfe derer Betroffene auf wichtige Aspekte, die es (auch und gerade) im Home-Office zu beachten gilt, aufmerksam gemacht werden.[4] Neben teils arbeitsrechtlichen Aspekten thematisieren diese vor allem datenschutz- und IT-sicherheitsrechtliche Aspekte. In diesem Beitrag möchten wir Ihnen einen Überblick[5] über die empfohlenen grundsätzlichen Maßnahmen geben, die maßgeblich zum Schutz aus IT-sicherheitsrechtlicher Perspektive, also zur Herstellung und Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Systeme[6] beitragen können.[7]

## I. Online-Tool „Virus fördert Viren"

Eine gelungene Art, Betroffene ‚an die Hand zu nehmen' und mit ihnen die wichtigsten Schritte für eine bessere IT-Sicherheit durchzugehen, bietet das Online-Tool „Virus fördert Viren".[8] Dieses Tool, eine Website, die im Rahmen des Hackathons *#WirVersusVirus*[9] entwickelt wurde, fragt interaktiv IT-sicherheitsrelevante Aspekte dezidiert technischer Natur ab und gibt zu diesen Tipps.

## II. Maßnahmen

Für alle, die lieber eine schriftliche Checkliste mögen, hier ein Überblick über die wichtigsten Überlegungen und Handlungsempfehlungen:

---

**1** Vgl. zu diesen Begrifflichkeiten *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*, Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser, Stand: Januar 2019 (zuletzt abgerufen am 25.04.2020), S. 5.

**2** Für Zahlen zu IT-Sicherheitsmaßnahmen, die im Home-Office Tätige laut einer Umfrage bisher getroffen haben, siehe *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Pressemitteilung – Deutschland-Umfrage »IT-Sicherheit im Home Office«, 31.03.2020, abrufbar unter: https://www.teletrust.de/presse/pressemitteilungen/it-sicherheit-im-home-office/ (zuletzt abgerufen am 25.04.2020).

**3** Laut des Digitalverbandes BITKOM wurde bei jedem dritten Beschäftigten erstmals Home-Office eingeführt, siehe *Pauly/Holdampf-Wendel*, Corona-Pandemie: Arbeit im Homeoffice nimmt deutlich zu, 18.03.2020 (zuletzt abgerufen am 25.04.2020).

**4** Siehe als Auswahl an Handreichungen, die dieser Übersicht zugrunde liegen: *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*, Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser (vgl. Fn. 1); *EU Agency for Cybersecurity's (ENISA) Executive Director, Lepassar*, Top Tips for Cybersecurity when Working Remotely; *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Home-Office? – Aber sicher! mit Tipps für sicheres mobiles Arbeiten; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)*, Datenschutz: Plötzlich im Homeoffice – und nun? (PDF); jeweils zuletzt abgerufen am 25.04.2020. Für eine Übersicht über die Handreichungen und Empfehlungen der Datenschutzbehörden auf internationaler Ebene siehe *Etteldorf*, COVID-19 Special – EU Member State Data Protection Authorities Deal with COVID-19: An Overview, EDPL 2020, 1.

**5** Selbstverständlich erhebt diese Darstellung nicht den Anspruch eines abschließenden und allumfassenden Überblicks. Je nach individuellem Einsatzszenario und Arbeitsbereich können andere Maßstäbe und Maßnahmen erforderlich sein. Bitte klären Sie gegebenenfalls für Sie relevante Besonderheiten mit Ihren Vorgesetzten ab; bei dem vorliegenden Überblick handelt es sich lediglich um grundsätzliche Empfehlungen!

**6** Vgl. Art. 32 Abs. 1 lit. b DS-GVO.

**7** Vgl. hinsichtlich der Anforderungen insbesondere Art. 32 sowie Art. 25 Abs. 1 DS-GVO.

**8** Siehe https://virus-foerdert-viren.netlify.com (zuletzt abgerufen am 25.04.2020).

**9** Siehe dazu *Bundesregierung*, Fragen und Antworten zum Hackathon #WirVersusVirus (zuletzt abgerufen am 25.04.2020).

### Generelle Überlegungen

1. Verwenden Sie (möglichst) die **IT (Geräte und Software) Ihres Unternehmens** und (möglichst) lediglich für berufliche Zwecke.
2. Bedarf es überhaupt dringend einer Verarbeitung von **personenbezogenen[10] oder geheimen Daten**, oder lässt sich diese verschieben? Arbeiten Sie zunächst mit Daten ohne Personenbezug[11] oder besonderer Relevanz, um sich an die neue Situation und die neuen Regelungen zu gewöhnen.
3. Grundsätzlich gilt: **Vermeiden** Sie die Verarbeitung (möglichst) **geheim zu haltender und personenbezogener Daten[12] – „je sensibler und damit schützenswerter personenbezogene Daten sind, desto stärker sind sie zu schützen"**[13].

### Organisatorische Maßnahmen

4. Klären Sie, welche **Kommunikationskanäle** (Messenger, E-Mail-Dienste oder beispielsweise Videokonferenz-Software[14]) wie und wozu genutzt werden dürfen.
5. Klären Sie die Kontaktmöglichkeiten, an die Sie sich im Falle von technischen Problemen, Daten- oder Geräteverlusten oder Fragen wenden können.
6. Vermeiden Sie Medienbrüche, arbeiten Sie möglichst **nur mit einem Medium**, um die Orte, an denen wichtige Daten festgehalten sind, zu minimieren.
7. Führen Sie regelmäßig **Datensicherungen** (möglichst im Rahmen der Infrastruktur Ihres Unternehmens, gegebenenfalls über einen Online-Zugriff[15]) durch; vermeiden Sie hingegen (möglichst) das Speichern personenbezogener oder geheimer Daten auf privater IT[16].
8. Verwenden Sie **sichere Passwörter und Persönliche Identifikationsnummern (PIN)**.[17]
9. Schützen Sie Ihre Monitore durch **Sichtschutzfolien**.

### Technische Maßnahmen

10. Verwenden Sie – je nach Gerät und Betriebssystem entsprechende – **Schutzsoftware wie Virenscanner und Firewalls**.
11. Halten Sie die **Software** all ihrer Geräte[18], insbesondere Betriebssysteme, Firewalls und Anti-Viren-Programme **auf dem neuesten Stand** und achten Sie auf **aktuelle Warnungen** des Bundesamtes für Sicherheit in der Informationstechnik.[19]
12. **Sperren** Sie Ihren **Bildschirm** – sowohl durch eine automatische Funktion durch Zeitablauf als auch immer manuell, wenn Sie den Arbeitsbereich verlassen.
13. **Sichern** Sie Ihr **WLAN und** Ihren **Router** durch sichere Passwörter ab.[20]
14. Nutzen Sie Möglichkeiten der **Zwei-Faktor-Authentisierung**.[21]
15. Nutzen Sie Möglichkeiten sicherer **Virtual Private Networks (VPN)**, um auf Ressourcen Ihres Unternehmens zuzugreifen.

**10** Für eine Definition siehe Art. 4 Nr. 1 i.V.m. ErwGr. 26 S. 3 f. DS-GVO.

**11** Vgl. für eine Definition anonymer Informationen ErwGr. 26 S. 5 DS-GVO.

**12** Entsprechend dem Datenverarbeitungsgrundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO: „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt […] („Datenminimierung")".

**13** *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)*, Telearbeit und Mobiles Arbeiten – Ein Datenschutz-Wegweiser (vgl. Fn. 1), S. 10, vgl. dazu insgesamt S. 6–10.

**14** Zur aus datenschutz- wie auch aus IT-sicherheitsrechtlicher Sicht nicht unumstrittenen Videokonferenz-Software Zoom siehe für eine datenschutzrechtliche Einschätzung *Roßnagel*, Zoom und Datenschutz (PDF), 03.04.2020, sowie aus IT-Sicherheitsperspektive *Ries*, Videokonferenz-Software: Ist Zoom ein Sicherheitsalptraum? UPDATE, 02.04.2020 (jeweils zuletzt abgerufen am 25.04.2020).

**15** Siehe dazu auch 15.

**16** Vgl. 1., 2. und 3 und insbesondere auch 18.

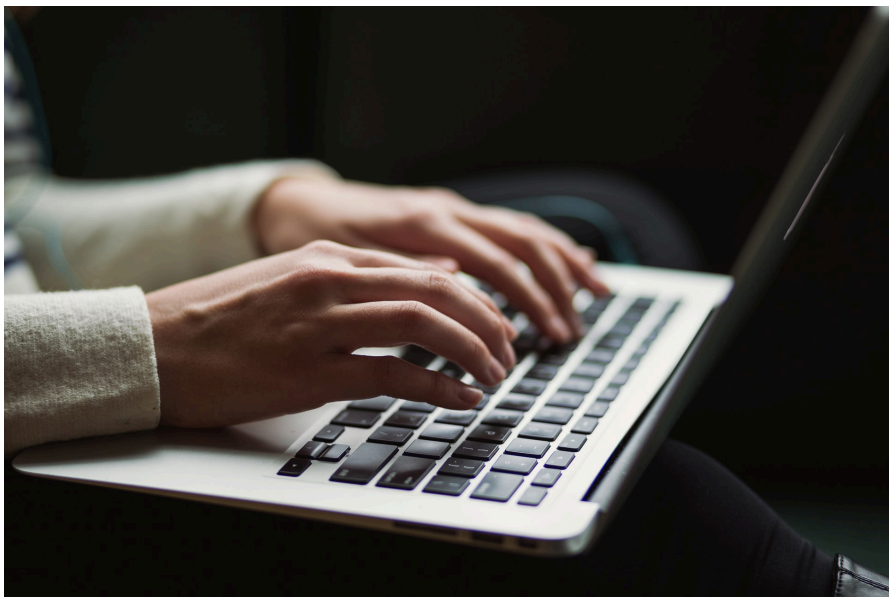
**17** Siehe dazu grundsätzlich *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, IT-Grundschutz-Kompendium Edition 2020 (zuletzt abgerufen am 24.04.2020) unter ORP.4.A8 sowie ORP.4.A22; als schnelle Anleitung siehe *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Sichere Passwörter – Faktenblatt, 01.02.2019 (zuletzt abgerufen am 24.04.2020).

**18** Damit sind neben Computern insbesondere auch (WLAN-)Router, Handys, aber auch andere Geräte gemeint, die über eine eigenständige Software und eine Verbindung zum Internet verfügen.

**19** Diese sind abrufbar unter: https://www.bsi.bund.de/DE/Service/Aktuell/aktuelles_node.html.

**20** Vgl. dazu 8. und Fn. 17.

**21** Vgl. dazu auch im Zusammenspiel 8.



16. **Verschlüsseln** Sie Ihre IT-Systeme wie Computer, Handys, insbesondere auch Festplatten und USB-Sticks.
17. Achten Sie auf eine **Ende-zu-Ende-Verschlüsselung**, falls Sie Messenger-Dienste verwenden.[22]
18. Verwenden Sie **keine privaten Festplatten oder USB-Sticks**, um das Risiko von Schadsoftware zu verringern.[23]

**Besondere Vorsichtsmaßnahmen im thematischen Zusammenhang mit der Corona-Pandemie**

19. Reagieren Sie **besonnen und hinterfragen Sie Mails oder Webseiten, die Sie (insbesondere im Zusammenhang mit der Corona-Pandemie) zur Angabe persönlicher Informationen animieren wollen.**[24] Klicken Sie (möglichst) nicht auf Links in E-Mails und öffnen Sie (möglichst) keine E-Mail-Anhänge. Seien Sie grundsätzlich bei E-Mails skeptisch; Absenderadressen lassen sich leicht ‚fälschen' oder irreführend darstellen. Versuchen Sie – falls Sie die Anliegen nicht als offensichtlich unbegründet und missbräuchlich identifizieren können – auf alternativem Wege die Absender und Anliegen zu verifizieren.
20. Informieren Sie sich über aktuelle Geschehnisse und Nachrichten zur Corona-Pandemie durch **etablierte und offizielle Kommunikationswege**[25], seien Sie vorsichtig bei alternativen Angeboten.[26]

## C. Ausblick

Vielleicht musste die Einrichtung Ihres Home-Office schnell gehen und Sie waren nicht darauf vorbereitet. Wir hoffen, Ihnen mit diesem Überblick die wichtigsten Aspekte und Maßnahmen für IT-Sicherheit im Home-Office haben aufzeigen zu können, möchten Sie jedoch zum Schluss nochmals darauf hinweisen, dass natürlich die Anweisungen Ihres Dienstvorgesetzten im Zweifel Vorrang vor unseren allgemeinen Empfehlungen haben, die zu treffenden Maßnahmen immer auch dem jeweiligen Arbeitsbereich und der jeweiligen Situation angemessen angepasst und getroffen werden müssen. Sollte sich – was wir alle nicht hoffen, aber in Anbetracht des Umfangs und der Auswirkungen der Pandemie derzeit durchaus realistisch erscheint – der Ausnahmezustand noch über eine längere Zeit erstrecken, sollten seitens des Unternehmens klare Regelungen zum Home-Office, insbesondere hinsichtlich technischer und organisatorischer Maßnahmen (TOMs), getroffen werden. Schützen Sie sich und den womöglich neuen Teil ihres *castles*, das Home-Office, und bleiben Sie gesund!

*Felix Sobala*

**22** Vgl. dazu auch 4.

**23** Vgl. dazu auch 1. und 7.

**24** Siehe dazu *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Vorsicht Phishing: Die Corona-Krise als Köder sowie Wie schützt man sich gegen Phishing? und allgemeiner zur Funktionsweise von Phishing Passwortdiebstahl durch Phishing (jeweils zuletzt abgerufen am 25.04.2020); zur konkreten Situation insbesondere auch *Verbraucherzentrale Nordrhein-Westfalen*, Achtung, Phishing! Wie Betrüger die Corona-Krise in E-Mails nutzen, 18.03.2020 (zuletzt abgerufen am 25.04.2020).

**25** Zum Beispiel über die Webseite des Robert-Koch-Instituts (zuletzt abgerufen am 25.04.2020).

**26** So wurde zum Beispiel von ‚gefälschten' digitalen Karten zur Ausbreitung des Corona-Virus berichtet, die als Vorwand zur Verbreitung von Schadsoftware genutzt wurden, siehe *Kerkmann*, Der perfekte Köder: Cyberkriminelle nutzen die Corona-Panik, 14.03.2020 (zuletzt abgerufen am 25.04.2020) (m.w.N.).

# Covid-19: Wegweiser für Informationsangebote

Die direkten und indirekten Auswirkungen der Corona-Pandemie lassen kaum einen Lebensbereich unberührt. Neben den vielen Einschränkungen und teils schweren Belastungen, die das Virus und Covid-19 selbst für Erkrankte, deren Familien und Kontaktpersonen mit sich bringt, können jedoch durchaus auch positive Entwicklungen vermerkt werden.

Die Digitalisierung in deutschen Schulen beispielsweise hätte wohl ohne den zwangsweisen Fernunterricht während der Ausgangsbeschränkungen nie einen derartigen Schub erfahren.[1] Dass die überwältigende Mehrheit der Schülerinnen und Schüler eine digitalere und modernere Unterrichtsform befürworten, war bereits vor der Pandemie klar.[2] 93% der Befragten fanden, dass digitale Medien den Unterricht interessanter machen und ganze 83% sahen in der Digitalisierung ihrer Schule und des Unterrichts eine Chance. Dass Politik und (Hoch-)Schulen nun im Zugzwang sind, lange versprochene und noch länger geforderte Maßnahmen umzusetzen, ist daher zu begrüßen. Klar ist aber auch: Ohne die nötige Infrastruktur geht es nicht. Während unsere dänischen Nachbarn schon seit Jahren digital vernetzt lernen und lehren, fehlt es in Deutschland schon an den Basics: stabiles, schnelles Internet, Geräte wie Laptops oder Tablets, die nötige Software für einen stabilen Unterricht und Online-Prüfungen.[3] Dabei besteht die Befürchtung, dass sich soziale Ungleichheiten weiter verstärken, etwa weil kein Geld für einen neuen Laptop da ist, die fehlende Betreuung und Hilfe durch Lehrkräfte von den Eltern mangels Zeit oder Bildung nicht kompensiert werden können oder die Internetverbindung im Heimatdorf keinen ruckelfreien Videochat zulässt.[4]

Auch in der Arbeitswelt setzt sich die Erkenntnis durch, wie viele Meetings oder Geschäftsreisen durch digitale Konferenzen ersetzt werden können und dass die Arbeit im Home-Office ganz und gar nicht unproduktiver ist als diejenige, die im Büro erledigt wird – dies wurde bereits in verschiedenen Studien festgestellt.[5] Natürlich gibt es verschiedene Probleme, die es noch zu adressieren gilt. Als Beispiele sind etwa negative Auswirkungen auf die Work-Life-Balance und psychische Belastungen[6] oder die Corona-bedingt chaotische Kinderbetreuung zu nennen.[7]

Eine der gravierendsten Schattenseiten des Ausnahmezustands ist sein Effekt auf die ohnehin fragile Pressefreiheit in Staaten, die generell eine unzensierte Berichterstattung unterbinden wollen. Laut Katja Gloger, Vorstandssprecherin der Organisation Reporter ohne Grenzen (ROG), bündle die Pandemie „bestehende repressive Tendenzen weltweit wie ein Brennglas".[8] Der Gedanke, der Gesundheitsschutz überwiege zahlreiche andere – und grundsätzlich nicht weniger wichtige – Belange, ist zwar aktuell richtig und wichtig: wenn auch die Bemühungen, Infizierte über Apps, Telekommunikationsdaten oder klassische „Ermittlungsarbeit" zu tracken und so die Infektionsrate möglichst gering zu halten, kritisiert werden, so besteht doch bei gesundem Menschenverstand insgesamt Verständnis für deren Notwendigkeit. Die Tatsache, dass derartige Kritik frei geäußert werden kann, trägt zu einem ausgewogenen Austausch und einer konstruktiven Debatte bei. Jedoch darf die Situation nicht als Rechtfertigung für dauerhafte einschneidende Maßnahmen missbraucht werden. Die Freiheits- und Persönlichkeitsrechte, die Bürgerinnen und Bürger etwa zugunsten der Nachverfolgbarkeit mehr oder weniger freiwillig preisgeben, dürfen nicht durch eine langfristige Durchsetzung staatlicher Überwachungsmaßnahmen und Beschränkungen „wegen der Pandemie" ausgehöhlt werden. Ein verlässlicher späterer „Rückbau" kritischer Maßnahmen ist daher eine unverzichtbare Voraussetzung für deren Implementierung.

Doch nicht nur der Mangel an Informationen infolge staatlicher Zensur ist ein Problem. Auch Fehlinformationen – Verharmlosung der Risiken, widersprüchliche Tipps zum Schutz vor Ansteckung, die Verbreitung nicht wirksamer „Behandlungen" mit Hausmitteln oder Globuli – wirken sich negativ aus. Beispielsweise führten die in Brasilien seitens der Regierung verbreiteten Fake News, das Virus sei harmlos, zu enormer Verunsicherung in der Bevölkerung und dazu, dass Drogengangs in den Favelas die Angelegenheit selbst in die Hand nahmen und ihrerseits Ausgangssperren verhängten.[9]

Auch wir möchten im uns möglichen Rahmen vertrauenswürdige Anlaufstellen und IT-Sicherheitstipps zur Verfügung stellen. Auf den folgenden Seiten finden Sie eine Auswahl zuverlässiger Informationen zur Pandemie und speziell zu arbeits- und IT-sicherheitsrechtlichen Aspekten. Bitte beachten Sie, dass aufgrund der rasanten Entwicklungen zum Zeitpunkt des Abrufs möglicherweise bereits aktualisierte Informationen der verlinkten Portale vorliegen können.

**1** Siehe z.B. die Initiative der Bundesregierung zum Thema Digitales Lernen in Zeiten der Corona-Pandemie – Schüler im Homeoffice (zuletzt abgerufen am 22.04.2020).

**2** *Banse*, Bitkom-Studie zum Digitalpakt: Schüler wollen mehr Digitalisierung, Deutschlandfunk.de vom 26.03.2020 (zuletzt abgerufen am 22.04.2020).

**3** Vgl. *Spiewak*, Um Klassen smarter, Zeit.de vom 06.11.2019 (zuletzt abgerufen am 20.04.2020).

**4** Vgl. *Frumkina*, Schule an digitalen Grenzen, Tagesschau.de vom 25.03.2020 (zuletzt abgerufen am 20.04.2020).

**5** Etwa die Studie der Universität Stanford, *Bloom et al.*, Does Working From Home Work? Evidence From A Chinese Experiment, The Quarterly Journal of Economics 2015, 165 oder die der Europäischen Union, *Eurofound and the International Labour Office*, Working Anytime, Anywhere: The Effects On The World Of Work, 2017.

**6** *Gebhardt*, Warnung vor dem Bore-out – Homeoffice kann psychische Probleme verursachen, SWR.de vom 05.04.2020 (zuletzt abgerufen am 20.04.2020).

**7** Vgl. *Schulze*, Zwischen Arbeiten und Kinderbetreuung, FAZ.de vom 18.04.2020 (zuletzt abgerufen am 22.04.2020).

**8** Reporter ohne Grenzen: Die Welt hat Chinas Zensur zu spüren bekommen, Heise Online vom 21.04.2020 (zuletzt abgerufen am 23.04.2020).

**9** *Gurk*, Wenn Gangs für die Gesundheit sorgen, SZ.de vom 02.04.2020 (zuletzt abgerufen am 23.04.2020).

## Anlaufstellen für Informationen auf Bundesebene

### Allgemeine Informationen

- Informationsseite der Bundesregierung
- Bundesministerium für Gesundheit: tagesaktuelle Informationen auf der offiziellen Seite sowie auf der speziell eingerichteten Website „Zusammen gegen Corona“
- Robert Koch Institut (zentrale Einrichtung der Bundesregierung auf dem Gebiet der Krankheitsüberwachung und -prävention)
- Bundesministerium des Inneren, für Bau und Heimat: Coronavirus: Fragen und Antworten
- Die Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration bietet Informationen in mehreren Sprachen
- Bundesministerium für Familie, Senioren, Frauen und Jugend: Allgemeine Informationen sowie Digitale Vereinbarkeit – Home-Office und mobiles Arbeiten – eine Toolbox für Unternehmen und Beschäftigte mit Familienaufgaben (vom 11.09.2017)
- Die Bundeszentrale für gesundheitliche Aufklärung (BZgA) hat eine spezielle Website eingerichtet: Infektionsschutz.de
- Corona-FAQ der Bundesagentur für Arbeit
- Institut für Arbeitsmarkt- und Berufsforschung (IAB) (Forschungseinrichtung der Bundesagentur für Arbeit): Folgen der Corona-Krise für den Arbeitsmarkt
  - IAB-Infoplattform: Homeoffice - Mobiles Arbeiten zu Hause
  - IAB-Forum: das Magazin des IAB: Homeoffice in Zeiten von Corona: In vielen Berufen gibt es bislang ungenutzte Potenziale (vom 25.03.2020)
- Bundesministerium für Justiz und Verbraucherschutz (BMJV)
- Informationen zur Digitalen Unterstützung in Zeiten von Corona auf der Website des Branchenverbandes Bitkom e.V.

### Informationen speziell zum Thema Arbeitsrecht

- Bundesregierung
  - Informationen für Arbeitnehmer
  - Interaktive Check-Liste zur IT-Sicherheit im Home-Office (YouTube): Virus fördert Viren, aufbereitet von „Der Hackathon der Bundesregierung“
  - Offizielle Website mit interaktivem Test, wie viele der erforderlichen Maßnahmen selbst bereits umgesetzt wurden und was man persönlich tun kann, um die IT-Sicherheit im Home-Office zu verbessern
- Der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit
  - Telearbeit und mobiles Arbeiten, ein Datenschutz-Wegweiser (PDF; Stand: Januar 2019)
  - Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie
  - Datenschutzrechtliche Informationen zur Corona-Krise
  - Datenschutz bei polizeilichen Maßnahmen (in der Corona-Pandemie)
  - Stellungnahme zum Entwurf eines Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite (PDF) (vom 23.03.2020)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Digital vernetzt in Corona-Zeiten
  - Home-Office? – Aber sicher!
  - IT-Grundschutz, Telearbeit
  - Aktueller Hinweis: Tipps für sicheres mobiles Arbeiten (vom 17.03.2020)
- Bundesministerium für Arbeit und Soziales (Arbeitsrechtliche Informationen)
  - Arbeits- und arbeitsschutzrechtliche Fragen zum Coronavirus
  - Übersicht mobiles und dezentrales Arbeiten (auch rechtliche Fragen, vom 01.01.2020)
- Aktuelle Informationen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA)
- Initiative Neue Qualität der Arbeit (INQA): Themendossier mit Schwerpunkt „Homeoffice“ (eine Initiative für Arbeitgeber und Beschäftigte)
- Hinweisseite des Bundesministeriums für Arbeit und Soziales
- FAQ der Vereinten Dienstleistungsgewerkschaft (verdi) für Beschäftigte

## Europa und International

- Informationsportal der Weltgesundheitsorganisation (WHO): Themenseite, Regionalbüro für Europa
- European Data Protection Board (edpb): Stellungnahme des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Covid-19-Pandemie (vom 19.03.2020) (Englisch)
- European Centre for Disease Prevention and Control (ecdc) (Englisch)
- DSK- Datenschutzkonferenz (Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder)
  - Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 03.04.2020:

Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie

- Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 13.03.2020, Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie

- ENISA, European Union Agency for Cybersecurity: Top Tips for Cybersecurity when Working Remotely (vom 15.03.2019) (Englisch)

## Bayern

- Bayerisches Landesamt für Gesundheit und Lebensmittelsicherheit
- Bayerisches Staatsministerium des Inneren, für Sport und Integration (Informationen zum Corona-Virus und zu landesspezifischen Maßnahmen in Bayern)
- Bayerisches Staatsministerium für Gesundheit und Pflege
- Die Verbraucherzentrale Bayern informiert über Folgen der Pandemie und die Rechte der Verbraucherinnen und Verbraucher
- Bayerisches Landesamt für Datenschutzaufsicht: Corona-Pandemie - Hinweise des BayLDA zu Datenschutz und Datensicherheit
- Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)
  - Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie
  - Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie
- Bußgeldkatalog „Corona-Pandemie“: Gemeinsame Bekanntmachung des Bayerischen Staatsministeriums des Innern, für Sport und Integration und des Bayerischen Staatsministeriums für Gesundheit und Pflege vom 02.04.2020, Az.: C2-2101-2-7 und GZ6a-G8000-2020/122-164
- Verordnung über eine vorläufige Ausgangsbeschränkung anlässlich der Corona-Pandemie (vom 24.03.2020)
- Verordnung zur Änderung der Bayerischen Infektionsschutzmaßnahmenverordnung (vom 31.03.2020)

## Andere Bundesländer

- Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg:
  - Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie (vom 13.03.2020)
  - Hinweise für Schulen und Lehrkräfte zur datenschutzgerechten Gestaltung des selbstständigen Lernens während der Corona-Pandemie (vom 23.03.2020)
  - Corona-Pandemie: Datenschutz und Heimarbeit (Hinweise vom 23 März 2020)
- Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Hinweise zur Corona-Pandemie und Datenschutz sowie Hinweise zur Erfassung von Kundendaten in der Gastronomie (vom 23.03.2020)
- Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: FAQ-Sammlung zum Thema Datenschutz in Zeiten von Covid-19 (vom 27.03.2020)
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
  - Sonderinformation zu Datenschutz in der Corona-Krise
  - Datenschutz: Plötzlich im Homeoffice – und nun?
- Sächsischer Datenschutzbeauftragter: Pandemie-Bekämpfung nicht ohne Datenschutz
- Landesbeauftragter für Datenschutz und Informationssicherheit Baden-Württemberg
  - Datenschutzfreundliche technische Möglichkeiten der Kommunikation (vom 27.03.2020)
  - Häufig gestellte Fragen („FAQs“) zum Thema Corona (vom 13.03.2020)
- Der Landesbeauftragte für den Datenschutz Niedersachsen
  - Informationen zum mobilen Arbeiten durch öffentliche Stellen, Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie

## Sonstiges

- LexCorona: Übersicht über die in Deutschland im Zusammenhang mit der sogenannten Corona-Krise erlassenen Rechtsakte (Gesetze, Rechtsverordnungen, Allgemeinverfügungen etc.) und Gerichtsentscheidungen u.A.
- FAQ der gesetzlichen Unfallversicherung VBG: Coronavirus (COVID-19) - Gesundheits- und Unfallversicherungsschutz – unter anderem auch im Home-Office

Stand: 30.04.2020

*Priska Katharina Büttel*

# Leiter des Forschungsprojekts und AutorInnen

## Prof. Dr. Dirk Heckmann

Dirk Heckmann (Jahrgang 1960) ist seit Oktober 2019 Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München, wo er sowohl der TUM School of Governance als auch der Fakultät für Informatik angehört. Zuvor hatte der in Freiburg i. Br. habilitierte Staatsrechtler von 1996 bis 2019 den Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau inne, wo er als Affiliate Professor nach wie vor die Forschungsstelle für IT-Recht und Netzpolitik (For..Net) und das Forschungsprojekt BayWiDI leitet.

Seine Lehr- und Forschungsschwerpunkte liegen im Schnittfeld von IT und Recht mit besonderem Fokus auf Datenschutzrecht, IT-Sicherheitsrecht, Legal Tech, E-Government, E-Health und Künstliche Intelligenz. Aus seiner Feder stammen der juris Praxiskommentar Internetrecht (6. Aufl. 2019) sowie weitere rund 200 Publikationen zu Recht und Digitalisierung.

2003 wurde Heckmann zum nebenamtlichen Verfassungsrichter am Bayerischen Verfassungsgerichtshof gewählt, 2007 in den Expertenkreis des Nationalen IT-Gipfels der Bundesregierung berufen. Seit 2014 ist er Vorsitzender der Deutschen Gesellschaft für Recht und Informatik, seit 2018 Direktor am Bayerischen Forschungsinstitut für Digitale Transformation bidt.

2015 wurde er in die Hauptjury des deutschen Computerspielpreises, 2016 in die Ethikkommission des Bundesverkehrsministeriums zum automatisierten und vernetzten Fahren und 2018 in die Datenethikkommission der Bundesregierung berufen.

## Lukas Schmidt

Lukas Schmidt ist seit Juli 2018 Wissenschaflicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau sowie seit Dezember 2018 Kollegiat des DFG-Graduiertenkollegs 1681/2 „Privatheit und Digitalisierung“. Das Studium der Rechtswissenschaften hat er 2016 mit der Ersten Juristischen Staatsprüfung in Passau abgeschlossen. Das Referendariat am OLG München hat er 2018 mit der Zweiten Juristischen Staatsprüfung abgeschlossen.

## Luisa Lorenz

Luisa Lorenz studiert Rechtswissenschaften an der Universität Passau im Studienschwerpunkt Informations- und Kommunikationsrecht und ist als Studentische Hilfskraft seit Juni 2017 für die Forschungsstelle für IT-Recht und Netzpolitik (For..Net) unter der Leitung von Prof. Dr. Dirk Heckmann tätig.

## Felix Sobala

Felix Sobala forschte von 2016 bis 2019 als Wissenschaftlicher Mitarbeiter am DFG-Graduiertenkolleg 1681/2 „Privatheit und Digitalisierung“ der Universität Passau im Fachbereich Rechtswissenschaften zu datenschutz- und privatheitsrechtlichen Themen. Seit 2019 ist er Wissenschaftlicher Mitarbeiter am Bayerischen Wissensnetzwerk Digitale Infrastrukturen, IT-Sicherheit und Recht für Unternehmen (BayWiDI) und promoviert zu Regulierungsansätzen des datenschutzrechtlichen Verarbeitungsgrundsatzes der Datensparsamkeit.

## Priska Katharina Büttel

Priska Katharina Büttel betreut seit Oktober 2019 als geschäftsführende Wissenschaftliche Mitarbeiterin der Forschungsstelle For..Net unter anderem das Projekt BayWiDI an der Universität Passau. Sie beschäftigt sich gegenwärtig im Rahmen ihrer Promotion mit Rechtsfragen im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz und Robotik zu medizinischen Zwecken.

# Impressum

*Sämtliche Abbildungen sind gemeinfrei-ähnlich freigegeben via Unsplash.com*


**Impressum**

Universität Passau
Innstraße 41
94032 Passau

Telefon: 0851/509-0
Telefax: 0851/509-1005

E-Mail: praesident@uni-passau.de
Internet: www.uni-passau.de

USt.-Id-Nr.: DE 811193057

**Organisation**

Gemäß Art. 11 Abs. 1 BayHSchG ist die Universität Passau als Hochschule des Freistaates Bayern eine Körperschaft des öffentlichen Rechts und zugleich staatliche Einrichtung. Aufsichtsbehörde ist das Bayerische Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in München (Anschrift: Salvatorstraße 2, 80333 München).

**Vertretung**

Die Universität Passau wird vom Vorsitzenden des Leitungsgremiums, Präsident Prof. Dr. Ulrich Bartosch, gesetzlich vertreten. Verantwortlicher im Sinne des § 5 TMG (Telemediengesetz) ist der Präsident. Für namentlich oder mit einem gesonderten Impressum gekennzeichnete Beiträge liegt die Verantwortung bei den jeweiligen Autorinnen und Autoren.

**Herausgeber**

Prof. Dr. Dirk Heckmann
Leiter der Forschungsstelle für IT-Recht und Netzpolitik (For..Net)

**Redaktion und Produktion**

Priska Katharina Büttel, Dipl.-Jur.
Lukas Schmidt, Ass. jur.
Felix Sobala, Jurist (Univ.)

**Layout und Satz**

Moritz Rowold
Studentische Hilfskraft


Das nächste Magazin erscheint Mitte September 2020. Sie finden das Magazin und die Möglichkeit, sich für den kostenlosen Versand an- und abzumelden, unter www.baywidi.de.

Hinweise, Anregungen, Lob und Kritik sind herzlich willkommen. Schreiben Sie uns einfach unter baywidi@uni-passau.de.