DATENSCHUTZMANAGEMENT IN KRISENZEITEN

LASSEN SIE DEN DATENSCHUTZ NICHT OPFER VON BETRIEBLICHEN ENTSCHEIDUNGEN WERDEN!

Praxisbezogene Tipps und Best-Practice-Anleitungen, mit denen Sie jederzeit pragmatisch und lösungsorientiert handeln können. So können Sie den Datenschutz auch in einer Krise wahren und nach einer Krise weiter voranbringen.

Rechtssicher und praxisgeprüft: Checklisten und Muster inklusive – auch als praktischen Download zur Weitergabe an Ihre Mitarbeiter

DAT-EMF-DMKrise-20-23

PRIVACYXPERTS

Inhalt

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn

Handelsregister: HRB 8165
Registergericht: Amtsgericht Bonn
vertreten durch den Vorstand: Richard Rentrop

Umsatzsteuer-Identifikationsnummer
gemäß §27a Umsatzsteuergesetz: DE 812639372

ISBN: 978-3-8125-2856-6

Kontakt
Telefon: 0228 - 9 55 01 50 (Kundendienst)
Telefax: 0228 - 3 69 64 80
E-Mail: kundendienst@privacyxperts.de
Internet: https://www.privacyxperts.de
V.i.S.d.P.: Michael Jodda,
Theodor-Heuss-Str. 2-4; D-53177 Bonn
Autor: Andreas Hessel, Losheim am See
Gutachter: Dustin Fürst, Hannover
Produktmanagement: Sara Münnich, Bonn

Bildnachweis:
Titel: Adobe Stock | Photocreo Bednarek

Redaktionelles Management: Nicole Brockmann, Madrid
Satz: Deinzer Grafik, Gartow
Druck: XXX **Bitte Text**

Datenschutz in Zeiten von COVID-19

Liebe Leserin, lieber Leser,

der Ausbruch von COVID-19 und die Pandemie haben dazu geführt, dass das gesamte öffentliche Leben in einer nie da gewesenen Form verändert wurde. Im Vordergrund stehen seit Beginn der Krise Maßnahmen zur Erhaltung der Gesundheit und Sicherheit der Bevölkerung. Aber auch das berufliche und private Leben hat sich verändert. Eine Vielzahl von Mitarbeitern arbeitet seit Wochen im Homeoffice oder mobil. Zudem werden verstärkt Technologien wie Cloud-Speicher, Videokonferenzen oder Kollaborationsplattformen wie Microsoft Teams, Zoom oder Slack im Unternehmen eingesetzt. Für Sie als Datenschutzbeauftragten ergibt sich in diesen Krisenzeiten eine Vielzahl von neuen Herausforderungen, die Sie meistern müssen.

In Betrieben müssen umfangreiche Maßnahmen zum Schutz der Belegschaft und der Besucher vor einer Infektion getroffen werden. Hierbei werden unter Umständen auch besonders schützenswerte Gesundheitsdaten erhoben. Denn es besteht z. B. die Verpflichtung, erkrankte Mitarbeiter zu erfassen und an die Gesundheitsbehörden zu melden. Aber auch die Erfassung von Kontaktpersonen und vieles mehr gehören nicht zu den normalen Verarbeitungstätigkeiten eines Unternehmens. Hier gilt es, diese personenbezogenen Daten vor Missbrauch zu schützen und die Datenverarbeitung nach den geltenden Vorgaben der Datenschutz-Grundverordnung zu regeln und durchzuführen.

Die Arbeit im Homeoffice birgt eine Vielzahl von Datenschutz- und Sicherheitsrisiken, denen sich Unternehmen stellen müssen. Oftmals mussten die Mitarbeiter in sehr kurzer Zeit ihren Arbeitsplatz verlassen und ins Homeoffice wechseln. Da ist es kein Wunder, wenn die technischen und organisatorischen Sicherheitsmaßnahmen zum Teil noch unvollständig oder unzureichend waren oder noch heute auf diesem Stand sind. Gleiches gilt für den Einsatz neuer Technologien. Schließlich wurden die Unternehmen und auch Sie als Datenschutzbeauftragter völlig unvorbereitet vor diese Situation gestellt. Die gängigen Notfallpläne waren für eine solche Pandemie zumeist ungeeignet. Daher mussten die Notfallstäbe oftmals schnelle und pragmatische Entscheidungen fällen. In solchen Krisensituationen kann es allzu leicht passieren, dass die Datensicherheit und der Datenschutz auf der Strecke bleiben.

Sie als Datenschutzbeauftragter wissen, dass der Datenschutz auch in Krisenzeiten gewahrt werden muss. Sie müssen auch in der Krise in Ihrem Unternehmen darauf hinwirken, dass sowohl die technischen als auch organisatorischen Maßnahmen angemessen umgesetzt werden. Dies gilt für die Arbeitsplätze und Verfahren im Unternehmen genauso wie für die im Homeoffice. Das können Sie aber nur erreichen, wenn Sie mit den Stakeholdern zusammenarbeiten und an deren Entscheidungen teilhaben. Als Datenschutzbeauftragter müssen Sie wissen, wie Sie mit diesen Stakeholdern umgehen, damit Sie Ihre Ziele erreichen können.

Sie sollten auch in den Notfallstäben aktiv mitarbeiten, um den Datenschutz voranbringen zu können. Andernfalls besteht die Gefahr, dass der Datenschutz den betrieblichen und geschäftlichen Entscheidungen zum Opfer fällt.

Sie als Datenschutzbeauftragter sind gerade in der Krise gefordert. Sie müssen aber nicht nur darauf hinwirken, dass alle datenschutzrechtlichen Anforderungen beachtet und die erforderlichen technischen und organisatorischen Maßnahmen umgesetzt werden. Sie müssen sich auch mit den Stakeholdern im Unternehmen auseinandersetzen. Nicht zu vergessen müssen die Mitarbeiter im Homeoffice geschult werden. Das fordert nicht nur Ihr Fachwissen. Um in dieser Krise erfolgreich zu sein, benötigen Sie auch Motivationsstärke, Empathie und Überzeugungskraft.

Lesen Sie hier, wie Sie sich als Datenschutzbeauftragter gegenüber den Stakeholdern im Notfallstab behaupten können, welche Maßnahmen Sie zur Absicherung von Homeoffice-Arbeitsplätzen ganz konkret fordern müssen und wie Sie Ihre Mitarbeiter schulen können.

Mit diesen praxisbezogenen Tipps und Best-Practice-Anleitungen können Sie den Datenschutz in der Krise nicht nur wahren, sondern voranbringen. Lesen Sie, wie Sie als Datenschutzbeauftragter pragmatisch und risikoorientiert in der Krise vorgehen und damit auch Ihre Position im Unternehmen nachhaltig stärken. Denn „Macher" sind die Gewinner jeder Krise. Das gilt auch für den Datenschutz.

Andreas Hessel

Andreas Hessel ist als Chief Information Security Officer langjähriger Leiter des Bereichs Informationssicherheit und Risikomanagement einer Landesbank. Darüber hinaus arbeitet er als externer Datenschutzbeauftragter und Berater im Bereich Cybersecurity.

Krisenmanagement. Wie arbeiten Sie mit den Stakeholdern zusammen?

In einer Krise kann das Unternehmen kritische Geschäftsprozesse nicht in dem erforderlichen Umfang durchführen – vielleicht fallen sie sogar ganz aus. Bei einer Pandemie kann es erhebliche Personalausfälle und Einschränkungen des öffentlichen Lebens geben.

Unternehmen bilden deshalb Notfallstäbe. Ihre Aufgabe ist, Maßnahmen zu ergreifen, die geeignet sind, kritische Geschäftsprozesse fortzuführen, die Gesundheit der Mitarbeiter zu schützen und hohe Schäden vom Unternehmen abzuwenden. Solche Notfallstäbe haben weitreichende Entscheidungsbefugnisse, die außerhalb der normalen Hierarchieebenen stehen. In der Regel sind in den Notfallstäben Mitglieder des Managements und Fachexperten vertreten. Hierzu zählen insbesondere Vertreter aus dem Gebäudemanagement, Personal und IT und weitere Manager, die für den Betriebsablauf von entscheidender Bedeutung sind.

In Krisen müssen kurzfristige organisatorische, aber auch technische Änderungen umgesetzt werden, die regelmäßig Einfluss auf das Sicherheits- und Datenschutzniveau des Unternehmens haben.

Beispiele: Einrichtung von Homeoffice-Arbeitsplätzen sowie die Erhebung von Infektionsketten und Gesundheitsdaten.

Die Vertreter in den Notfallstäben müssen kurzfristige Entscheidungen treffen. Da diese weitreichende Folgen auf das gesamte Unternehmen haben können, ist es wichtig, dass Fachexperten die Entscheider beraten. Zu diesen Experten gehören auch Sie als Datenschutzbeauftragter, denn nur Sie können tatsächlich prüfen, welche datenschutzrechtlichen Risiken die Notfallmaßnahmen mit sich bringen.

Datenschutz gilt auch in Krisenzeiten. Daher müssen Sie als Datenschutzbeauftragter darauf hinwirken, dass Sie zumindest beratendes, aber definitiv ständiges Mitglied im Notfallstab sind. Auf diese Rolle sollten Sie sich gut vorbereiten. Im Notfallstab müssen Sie bereit sein, kurzfristige und pragmatische Entscheidungen zu treffen bzw. Entscheidungen des Notfallstabs sehr kurzfristig zu prüfen.

Oftmals fehlt in solchen Situationen die Zeit für umfangreiche Prüfungen, Dokumentationen oder Gutachten. Hier gilt es, die Stakeholder zu unterstützen, aber auch eventuelle Risiken transparent zu machen. Sie müssen in der Krise als Datenschutzbeauftragter oft Entscheidungen alleine auf Basis Ihrer Erfahrungen treffen. Das erfordert nicht nur Mut zum Risiko, sondern auch Standhaftigkeit, wenn Ihre Entscheidungen eben nicht so ausfallen, wie die Stakeholder es vielleicht erwartet hätten. In solchen Situationen gilt es, konstruktiv und vor allem zielorientiert vorzugehen.

Aber wie gehen Sie konkret mit Stakeholdern um, damit Sie Ihrer Aufgabe als Datenschutzbeauftragter auch in Krisenzeiten gerecht werden und gleichzeitig wichtige Entscheidungen der Stakeholder nicht torpedieren? Beachten Sie die folgenden vier Schritte und Sie werden Ihre Ziele erreichen.

4 Schritte zum Erfolg: So überzeugen Sie die Stakeholder

Schritt 1: Sie müssen in Erfahrung bringen, wer Ihre Stakeholder sind, welche Rolle sie im Unternehmen und welche Rolle sie im Notfallstab haben. Diese können durchaus unterschiedlich sein. So können Sie bei bestimmten Themen ganz konkret die Themenverantwortlichen ansprechen. Das führt in der Regel dazu, dass Sie Kompetenzschwierigkeiten direkt umgehen und den Respekt des Stakeholders erlangen. Denn Sie wissen, wen Sie ansprechen müssen!

Schritt 2: Analysieren Sie, welche individuellen Standpunkte und Ziele die Stakeholder verfolgen. Wie stehen sie zum Thema Datenschutz? Was erwarten sie von jedem einzelnen? Oder was sind ihre Befürchtungen? Dann können Sie sich auf Konfliktgespräche besser vorbereiten. Sie können aber auch Allianzen schmieden und bei schwierigen Themen die Stakeholder ansprechen, die vielleicht grundsätzlich dem Datenschutz zugeneigt sind.

Schritt 3: Erstellen Sie einen Plan, wie Sie konkret mit den jeweiligen Stakeholdern umgehen wollen: persönliche Ansprache, Notizen, Flipcharts, Präsentationen usw. Jeder hat seine Vorlieben. Nur wenn Sie für jeden Einzelnen den richtigen Kommunikationskanal finden, werden Sie auch überzeugen.

Schritt 4: Planen Sie, wie Sie ganz konkret im Notfallstab auftreten möchten und wie Sie Ihre Themen platzieren wollen. Schlagen Sie z. B. vor, dass es im Notfallstab immer einen Zeitslot für Datenschutz gibt oder dass Datenschutz immer ein fester Punkt der Agenda ist. Bereiten Sie dann Ihre Themen entsprechend vor und denken Sie daran, dass am Ende immer eine Lösung stehen muss.

Diese 4 Mittel helfen Ihnen, um zu überzeugen

1. Verständnis
Versuchen Sie, den Stakeholder zu verstehen! Hierbei ist es wichtig, nicht nur die Position, sondern den Menschen hinter der Position zu kennen. Frage Sie sich: Was treibt diese Person an? Welchen Zwängen ist sie unterworfen? Welche Emotionen hat sie, wenn es um Datenschutz (oder dessen Auswirkungen) geht? Welche Bedenken haben Sie? Was wollen Sie erreichen und warum?

2. Beziehung
Nun geht es darum, eine Beziehung zu den Stakeholdern aufzubauen. Je mehr Vertrauen besteht, desto offener wird der Umgang mit dem Stakeholder. Dadurch können viele Probleme schon frühzeitig angesprochen und aus der Welt geschafft werden. Suchen Sie das persönliche Gespräch auch außerhalb des Notfallstabs und zu anderen Themen. Vielleicht lassen Sie auch

private Themen in das Gespräch einfließen. Erzählen Sie z. B. von Ihren ganz persönlichen Erfahrungen in der Krise oder erkundigen Sie sich nach dem Empfinden Ihres Gegenübers. Empathie ist eine sehr gute Möglichkeit, Beziehungen aufzubauen.

3. Kommunikation
Finden Sie für jeden Stakeholder die richtige Art der Kommunikation und nehmen Sie sich Zeit dafür (siehe Schritt 3). Achten Sie darauf, dass eine gelungene Kommunikation aus einem guten Zusammenspiel zwischen Sender und Empfänger besteht. Der Sender verpackt seine Botschaft und der Empfänger entschlüsselt sie – das kann leicht zu Missverständnissen führen!

4. Konsultation
Sie sollten die Stakeholder regelmäßig über den aktuellen Stand der Datenschutzmaßnahmen informieren und sie involvieren. Je früher und häufiger Sie sich mit den Stakeholdern beraten, desto besser. Denn so bauen Sie nicht nur Widerstände ab und eine gute Beziehung auf, sondern so profitieren beide Seiten von dem Fachwissen des anderen.

Fazit
Als Datenschutzbeauftragter müssen Sie sich auf die Arbeit im Notfallstab vorbereiten. Dies gilt insbesondere für die Kommunikation. Sie sollten im Notfallstab als kompetenter Macher auftreten: immer entscheidungsfreudig, risikoorientiert mit sachgerechten pragmatischen Lösungen. Sie haben im Notfallstab die Möglichkeit, den Datenschutz nicht nur in der Krise zu wahren, sondern auch Ihre Position im Unternehmen zu verbessern. Denn ein guter Krisenmanager hat immer die Aufmerksamkeit aller Stakeholder und dies auch nach der Krise.

Datenverarbeitung. Was müssen Sie dabei beachten?

Alle Datenschutzanforderungen sind selbstverständlich auch in der Krise im Unternehmen umzusetzen. Als Datenschutzbeauftragter stehen Sie hierbei vor zwei wesentlichen Herausforderungen: Zum einen werden kurzfristig Verfahren geändert bzw. neue technische Verfahren eingeführt und zum anderen werden auch neue sensible personenbezogene Daten im Unternehmen erhoben. Hier gilt es zunächst zu prüfen, welche dieser Daten das Unternehmen überhaupt erheben darf.

Der einzelne Betroffene bleibt natürlich „Herr seiner Daten", gerade auch seiner besonders sensiblen Gesundheitsdaten. Dabei kann aber eine arbeitsvertragliche Pflicht bestehen, durch Angaben über Aufenthaltsorte oder Kontaktpersonen dem Arbeitgeber eine Einschätzung zu ermöglichen, ob Gesundheitsrisiken für den Betroffenen oder andere Beschäftigte bestehen.

Bei den Daten, die das Unternehmen während der Pandemie verarbeiten darf, kann es sich insbesondere um folgende Informationen handeln:
- Informationen über Personen, bei denen eine Infektion festgestellt wurde oder die Kontakt mit einer nachweislich infizierten Person hatten
- Informationen über Personen, die sich im relevanten Zeitraum in einem vom Robert-Koch-Institut (RKI) als Risikogebiet eingestuften Gebiet aufgehalten haben

Erlaubt sind die Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern, insbesondere um festzustellen, ob diese
- selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen,
- sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben.

Die Offenlegung personenbezogener Daten von nachweislich infizierten oder unter Infektionsverdacht stehenden Personen zur Information von Kontaktpersonen ist dagegen nur rechtmäßig, wenn die Kenntnis der Identität für die Vorsorgemaßnahmen der Kontaktpersonen ausnahmsweise erforderlich ist.

FAQ

Dürfen Arbeitgeber aktuell private Handynummern oder andere Kontaktdaten von der Belegschaft erheben, um die Beschäftigten im Falle einer Schließung des Betriebs oder in ähnlichen Fällen kurzfristig warnen oder auffordern zu können, zu Hause zu bleiben?

Zur Corona-Prävention wird von vielen (Berufs-)Verbänden der Aufbau eines auf den jeweiligen Betrieb zugeschnittenen innerbetrieblichen Kommunikationsnetzwerks empfohlen, damit Unternehmen je nach Pandemiephase bestimmte Maßnahmen treffen können. Eine solche Empfehlung spricht ebenfalls das Handbuch des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe aus.

Damit die Beschäftigten auch kurzfristig gewarnt werden können und gar nicht erst im Betrieb oder bei der Arbeit erscheinen, dürfen Arbeitgeber von ihren Beschäftigten auch die aktuelle private Handynummer etc. abfragen und temporär speichern. Dies kann allerdings nur im Einverständnis mit dem Beschäftigten erfolgen; eine Pflicht zur Offenlegung privater Kontaktdaten besteht für die Beschäftigten nicht, wird jedoch regelmäßig in ihrem eigenen Interesse liegen.

Mein Tipp
Als Datenschutzbeauftragter müssen Sie darauf hinwirken, dass alle Daten, die Ihr Unternehmen zur Bewältigung der Pandemie erhoben hat (Gesundheitsdaten, private Telefonnummern usw.), nach der Krise gelöscht werden.

Dürfen Arbeitgeber Informationen darüber erheben und weiterverarbeiten, ob ein Beschäftigter in einem Risikogebiet war oder mit einem Erkrankten direkten Kontakt hatte etc.?

Arbeitgeber sind aufgrund ihrer Fürsorgepflicht und nach dem Arbeitsschutzgesetz verpflichtet, die erforderlichen Maßnahmen zu treffen, um die betriebliche Sicherheit und Gesundheit der Belegschaft zu gewährleisten. Für diesen Zweck ist es datenschutzrechtlich zulässig, Informationen darüber zu erheben, zu welchen Personen der erkrankte Mitarbeiter Kontakt hatte. Gemäß Art. 6 Abs. 1 Buchstabe c Datenschutz-Grundverordnung (DSGVO) in Verbindung mit Art. 9 Abs. 1, Abs. 4 DSGVO und § 26 Abs. 3 Satz 1, § 22 Abs. 1 Nr. 1 Buchstabe b Bundesdatenschutzgesetz kann der Arbeitgeber die erforderlichen Daten zum Zweck der arbeitsmedizinischen Vorsorge verarbeiten.

Der Arbeitgeber darf demnach beispielsweise auch Urlaubsrückkehrer befragen, ob sie sich in einem etwa durch das RKI festgelegten Risikogebiet aufgehalten haben.

Dürfen Arbeitgeber den Beschäftigten mitteilen, dass ein bestimmter Mitarbeiter am Virus erkrankt ist und sogar den Namen nennen, um darauf aufbauend mögliche Kontaktpersonen freizustellen?

Der Name des betroffenen Mitarbeiters sollte grundsätzlich nicht genannt werden. Gleichzeitig sind Mitarbeiter, die in direktem Kontakt mit einem Infizierten standen, zu warnen. Der Arbeitgeber stellt sie in der Regel von der Arbeit frei, um eine Ansteckungsgefahr zu vermeiden. Regelmäßig kann eine derartige Maßnahme abteilungs- bzw. teambezogen ohne konkrete Namensnennung erfolgen. Stellen Gesundheitsämter Anfragen, ist von einer Übermittlungspflicht auszugehen.

Fazit
Als Datenschutzbeauftragter müssen Sie darauf hinwirken, dass Ihr Arbeitgeber auch während der Pandemie die Zweckbindung und das Minimalprinzip wahrt. Sprechen Sie mit der Personalabteilung und wirken Sie darauf hin, dass sie diese Prinzipien umsetzt. Ebenso müssen Löschfristen festgelegt werden. Vergessen Sie nicht, dass Gesundheitsdaten in verschlüsselter Form gespeichert werden sollten und dass auch nur berechtigte Personen darauf zugreifen dürfen. Sprechen Sie hierzu mit Ihrer IT-Abteilung. Sorgen Sie dafür, dass insbesondere die Gesundheitsdaten an einer zentralen Stelle gespeichert werden. Nur so kann sichergestellt werden, dass diese Daten nach der Krise auch gelöscht werden.

Auftragsverarbeitung. Was müssen Sie mit den Dienstleistern klären?

Hat Ihr Arbeitgeber Mitarbeiter zur Arbeit im Homeoffice verpflichtet, müssen Sie als Datenschutzbeauftragter prüfen, ob in Verträgen zur Auftragsverarbeitung Regelungen zum Homeoffice bestehen. Regelmäßig besteht zumindest eine Melde- wenn nicht gar ausdrückliche Genehmigungspflicht gegenüber dem Auftraggeber. Eventuell werden sogar konkrete technische und organisatorische Sicherheitsmaßnahmen für die Datenverarbeitung im Homeoffice gefordert. Dies gilt sowohl für Verträge mit Ihren Auftragsverarbeitern als auch für Verarbeitungen, die Sie im Auftrag durchführen. Auch die Datenschutzaufsichtsbehörden fordern ausdrückliche Regelungen für Homeoffice-Arbeitsplätze bei der Auftragsverarbeitung.

Fazit
Prüfen Sie die bestehenden Verträge und setzen Sie sich mit den Dienstleistern in Verbindung. Falls Ihre Verträge keine Regelungen zum Homeoffice vorsehen, sollten Sie zumindest schriftliche Vereinbarungen mit konkreten Vorgaben zur Arbeit im Homeoffice mit den Dienstleistern treffen.

Homeoffice. Welche Sicherheitsmaßnahmen sind zu beachten?

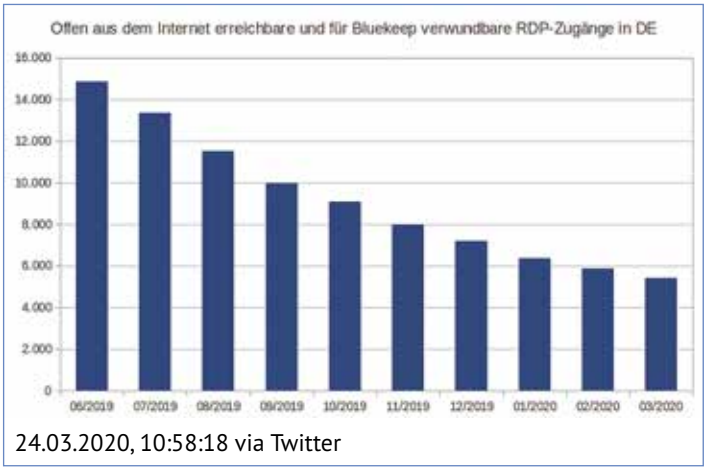
Während einer Pandemie ist es erforderlich, Kontakte unter Mitarbeitern möglichst zu verhindern. Aus diesem Grund arbeiten viele Mitarbeiter im Homeoffice. Was zunächst nur als technische und organisatorische Herausforderung wahrgenommen wird, birgt jedoch sehr hohe Risiken. Insbesondere sind die Risiken der Datensicherheit zu beachten.

Daneben gibt es auch vertragliche und organisatorische Herausforderungen, die zu meistern sind. Unter Risikogesichtspunkten müssen Sie als Datenschutzbeauftragter prüfen, ob die Anforderungen an die Räumlichkeiten, die Sicherheit der IT-Systeme und die Schulung der Mitarbeiter erfüllt sind. Denn nicht jede Ecke in einem Zimmer ist ein Arbeitsplatz. Inwieweit die konkreten Anforderungen erfüllt sind, können Sie mit den nachfolgenden Checklisten prüfen.

CHECKLISTE: Sicherheitsanforderungen Homeoffice

	Erfüllt?
Räumlichkeiten	☐ Ja ☐ Nein
Abschließbarer Raum vorhanden?	☐ Ja ☐ Nein
Abschließbarer Schrank/Schubladen vorhanden?	☐ Ja ☐ Nein
Arbeitsschutzvorgaben erfüllt?	☐ Ja ☐ Nein
IT-System (Notebook, Rechner)	
Lokale Drucker gesperrt?	☐ Ja ☐ Nein
Regelmäßige Aktualisierung des Virenscanners, Betriebssystems, Software sichergestellt (zentrale Verwaltung, Richtlinien usw.)?	☐ Ja ☐ Nein
Firewall aktiviert?	☐ Ja ☐ Nein
Verschlüsselung der Festplatte durchgeführt?	☐ Ja ☐ Nein
USB-Schnittstellen gesperrt?	☐ Ja ☐ Nein
Automatische Sperrung des Bildschirmes und Passwortabfrage nach 5 Minuten Inaktivität aktiviert?	☐ Ja ☐ Nein
Verbindung in das Firmennetzwerk	
VPN-Verbindung (Virtual Private Network) mit Zwei-Faktor-Authentifizierung (2FA, Passwort und Token) mit sicherem Passwort eingerichtet?	☐ Ja ☐ Nein
Verbindung zum Internet ausschließlich über VPN-Verbindung möglich?	☐ Ja ☐ Nein
Drahtloses Heimnetzwerk (DSL-Router) mit sicherem WPA2-Schlüssel gesichert?	☐ Ja ☐ Nein
Administrationszugang zum DSL-Router im Heimnetzwerk mit sicherem Passwort (mindestens zwölf Zeichen) gesichert?	☐ Ja ☐ Nein
Kommunikation	
Keine Kommunikation über private E-Mail-Accounts oder private Cloudspeicher?	☐ Ja ☐ Nein

Insbesondere Sicherheitslücken auf RDP-Servern führen aktuell immer wieder zu schweren Datenschutzpannen. Eine aktuelle Auswertung des CERT-Bundes zeigt, dass trotz mehrmaliger Warnungen des Bundesamts für Sicherheit in der Informationstechnik noch immer rund 5.000 Server mit einer schwerwiegenden Sicherheitslücke betrieben werden.



24.03.2020, 10:58:18 via Twitter

Fazit

Die Sicherheit eines Homeoffice-Arbeitsplatzes ist eine zentrale Anforderung in der Krisensituation. Als Datenschutzbeauftragter müssen Sie sich mit der IT-Abteilung in Verbindung setzen und darauf hinwirken, dass die erforderlichen Sicherheitsmaßnahmen tatsächlich umgesetzt werden.

CHECKLISTE: Sicherheit von RDP-Verbindungen

Anforderung	Erfüllt?
Ist der RDP-Zugang direkt erreichbar oder wird dieser über ein RDP-Gateway zur Verfügung gestellt, das nach außen nur das HTTPS-Protokoll nutzt?	☐ Ja ☐ Nein
Wird im Zusammenhang mit RDP eine 2FA/MFA verwendet?	☐ Ja ☐ Nein
Wird im Zusammenhang mit RDP eine Endpoint-Protection-Lösung eingesetzt?	☐ Ja ☐ Nein
Ist die Reichweite des RDP-TCP-Ports eingeschränkt (nur bestimmte IP-Adressen können sich verbinden)?	☐ Ja ☐ Nein
Werden administrative Anmeldungen per RDP unterbunden?	☐ Ja ☐ Nein
Ist ein eigener RDP-Port für Administratoren eingerichtet und ist der auf spezielle IP-Adressen beschränkt?	☐ Ja ☐ Nein
Wird IPSec genutzt?	☐ Ja ☐ Nein
Werden speziell gehärtete RDP-Gateway Server genutzt?	☐ Ja ☐ Nein
Werden die RDP-Systeme regelmäßig mit Sicherheitspatches versorgt?	☐ Ja ☐ Nein

Sicher ist der RDP-Zugang dann, wenn alle Anforderungen umgesetzt werden. Insbesondere das Aufspielen von Sicherheitspatches muss garantiert sein.

Videokonferenzen. Was können Sie empfehlen, was müssen Sie prüfen?

In der COVID-19-Krise haben Videokonferenzen in der Unternehmenskommunikation enorm an Bedeutung gewonnen. Nicht nur für die interne Kommunikation zwischen Beschäftigten im Unternehmen und den Kollegen im Homeoffice, sondern auch für die Kommunikation mit Kunden, Bewerbern und Geschäftspartnern spielen Videokonferenzsysteme eine wichtige Rolle. Da die Systeme in der Regel browserbasiert genutzt werden können und keinerlei Installationen auf den Notebooks erforderlich sind, kann jeder Mitarbeiter beliebige Produkte anwenden und auch mit beliebigen Partnern kommunizieren. Da bei solchen Systemen zum einen personenbezogene Daten und zum anderen auch Unternehmensdaten verarbeitet werden, müssen Sie als Datenschutzbeauftragter den sicheren und ordnungsgemäßen Einsatz dieser Videosysteme prüfen.

Als Datenschutzbeauftragter sollten Sie zunächst die Bedrohungen kennen, die beim Einsatz von Videokonferenzsystemen zu beachten sind. Die nachfolgende Checkliste zeigt die Risiken und die erforderlichen Gegenmaßnahmen.

CHECKLISTE: Bedrohungen und Sicherheitsmaßnahmen beim Einsatz von Videokonferenzsystemen

Bedrohung	Sicherheitsmaßnahme	Beachtet?
Unzureichend abgesicherte Cloud-Dienste	Auswahl Dienstleister	☐ Ja ☐ Nein
Fehlerhafte Bedienung und Nutzung	Schulung der Mitarbeiter	☐ Ja ☐ Nein
Automatische Annahme von eingehenden Verbindungsanfragen	Auswahl Tool und sachgerechte Administration	☐ Ja ☐ Nein
Gezieltes Ausspähen von Räumen	Auswahl Tool und sachgerechte Administration	☐ Ja ☐ Nein
Verlust der Vertraulichkeit durch Kompromittierung von Videoendpunkten.	Endgerätesicherheit	☐ Ja ☐ Nein
Leistungsüberwachung und Profiling	datenschutzkonforme Einstellungen, ggf. Betriebsvereinbarung	☐ Ja ☐ Nein
Kein ordnungsgemäßer Benutzerwechsel für Videoendpunkte	Auswahl Tool und sachgerechte Administration	☐ Ja ☐ Nein
Versehentliche Preisgabe von Informationen	Auswahl Tool, Schulung der Mitarbeiter	**☐ Ja ☐ Nein**
Unzureichende Prüfung der Identität von Kommunikationspartnern	Auswahl Tool und sachgerechte Administration	**☐ Ja ☐ Nein**
Konfigurationsfehler bei Videokonferenzlösungen	sachgerechte Administration	**☐ Ja ☐ Nein**
Missbrauch von Administrations- und Wartungszugängen	Auswahl Tool und sachgerechte Administration	**☐ Ja ☐ Nein**
Unzureichende Organisation des Betriebs eines Videokonferenzsystems	sachgerechte Administration	☐ Ja ☐ Nein
Unzureichendes Identitäts- und Berechtigungskonzept	Freigabeverfahren und sachgerechte Administration	**☐ Ja ☐ Nein**
Unzureichend abgesicherte Aufzeichnung, Protokollierung und Dateiablage	sachgerechte Administration	☐ Ja ☐ Nein
Unzureichende Kenntnis von Technik und Regelungen	sachgerechte Administration, Schulung Mitarbeiter	☐ Ja ☐ Nein

Hier drohen tatsächlich erhebliche Datenschutzverstöße weil die Aufsichtsbehörden das Thema Videokonferenzen derzeit im Fokus haben. Als Datenschutzbeauftragter sollten Sie diese Checkliste gemeinsam mit Ihrer IT-Abteilung durchgehen und darauf hinwirken, dass sie alle Maßnahmen sachgerecht umsetzt.

Hinweis: Die Datenschutzaufsichtsbehörden vertreten in der datenschutzrechtlichen Bewertung von Videokonferenzsystemen einmal mehr keine einheitliche Meinung. Die Verlautbarungen reichen von „sollten nicht eingesetzt werden" bis zu „Alle gängigen Videokonferenzsysteme können datenschutzkonform genutzt werden". Da es keine expliziten Verbote gibt, sind Sie als Datenschutzbeauftragter gefordert. Sie müssen Vorgaben dazu machen, welche Anforderungen solche Systeme erfüllen müssen, um datenschutzkonform genutzt werden zu können.

§

Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit
„Der HBDI geht daher davon aus, dass für die Dauer der Krisenbewältigungsmaßnahmen die gegenwärtig erhältlichen Videokonferenzsysteme aufgrund einer vorläufigen positiven Beurteilung gemäß Art. 6 Abs. 1 Buchs. d) und e) DSGVO als erlaubt gelten."

CHECKLISTE: Datenschutzkonforme Nutzung von Videokonferenzsystemen

Anforderung	Erfüllt?
Sind Regelungen zum Einsatz der Konferenzsoftware etabliert und gibt es Sanktionsandrohung bei Verstößen seitens Mitarbeiter?	☐ Ja ☐ Nein
Werden sogenannte virtuelle Hintergründe (verwischen des Hintergrunds, Bilder usw.) eingesetzt (sonst Gefahr mangelnder Privatsphäre, ggf. ungeregelter Abfluss von Unternehmensinformationen)?	☐ Ja ☐ Nein
Sind sichere Zugangsbeschränkungen/Identifikation der Teilnehmer etabliert (sonst drohen Verlust von Geschäftsgeheimnissen oder womöglich Datenpannen)?	☐ Ja ☐ Nein
Gibt es Löschrichtlinien für die personenbezogenen Daten (ohne Regelung und Anwendung drohen mögliche Verstöße gegen das Datenschutzrecht)?	☐ Ja ☐ Nein
Ist eine Meldekette für Störungen oder Auffälligkeiten bei der IT-Nutzung etabliert (ohne Meldekette drohen Datenverluste, Kompromittierung der IT-Sicherheit,; Datenpannen)?	☐ Ja ☐ Nein
Ist sichergestellt, dass der Dienstleister die datenschutzrechtlichen Anforderungen erfüllt (Vertrag Auftragsverarbeitung, EU-Standardvertragsklauseln, Datenhaltung in Deutschland usw.)?	☐ Ja ☐ Nein
Werden die Kommunikation und auch ggf. bereitgestellt Dateien sicher verschlüsselt?	☐ Ja ☐ Nein
Kann der Anbieter Zertifikate zu Datensicherheit (ISO 27001 usw.) vorlegen?	☐ Ja ☐ Nein

Empfehlung: Gängige Lösungen wie Cisco WebEx, GoToMeeting oder Microsoft Teams. Auch Zoom, das wegen zahlreicher Sicherheitslücken kritisiert wurde, erfüllt mittlerweile alle datenschutzrechtlichen Mindestanforderungen. Sie sollten ein besonderes Augenmerk darauf legen, ob die erforderlichen Sicherheitsmaßnahmen zentral administriert werden können. Dies hat immer den Vorteil, dass Fehlkonfigurationen der Mitarbeiter ausgeschlossen werden können. Microsoft Teams ist ein Beispiel für ein zentral administrierbares Videokonferenzsystem.

Mein Tipp
Erstellen Sie gemeinsam mit der Personal- oder Marketingabteilung einen Flyer zur datenschutzkonformen Nutzung von Videokonferenzsystemen und sorgen Sie dafür, dass dieser allen Mitarbeitern zur Verfügung gestellt wird. Damit können Sie sicher sein, dass das Thema die erforderliche Aufmerksamkeit erhält und gleichzeitig der Datenschutz präsent ist.

Auch wenn einige Aufsichtsbehörden derzeit bei gängigen Videokonferenzsystemen Datenschutzmängel sehen, gab es bisher noch keine konkreten Verbote. Demnach können auch keine Bußgelder verhängt werden, weil Sie im Unternehmen solche Systeme nutzen. Die kritische Haltung der Aufsichtsbehörden im Hinblick auf Videokonferenzsysteme wird derzeit in Fachkreisen intensiv diskutiert. Ebenso wehren sich auch die Hersteller wie Zoom oder Microsoft. Die meisten Juristen vertreten die Meinung, dass keine Bußgelder zu befürchten sind. Wichtig ist aber, dass Sie als Datenschutzbeauftragter alle erforderlichen Dokumentation- und Informationspflichten bei der Nutzung von Videokonferenzsystemen erfüllen.

Dazu zählen neben den Einträgen im Verzeichnis der Verarbeitungstätigkeiten eine Information zur Datenverarbeitung für die Nutzer - an Besten online - und eventuelle die Durchführung einer Datenschutzfolgenabschätzung. Mit diesen formalen Anforderungen können Sie auch gegenüber einer Aufsichtsbehörde nachweisen, dass Sie datenschutzkonform gehandelt haben.

Fazit
Zusammenfassend lässt sich sagen, dass Sie als Datenschutzbeauftragter auch in Krisenzeiten Ihrem Unternehmen zahlreiche Lösungswege aufzeigen können, sofern folgende Maßgaben beachtet werden:

- Bei der Auswahl einer geeigneten Videokonferenzlösung bzw. eines Anbieters kommt es darauf an, dass die benötigten bzw. gewünschten Funktionalitäten abgebildet werden und das Unternehmen/der Anwender diese in geeigneter Weise einsetzen kann. Dazu gehört auch, dass sich Funktionalitäten je nach Bedarf an- und abschalten lassen.
- Das Produkt sollte zudem in der Lage sein, die Wahrnehmung der Betroffenenrechte gewährleisten zu können.
- Mit dem Anbieter sollte ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen werden können, sofern es sich nicht um eine gemeinsame Verantwortlichkeit handelt. Dazu sollten geeignete und benutzerfreundliche technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO in der Anwendung implementiert sein, um den einfachen, aber sicheren Umgang sicherzustellen.
- Gleichzeitig ist aber auch die innerbetriebliche Organisation von Bedeutung, da der datenschutzkonformer Einsatz von Videokonferenzsystemen auch maßgeblich vom Verhalten eines jeden Mitarbeiters abhängt. Interne Richtlinien sind dafür ein sehr wichtiges Instrument, sie sollten nicht nur erstellt werden, sondern Beschäftigten inhaltlich durch Mitarbeiterschulungen vermittelt und in der täglichen Arbeit jederzeit zur Verfügung stehen.
- Schlussendlich sollten die Einführung und Umsetzung obiger Maßnahmen, möglicherweise etwaige Datenschutzfolgenabschätzungen (DSFA) zwecks Erfüllung der Rechenschaftspflicht dokumentiert werden (ggf. auch im Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO).

Bitte +1 Zeile

Nur so können Sie eventuellen Prüfungen seitens der Datenschutzaufsichtsbehörden beruhigt entgegensehen.

Dokumentation. Wie stellen Sie die Dokumentationspflichten sicher?

In Krisenzeiten werden Verfahren geändert und etablierte Kontrollen oder Dokumentationsanforderungen außer Kraft gesetzt. Diese Entscheidungen werden regelmäßig im Notfallstab beschlossen und dann zur Umsetzung an die Fachbereiche kommuniziert. In der Krise gelten dennoch alle datenschutzrechtlichen Dokumentations- und Nachweispflichten.

Sie als Datenschutzbeauftragter sollten auf diese rechtlichen Anforderungen hinweisen und darauf hinwirken, dass die Beteiligten diese auch in Krisenzeiten beachten. Es kann jedoch in dieser Krisensituation durchaus erforderlich sein, Verfahren temporär zu ändern, um z. B. Prozesse schneller oder mit weniger Personal durchführen zu können. Solche Verfahrensänderungen müssen jedoch dokumentiert und von Ihnen auf ihre Datenschutzrelevanz hin geprüft werden.

Mein Tipp
Erstellen Sie ein Formular für die Dokumentation von Verfahrensänderungen und wirken Sie darauf hin, dass der Leiter des Notfallstabs die Fachbereiche anweist, Verfahrensänderungen mithilfe des Formulars zu dokumentieren. Vereinbaren Sie, dass die Formulare zentral abgelegt werden und dass wesentliche Änderungen an Verfahren mit personenbezogenen Daten mit Ihnen abzustimmen sind. So sind Sie jederzeit informiert und können ggf. nachprüfen, ob der Datenschutz im Unternehmen auch in der Krise umgesetzt wird. (Ein Muster-Formular finden Sie in den Anlagen auf Seite XX).

Achtung!
Verstöße gegen Dokumentationspflichten, wie etwa aus Art. 30 DSGVO (Erstellung von Verarbeitungsverzeichnissen) oder Art. 33 Abs. 5 DSGVO (Dokumentation eines Datenschutzvorfalls), können sogar direkt bußgeldbewährt sein (vgl. Art. 83 Abs. 4 lit. a) DSGVO).

Ergeben sich Risiken, sind diese zu beschreiben und z. B. dem Leiter des Notfallstabs zur Kenntnis zu bringen. Der Leiter des Notfallstabs oder der jeweilige Kompetenzträger im Unternehmen kann dann die Verfahrensänderung und damit auch die Akzeptanz der Risiken genehmigen. Dies natürlich nur dann, wenn die Rechte der Betroffenen nicht einem zu hohen Risiko ausgesetzt werden.

Hier sind Sie auch als Datenschutzbeauftragter gefragt. Denn Datenschutzrisiken müssen ebenso analysiert und bewertet werden.

Mein Tipp
In der Krise ist es oft schwierig, papiergebundene Formulare, die z. B. zur Erfüllung der Informationspflichten genutzt werden, oder auch formulargebundene Einwilligungserklärungen zu verwenden. Setzen Sie sich dafür ein, dass elektronische Verfahren etabliert werden, die geeignet sind, die papiergebundenen Formulare zu ersetzen. So kann eine Einwilligungserklärung auch per E-Mail abgegeben werden oder ein Kunde erhält die Informationen zum Datenschutz per Link auf die Datenschutzerklärung auf der Firmenwebseite. In einigen Fällen (schriftliche Einwilligungen usw.) müssen solche E-Mails oder andere elektronische Dokumente aufbewahrt werden. Nach der Krise können diese elektronischen Dokumente ggf. elektronisch archiviert oder einfach ausgedruckt werden. So können die Dokumentations- und Nachweispflichten pragmatisch erfüllt werden.

Die Dokumentation sollte den folgenden Zwecken dienen:
- Transparenz und Effizienz intern und extern schaffen
- Mitarbeiter sensibilisieren und schulen
- nachvollziehbares Prozessmanagement
- Datenschutzkonformität nach der DSGVO sicherstellen
- Grundlage für mögliche Audits
- Grundlage für eine etwaige Zertifizierung
- Kommunikationsmittel und Nachweis gegenüber der Aufsichtsbehörde
- Vertragsmanagement
- Kommunikationsmittel gegenüber Dritten (Auftragsverarbeitung, Vergabe usw.).

Datenschutz ist ohne sachgerechte Dokumentation kaum möglich. Gerade in Krisenzeiten ist es sehr wichtig, dass alle Verfahren und Prozessänderungen dokumentiert werden. Um diese Anforderungen erfüllen zu können, sollten Sie auf die Unterstützung einer Datenschutzsoftware bauen. Auf dem Markt gibt es sehr viele gute Software für den Datenschutzbeauftragten, die Sie gerade bei Ihren Dokumentationspflichten unterstützen kann.

Sie sollten sich einige Produkte wie z. B. audatis Manager, otris privacy oder privacySoft einmal anschauen. Auch Produkte wie Verinice (BSI Grundschutz) sind für Sie als Datenschutzbeauftragter eine wertvolle Unterstützung. Solche Tools sind zumeist auch für die Dokumentation der TOMs geeignet und decken damit die Dokumentationspflichten vollständig ab. Solche Tools können Ihnen sehr viel Zeit einsparen. Insbesondere bei Prüfungen seitens der Aufsichtsbehörden können Sie auf Knopfdruck alle Informationen bereitstellen. Gleiches gilt bei Auskunftsersuchen von Betroffenen.

Fazit
Die genannten Zwecke müssen die Dokumentationen auch in der Krisensituation erfüllen. Mögliche Erleichterungen können z. B. dadurch erzielt werden, dass die Dokumentation zunächst formlos und nur in Stichpunkten erfolgt. Als Datenschutzbeauftragter sollten Sie sich mit den Fachabteilungen in Verbindung setzen und gemeinsam Möglichkeiten erarbeiten, wie die Dokumentationspflichten erfüllt werden können und welche Erleichterungen möglich sind.

Rechte der Betroffenen. Was müssen Sie konkret beachten?

In der Krise sind grundsätzlich alle Rechte der Betroffenen zu wahren. Hierzu zählen insbesondere die nachfolgenden Prozesse:

- transparente Information und Kommunikation (Art. 12 DSGVO)
- Informationspflicht und Recht auf Auskunft (Artt. 13, 14, 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung, Einschränkung der Verarbeitung Mitteilungspflichten (Artt. 17, 18, 19 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht und automatisierte Entscheidungsfindung, Beschränkungen (Artt. 21, 22, 23 DSGVO)

Die Aufsichtsbehörden haben kommuniziert, dass auch in der Krise sichergestellt sein muss, dass diese Rechte der Betroffenen gewahrt werden. Die Herausforderungen in der Krise liegen hier regelmäßig darin, dass die Prozessverantwortlichen gerade im Homeoffice nicht auf alle Daten und Dokumente zugreifen können und interne Kommunikationswege getrennt sind. Es kann z. B. das Auskunftsersuchen eines Betroffenen nicht bearbeitet werden, weil die Post nicht an das Homeoffice weitergeleitet wird. So verstreichen schnell Bearbeitungsfristen. Zu bedenken ist auch, dass Mitarbeiter im Homeoffice oftmals nicht auf alle Unternehmensanwendungen oder Daten zugreifen können, weil die Systeme nicht remote erreichbar sind. Dann können auch keine Berichtigungen, Auskunftsersuchen oder Löschungen durchgeführt werden.

§

Zentrale Fristen in der DSGVO

- Art. 12 Abs. 3 in Verbindung mit Art. 15 DSGVO: Auskunft in der Regel innerhalb eines Monats, Verlängerung um weitere zwei Monate bei Komplexität und hoher Anzahl von Anträgen
- Art. 33 Abs. 1 DSGVO: Meldung von Datenschutzverletzungen in der Regel binnen 72 Stunden nach Kenntnis

Sie sollten demnach prüfen, ob folgende Anforderungen für die genannten Prozesse erfüllt sind.

CHECKLISTE: Prozesse zur Wahrung der Rechte der Betroffenen

Anforderung	Erfüllt?
Sind für alle Prozesse Verantwortliche und Vertreter benannt und sind diese auch im Einsatz?	☐ Ja ☐ Nein
Ist sichergestellt, dass die Post auch an die Mitarbeiter im Homeoffice zugestellt wird?	☐ Ja ☐ Nein
Ist organisiert, dass zentrale Anlaufstellen für Externe funktionsfähig sind (Pförtner, Telefonzentrale, Info-E-Mail-Adresse, Servicestellen usw.)?	☐ Ja ☐ Nein
Ist sichergestellt, dass die Kommunikationszentralen die Mitarbeiter im Homeoffice erreichen können (Telefonlisten, Adresslisten usw.)?	☐ Ja ☐ Nein
Ist sichergestellt, dass die Mitarbeiter im Homeoffice alle Kollegen erreichen können (Telefonlisten usw.)?	☐ Ja ☐ Nein
Ist sichergestellt, dass bei Ausfall von Personal kurzfristige Vertretungen eingerichtet werden können (Berechtigungsvergabe, E-Mail-Umleitungen, Schlüssel, Programmzugriffe usw.)?	☐ Ja ☐ Nein
Ist dafür gesorgt, dass Mitarbeiter im Homeoffice ggf. Post versenden können (Druckereinrichtung usw.)?	☐ Ja ☐ Nein
Sind die Mitarbeiter und deren Vertreter ausreichend geschult und sensibilisiert (Priorisierung der Bearbeitung, Bearbeitungsfristen usw.)?	☐ Ja ☐ Nein

Gerade die Wahrung der Rechte der Betroffenen ist immens wichtig. Termine werden leicht überschritten, Auskünfte unzureichend erstellt oder Anfragen von Betroffenen werden einfach ignoriert oder übersehen. Versäumnisse oder Fehlhandlungen führen hier regelmäßig zu Beschwerden der Betroffenen bei den Datenschutzaufsichtsbehörden. Solche Beschwerden sind ein hohes Risiko, da die Aufsichtsbehörden diesen Beschwerden nachgehen müssen.

Je nachdem, welche Betroffenenrechte nicht gewahrt wurden, reagieren die Aufsichtsbehörden mit empfindlichen Bußgeldern. Das ist auch nachvollziehbar, denn der Datenschutz soll ja gerade die Rechte der Betroffenen schützen.

Fazit

Als Datenschutzbeauftragter sollten Sie auch in der Krise darauf hinwirken, dass alle erforderlichen Prozesse zur Wahrung der Rechte der Betroffenen ordnungsgemäß und fristgerecht im Unternehmen durchgeführt werden können. Dazu ist es auch notwendig, den Mitarbeitern und Führungskräften deutlich zu machen, dass diese Prozesse hohe Priorität haben. Denn sonst bleiben z. B. Auskunftsersuchen oder Löschanträge liegen, weil sie allgemeinen Geschäftsanforderungen untergeordnet werden oder erst gar nicht bei den Verantwortlichen ankommen.

Schulung. Was müssen Sie den Mitarbeitern an die Hand geben?

Mitarbeiter zu schulen und zu sensibilisieren ist gerade in der Krise sehr wichtig. Müssen die Mitarbeiter sich doch kurzfristig an neue Arbeitsprozesse, Arbeitsweisen und auch neue IT-Systeme gewöhnen. Da kann es leicht zu Datenpannen mit schwerwiegenden Folgen kommen.

Als Datenschutzbeauftragter sollten Sie schnellstmöglich die folgenden Schritte unternehmen:

- Kommunizieren Sie, dass verbindliche Regelungen zum Homeoffice benötigt werden, weil es eine gesetzliche Anforderung (DSGVO) ist.
- Erläutern Sie, wie ein Mitarbeiter seinen Laptop sichern kann, wie er Updates ziehen und den Virenschutz aktivieren kann.
- Erläutern Sie, wie der VPN-Zugang zu installieren oder zu nutzen ist bzw. wie die firmeneigene Cloud-Lösung genutzt werden kann.
- Wenn es bislang keinen Web Access gab: Erläutern Sie Ihren Mitarbeitern, wie sie über die Weboberfläche an die E-Mails gelangen können.
- Kommunizieren Sie zu Meldepflichten und Meldewegen bei einer Datenpanne.
- Sensibilisieren Sie zu Risiken des Social Engineering und Social Hackings. Emotet & Co. kommen zu Zeiten von COVID-19 über entsprechende E-Mail- und sonstige elektronische Nachrichten verstärkt ins Firmennetzwerk!
- Sensibilisieren Sie zu den Risiken neuer Kommunikationsverfahren wie Videokonferenz, Telefonkonferenz, WhatsApp usw.

Mein Tipp
Drehen Sie doch ein kurzes Video (maximal drei Minuten), in dem Sie den Mitarbeitern die wichtigsten Sicherheitsmaßnahmen erläutern. So können Sie präsent bleiben und sicher sein, dass Sie die Aufmerksamkeit erhalten, die Sie benötigen. Publizieren Sie das Video im Intranet. Wenn Sie regelmäßig solche Videos veröffentlichen, bleiben Sie in Kontakt mit den Mitarbeitern und bringen den Datenschutz im Unternehmen voran. Eine andere Möglichkeit sind Webinare zu zentralen Datenschutzthemen. Auch damit können Sie mit geringem Aufwand sehr effektiv schulen.

Darüber hinaus sollten Sie darauf hinwirken, dass die Mitarbeiter nachfolgende Sicherheitsanforderungen beachten:

- Es müssen sichere Passwörter für Notebook und VPN-Einwahl eingesetzt werden.
- Rechner müssen beim Verlassen des Arbeitsplatzes unverzüglich gesperrt werden. Bei mobiler Nutzung sind Blickschutzfilter vorzusehen.
- Sprachassistenten wie Alexa, Siri und Google Assistant sollten ausgeschaltet werden (Mithören von Telefonaten usw.).
- Telefonate sollten vertraulich geführt werden, Mithören von Familienmitgliedern möglichst vermeiden (analog Telefonieren in der Öffentlichkeit).
- Familienmitglieder oder Besucher sind Dritte!
- Akten müssen sicher entsorgt werden.
- Daten müssen im Unternehmensnetzwerk gesichert werden.
- Die Nutzung privater E-Mail-Accounts oder privater Cloud-Speicher, privater USB-Sticks usw. ist verboten.
- Betriebliche USB-Sticks müssen verschlüsselt werden.

Fazit
Gerade in Krisenzeiten ist es wichtig, die Mitarbeiter regelmäßig zur Datensicherheit und Datenschutz zu sensibilisieren und zu schulen. Nutzen Sie alle Kanäle, die Ihnen zur Verfügung stehen, und weisen Sie insbesondere auf die Risiken unsicherer Passwörter, Phishing und Social Engineering in Zeiten von COVID-19 hin.

Mitarbeiter im Homeoffice und vor Ort. Wie stellen Sie den Datenschutz sicher?

Um Ansteckungen zu vermeiden, befindet sich ein Großteil der Mitarbeiter eines Unternehmens im Homeoffice. Ein Teil arbeitet jedoch vor Ort, da nicht alle Arbeiten aus dem Homeoffice erledigt werden können. Eine Herausforderung dabei sind die sichere Kommunikation zwischen diesen räumlich entfernten Gruppen und die Übergabe von papiernen Dokumenten. Aus Sicherheitsgründen sollten private Drucker im Homeoffice nicht erlaubt sein.

Als Datenschutzbeauftragter sollten Sie darauf hinwirken, dass im ersten Schritt sichergestellt wird, dass alle Beschäftigten ausschließlich über entsprechend gesicherte dienstliche E-Mail-Adressen kommunizieren. Die Nutzung privater E-Mail-Adressen muss verboten sein.

Setzen Sie sich mit den Fachabteilungen und der IT in Verbindung und lassen Sie erheben, welche Daten sich derzeit an welchen Stellen befinden. So können Sie auch in der Krise prüfen, ob diese Daten datenschutzkonform verarbeitet werden, und nach der Krise ermitteln, ob Daten ins Unternehmen

zurückzuführen sind oder an bestimmten Stellen gelöscht werden müssen. Zudem helfen Ihnen diese Informationen auch bei der Beantwortung eines Auskunftsersuchens oder der Erstellung von unternehmensweiten Löschkonzepten nach der Krise.

Ist kein solcher Cloud-Speicher vorhanden, können Sie auch entsprechende Dienste im Internet nutzen.

Eine gute Lösung ist Firefox Send (https://send.firefox.com). Dieser Service ermöglicht einen sicheren Datenaustausch.

CHECKLISTE: Bedrohungen und Sicherheitsmaßnahmen beim Einsatz von Videokonferenzsystemen

Speicherort	Sensibilitätsstufe (offen, intern, vertraulich, streng vertraulich)	Verantwortlicher Fachbereich	Genutzt?
Rechenzentrum intern			☐ Ja ☐ Nein
Rechenzentrum Dienstleister			☐ Ja ☐ Nein
Cloud-Dienste (E-Mail, Office 365, CRM-Lösungen)			☐ Ja ☐ Nein
Interne PCs			☐ Ja ☐ Nein
Extern Homeoffice			☐ Ja ☐ Nein
Mobile Geräte (Notebook, Smartphone usw.)			☐ Ja ☐ Nein
Cloud-Speicher (DropBox, iCloud, OneDrive)			☐ Ja ☐ Nein
Mobile Datenträger (USB, Kamera, CD)			☐ Ja ☐ Nein

Mein Tipp
Sollte es aus technischen Gründen nicht möglich sein, dass Mitarbeiter ihre geschäftlichen E-Mail-Adressen nutzen, prüfen Sie den Einsatz von Messengern wie WhatsApp, Signal oder Threema. Solange keine Dokumente auf diesem Wege ausgetauscht werden, können die Beschäftigten auch private Smartphones nutzen. Müssen die Mitarbeiter auch Dokumente (Fotos von Dokumenten) austauschen, sollten sie dienstliche Smartphones nutzen. Die Kommunikation ist Ende-zu-Ende-verschlüsselt und damit sicherer als die Nutzung privater E-Mail-Adressen.

Wenn Mitarbeiter papiergebundene Dokumente austauschen müssen, sollten Sie darauf hinwirken, dass diese Dokumente eingescannt und entweder per dienstliche E-Mail oder auf einem Cloud-Speicher des Unternehmens bereitgestellt werden. Bei der Nutzung von Cloudspeichern sollten Sie eine verschlüsselte Ablage fordern.

Müssen Dokumente im Homeoffice unterzeichnet werden, bleibt tatsächlich nur der Postversand oder Sie können den Mitarbeitern im Homeoffice ein Faxgerät zur Verfügung stellen. Dann sollten Sie aber auch einen Schredder bereitstellen, damit die Mitarbeiter die Dokumente auch datenschutzkonform vernichten können.

Fazit
In der Krise müssen Sie darauf hinwirken, dass die Daten des Unternehmens kontrolliert und nach organisatorischen Vorgaben verarbeitet werden. Dazu sollten Sie sich mit der IT-Abteilung und der Fachabteilung in Verbindung setzen und entsprechende technische und organisatorische Maßnahmen erarbeiten, die sicherstellen, dass Daten jederzeit unter der Kontrolle des Unternehmens stehen. Ebenso muss gewährleistet werden, dass Daten auch in der Krise nach den datenschutzrechtlichen Vorgaben verarbeitet werden.

Cloud-Speicher. Was müssen Sie konkret beachten?

Cloud-Speicher bieten gerade in der jetzigen Krise eine sehr gute Möglichkeit, Dateien mit Mitarbeitern im Homeoffice oder anderen Stellen auszutauschen. Der Funktionsumfang reicht hierbei von der Bereitstellung eines Cloud-Speichers bis hin zu komplexen Services wie z. B. Microsoft 365 ehemals Office 365. Solche Services bieten Funktionen wie Videokonferenzen, E-Mail, Cloud-Speicher und vieles mehr in einem Produkt. Diese Cloud-Services oder Cloud-Speicher bergen jedoch erhebliche Datenschutzrisiken. Als Datenschutzbeauftragter sollten Sie sich mit der IT-Abteilung in Verbindung setzen und darauf hinwirken, dass sie die nachfolgenden Risiken vor der Nutzung eines Cloud-Services analysiert und entsprechende risikominimierenden Maßnahmen umsetzt.

Risiken bei der Nutzung von Cloud-Services

- unzureichende vertragliche Regelungen in Hinblick auf Datenschutz (Vertrag Auftragsverarbeitung usw.)
- unklare Informationen über Speicherort der Daten (innerhalb der EU oder nicht)
- unzureichende Netzwerk-Performance für eine flächendeckende Nutzung
- möglicher „Vendor Lock-in“ (Abhängigkeit vom Dienstleister) bzw. hohe Kosten einer späteren Migration
- keine oder unvollständige Integration in interne Prozesse und Infrastruktur
- unzureichende Härtung/unsichere Konfiguration des Cloud-Diensts
- fehlende Schulung der Anwender/Administratoren in Bezug auf die Datensicherheit und den Datenschutz
- stetige, plötzliche und/oder komplexe Veränderungen der Cloud-Angebote
- unzureichende Definition der Zuständigkeiten von Anbieter und Nutzer (gemeinsame Verantwortlichkeit usw.)

Eine detaillierte Checkliste zu den Risiken der Cloud-Nutzung finden Sie in den Anlagen auf Seite 24.

Mein Tipp
Gerade die für die Nutzung umfangreicher Cloud-Services erforderliche Bandbreite im Unternehmensnetzwerk und am Internetzugang wird oft unterschätzt. Weisen Sie darauf hin, dass die IT-Abteilung diese Bandbreitenanforderungen prüfen soll. Insbesondere die Kombination von Videokonferenzen und Nutzung von Cloud-Speichern führt leicht zu Performance-Problemen auch im internen Netz. Das kann zu Ausfällen von Produktivsystemen führen.

Als Datenschutzbeauftragter sollten Sie bei der Nutzung von Cloud-Services darauf hinwirken, dass zumindest die nachfolgenden Anforderungen umgesetzt werden:

- Grundsätzlich sollten betriebliche Daten auf Cloud-Speichern des Unternehmens gespeichert werden.
- Die Nutzung privater Cloud-Speicher sollte verboten sein.
- Wenn Sie mit Dienstleistern arbeiten, muss sichergestellt sein, dass die Daten verschlüsselt übertragen und verschlüsselt abgelegt werden.
- Die Rechenzentren sollten in EWG-/EU-Ländern stehen.
- Ein Vertrag zur Auftragsverarbeitung muss vorhanden sein.
- Eine 2FA ist erforderlich.
- Administration und Benutzerverwaltung sollten zentral in der IT-Abteilung liegen.
- Das Need-to-know-Prinzip muss auch in der Cloud durchgesetzt werden.
- Freigaben für Externe sollten nur mit Passwort und Anmeldung möglich sein.

Fazit
Es gibt in Deutschland viele Anbieter von reinen Cloud-Speichern. Diese Services können in der Regel schnell und unproblematisch im Unternehmen eingeführt werden. Umfangreichere Cloud-Services wie Microsoft 365 erfüllen in der Regel auch alle datenschutzrechtlichen Anforderungen. Hier liegen die Risiken in der Regel darin, dass diese komplexen Services nicht sachgerecht administriert und die Nutzer nicht ausreichend geschult werden. In der Krise wird dies auch kaum möglich sein. Sie sollten demnach darauf hinwirken, dass nur die Dienste genutzt werden, die in der Krise tatsächlich nötig sind, und dass diese Dienste sachgerecht administriert werden. Auch die Schulung der Mitarbeiter ist absolut erforderlich.

UYOD. Ist ein Betrieb zulässig?

Vor der Krise wurde viel darüber diskutiert, welche Maßnahmen erforderlich sind, wenn Mitarbeiter Unternehmensdaten auf privaten Endgeräten verarbeiten dürfen. Bring your own Device (BYOD) birgt nach wie vor erhebliche Risiken, die aber mit entsprechenden umfangreichen Sicherheitsmaßnahmen minimiert werden können. In Krisenzeiten, in denen viele Mitarbeiter im Homeoffice arbeiten, fordern natürlich zahlreiche Unternehmen, dass diese ihre privaten Endgeräte nutzen. Use your own Device (UYOD) ist demnach das Motto in der Krise. Sie als Datenschutzbeauftragten stellt UYOD vor die gleichen Herausforderungen wie BYOD.

Mein Tipp
Der Bundesbeauftragte für Datenschutz und Informationsfreit hat 2019 gefordert, dass private Endgeräte nicht für betriebliche Zwecke eingesetzt werden dürfen. Inwieweit dies in einem Bußgeldverfahren tatsächlich vor Gericht Bestand haben kann, ist nicht klar. Als Datenschutzbeauftragter sollten Sie aber zumindest auf dieses Risiko hinweisen.

Nutzen Mitarbeiter trotzdem ihre privaten Geräte, sollten Sie als Datenschutzbeauftragter verlangen, dass zumindest die nachfolgenden Anforderungen umgesetzt werden. Denn ohne verbindliche Regelungen drohen Datenschutzpannen.

- Sicherheitsrichtlinie festlegen und Mitarbeiter sensibilisieren
- IT-Sicherheit der eingesetzten Systeme (Sicherheitskonzept UYOD)
- Datenträgerverschlüsselung
- sicherer Remote-Zugriff (idealerweise VPN), notfalls sichere Cloud-Lösungen (nicht Dropbox oder Ähnliches)
- Datensicherung, idealerweise nicht lokal
- zeitnahe Verlustmeldung (Meldeketten)
- Support für Telearbeitsplätze
- Aufklärung über Gefahren bei Arbeiten mit unternehmensfremden IT-Systemen
- Entsorgung von vertraulichen Informationen.
- sichere und verifizierte Kommunikationswege

Mein Tipp
Beim Einsatz von UYOD und der Nutzung von Cloud-Services sollten Sie prüfen, ob eine DSFA erforderlich ist. So können Sie die Risiken und die datenschutzrechtlichen Belange am besten darstellen und auch die Unternehmensleitung sachgerecht informieren.

Fazit
Grundsätzlich sollten keine betrieblichen Daten auf privaten Endgeräten verarbeitet werden. UYOD ist daher unter Sicherheits- und Datenschutzgesichtspunkten ein sehr hohes Risiko. Ziel muss es sein, keine Unternehmensdaten auf den privaten Endgeräten zu speichern, sondern ausschließlich im Unternehmensnetz oder verschlüsselt in der Cloud. Ebenso müssen die Netzwerkverbindungen mit VPN/2FA und die Cloud-Services mit 2FA abgesichert werden. Können diese Anforderungen nicht umgesetzt werden, müssen Sie als Datenschutzbeauftragter zumindest auf die hohen Risiken hinweisen. Dies können Sie am besten mit einer DSFA. Damit können Sie alle Risiken dokumentieren und sachgerecht bewerten.

Schulung. Wie erreichen Sie die Mitarbeiter in der Krise?

Als Datenschutzbeauftragter müssen Sie die Mitarbeiter gerade in der Krise zu vielen neuen Themen schulen und sensibilisieren. Die Herausforderung besteht aber nicht nur darin, die Themen festzulegen und adressatengerecht aufzubereiten. Sie müssen die Mitarbeiter im Homeoffice und im Unternehmen gleichermaßen erreichen. Vielleicht arbeiten Sie ja auch im Homeoffice und haben keinen direkten Kontakt mehr zu den Mitarbeitern.

Gerade die Mitarbeiter im Homeoffice erhalten Informationen in der Regel per E-Mail oder über das zentrale Intranet des Unternehmens. In Krisensituation werden die Mitarbeiter mit unzähligen Informationen überflutet. Meldungen der Geschäftsleitung, des Notfallstabs, der Personalabteilung und nicht zuletzt der Vorgesetzten überschlagen sich geradezu. Sie müssen also einen Weg finden, die Mitarbeiter so anzusprechen, dass Ihre Botschaften nicht in der großen Informationsflut untergehen. Zudem müssen Sie beachten, dass die Mitarbeiter in der Krise oft gestresst und meist auch überarbeitet sind.

Wie Sie Mitarbeiter in der Krise schulen – in 3 Schritten zum Erfolg

Schritt 1: Wählen Sie zunächst die Themen aus, die Sie schulen wollen. Versuchen Sie, Ihre Themen so kurz wie möglich zu beschreiben, also wenige Folien mit wenigen Bullet Points und wenig Text, und Ihre Botschaften humorvoll und nicht mit erhobenem Zeigefinger zu verfassen. Nutzen Sie Bilder, Grafiken und Animationen. Kein Mitarbeiter wird in der Krise umfangreiche Schulungstexte lesen wollen.

Schritt 2: Wählen Sie das Medium aus, über das Sie die Mitarbeiter schulen wollen. Sie sollten ein Medium aussuchen, das Aufmerksamkeit hervorruft:

Option 1: Video

Drehen Sie z. B. mit Ihrem Smartphone ein Video, in dem Sie die Mitarbeiter persönlich ansprechen und Ihre Botschaften verbal vortragen.

Option 2: Screen Cast mit Ton (Bildschirm aufzeichnen)

Erstellen Sie eine PowerPoint-Präsentation, zeichnen Sie Ihren Vortrag mit einem Screen-Cast-Programm inklusive Ton auf und stellen Sie diesen Film im Intranet bereit. Solche Tools gibt es kostenlos (z. B. VLC-Player, Quick Time Player, Cam Studio).

Option 3: Webinar

Wollen Sie in Kontakt mit Ihren Mitarbeitern treten und vielleicht mehr als nur ein paar Minuten schulen, können Sie ein Webinar veranstalten. Es gibt Angebote namhafter Hersteller wie z. B. Clickmeeting oder Zoom, die für eine monatliche Gebühr von 22 € zu nutzen sind.

Option 4: PowerPoint als Bildschirmpräsentation

Sie können auch eine PowerPoint-Präsentation erstellen und diese als Bildschirmpräsentation abspeichern. Verwenden Sie plakative Bilder, Animationen und eingängliche Texte. Diese Präsentationen dürfen auch nicht umfangreich sein, sonst verlieren Sie schnell die Aufmerksamkeit der Zuschauer.

Schritt 3: Haben Sie Ihre Schulung ausgearbeitet, müssen Sie noch dafür sorgen, dass die Mitarbeiter an der Schulung teilnehmen. Gehen Sie auf die Unternehmensleitung zu und bitten Sie um ein entsprechendes Rundschreiben der Unternehmensführung oder sprechen Sie die Mitarbeiter per E-Mail an. Lassen Sie sich etwas einfallen und sprechen Sie vielleicht mit den Kollegen aus der Marketingabteilung.

Fazit
Mit diesen drei Schritten können Sie die Mitarbeiter auch im Homeoffice oder am Arbeitsplatz erreichen und schulen. Nutzen Sie neue Medien und interessant aufbereitete Botschaften. Gerade Mitarbeitern im Homeoffice fehlen persönliche Kontakte. Da ist eine Videobotschaft gerne gesehen. So erreichen Sie die Mitarbeiter auch in Krisenzeiten und bringen den Datenschutz voran.

Löschkonzept. Was müssen Sie beachten, was müssen Sie fordern?

In der Krise werden Daten oft außerhalb der normalen Verfahren gespeichert und verarbeitet. So werden beispielsweise umfangreiche Dateien per E-Mail verteilt, weil der Kollege im Homeoffice nicht auf das gemeinsame Laufwerk oder die entsprechende Anwendung zugreifen kann. Dateien werden auf den lokalen Rechnern im Homeoffice gespeichert, weil das Arbeiten über VPN zu langsam ist, oder es werden Daten in einer neuen Cloud gespeichert. Die Möglichkeiten sind nahezu unbegrenzt.

Mein Tipp
Oft senden Mitarbeiter in der Krise Dateien mit umfangreichen personenbezogenen Daten per E-Mail. In der Regel werden diese Dateien auch außerhalb des E-Mail-Postfachs gespeichert. Solche Dateianhänge sollten in den Postfächern gelöscht werden. Sensibilisieren Sie Ihre Mitarbeiter entsprechend. Das reduziert auch die Größe der Postfächer und macht das E-Mail-Programm schneller. Wirken Sie darauf hin, dass solche Daten möglichst zentral gespeichert werden. So kann eine Löschung in der Regel besser gewährleistet werden.

Als Datenschutzbeauftragter stehen Sie vor der Herausforderung, dass all diese Daten zum einen in den zentralen Datenspeicher oder die jeweiligen Anwendungen zurückgeführt werden und zum anderen auf den jeweiligen Datenspeichern wieder gelöscht werden müssen.

Um diese Herausforderungen meistern zu können, müssen Sie wissen, wo sich die Daten befinden. Dazu können Sie die in Kapitel 2 vorgestellte Checkliste nutzen. Nach der Krise müssen Sie die Fachabteilungen auffordern zu prüfen, welche Daten auf den jeweiligen Speicherorten gelöscht werden können.

Denken Sie insbesondere daran, dass Sie die nachfolgen Maßnahmen nicht vergessen:

- Akten im Homeoffice müssen vernichtet oder ins Unternehmen zurückgeführt werden.
- Daten auf privaten PCs sind zu löschen.
- Daten des Notfallstabs sind zu löschen (Gesundheitsdaten usw.).
- Gesundheitsdaten in E-Mails müssen nachträglich gelöscht werden (Excel-Listen usw.), eventuell auch auf privaten E-Mail-Accounts.
- Geschäftsgeheimnisse auf privaten E-Mail-Accounts sind zu löschen.

Fazit
Das Löschen von Daten, die in der Krise auf unterschiedlichsten Systemen abgelegt wurden, ist eine große Herausforderung, der Sie sich als Datenschutzbeauftragter stellen müssen. Der Aufwand wird erheblich sein, Sie können ihn aber durch geeignete Dokumentationen reduzieren. Weisen Sie Ihre Unternehmensleitung auf diesen Umstand hin und plädieren Sie dafür, dass die Fachabteilungen die entsprechenden Dokumentationen erstellen müssen. Gerade beim Einsatz von Homeoffice sollten Sie fordern, dass die Notebooks nach der Krise in der IT-Abteilung abgeliefert und dort vollständig gelöscht oder zurückgesetzt werden. Nur so können Sie sicherstellen, dass alle Daten, die vielleicht doch lokal gespeichert wurden, tatsächlich auf dem Gerät gelöscht werden.

Berechtigungen. Was müssen Sie konkret prüfen?

Als Datenschutzbeauftragter sollten Sie darauf hinwirken, dass auch während der Krise alle im Unternehmen das Prinzip der minimalen Berechtigungen wahren. Selbst wenn es in der Krise regelmäßig erforderlich wird, Berechtigungen kurzfristig zu erweitern oder im Zusammenhang mit Vertretungsregelungen an Mitarbeiter zu vergeben, muss dies innerhalb eines geregelten Prozesses erfolgen. Insbesondere müssen auch in der Krise alle Änderungen an bestehenden Berechtigungen von den jeweiligen Kompetenzträgern genehmigt und dokumentiert werden. Andernfalls können die datenschutzrechtlichen Anforderungen nicht umgesetzt werden. Es drohen nicht nur Bußgelder, sondern auch Datenpannen und Missbrauch.

Sorgen Sie dafür, dass ein Prozess zur Änderung oder Vergabe von Berechtigungen in Krisenzeiten definiert wird. Dieser Prozess muss sicherstellen, das Minimalprinzip einzuhalten, und eine Dokumentation der Änderungen gewährleisten.

Ein solcher Prozess könnte wie folgt ausgestaltet sein:

1. Es wird eine zentrale E-Mail-Adresse Berechtigungen@Unternehmen.de eingerichtet.
2. Der Mitarbeiter beantragt Berechtigungen bei seinem Vorgesetzten per E-Mail.
3. Der Vorgesetzte leitet diese E-Mail mit seiner Genehmigung an die IT oder die jeweilige verantwortliche Stelle (Schlüsseldienst, Hausverwaltung. Personalabteilung usw.) weiter.
4. Die Stelle, die die Berechtigungen vergibt, prüft den Antrag erneut auf Zulässigkeit und leitet die Mail des Vorgesetzen

mit dem Vermerk „eingerichtet“ an die zentrale E-Mail-Adresse weiter.

Für die Einhaltung des Minimalprinzips ist der jeweilige Vorgesetzte verantwortlich. Die einrichtende Stelle prüft den Berechtigungsantrag darauf hin, ob diese Berechtigung nicht gegen bestehende Regelungen verstößt. Dies ist erforderlich, weil der Vorgesetzte im Fachbereich eventuell nicht über entsprechende Detailkenntnisse verfügt, um die Kritikalität der beantragten Berechtigungen abschätzen zu können.

Beispiel: Freigabe von umfangreichen Administrationsrechten für einen Sachbearbeiter.

Die E-Mail im zentralen E-Mail-Postfach enthält durch die Weiterleitungen im Prozess alle Informationen, die für eine ordnungsgemäße Dokumentation erforderlich sind. Damit ist für jede Änderung der Antrag des Mitarbeiters, die Genehmigung des Kompetenzträgers und die Bestätigung der Rechtevergabe enthalten.

Wie ein solcher Prozess letztlich im Unternehmen umgesetzt wird, ist nebensächlich. Der Prozess muss lediglich sicherstellen, dass die Beantragung, die Genehmigung und die Einrichtung der Kompetenzen an einer zentralen Stelle dokumentiert werden. Wirken Sie darauf hin, dass die Dokumentationen nachvollziehbar sind.

Mein Tipp
Weisen Sie darauf hin, dass dieser Prozess auch wichtig ist, um kriminellen Handlungen vorzubeugen. Ohne Genehmigung und Dokumentation könnte sich z. B. ein Mitarbeiter Berechtigungen erschleichen, mit denen er Gelder auf fremde Konten überweisen kann. Die Einrichtung von Berechtigungen auf Zuruf muss auch in Krisenzeiten unterbunden werden.

Nach der Krise kann anhand dieser Dokumentation geprüft werden, ob die Berechtigungen wieder entzogen werden müssen und ob die entsprechenden Berechtigungen in den jeweiligen Zielsystemen oder Verfahren ordnungsgemäß eingerichtet wurden. Ebenso müssen diese Berechtigungen eventuell im zentralen Berechtigungsmanagement dokumentiert werden.

Fazit
Ein sachgerechtes Verfahren zur Einrichtung oder Änderungen von Berechtigungen ist essenziell für den Datenschutz und die Datensicherheit. Auch wenn viele Verantwortliche in Unternehmen während der Krise darauf pochen, solche Prüf- und Genehmigungsprozesse temporär einzustellen, gilt: Verdeutlichen Sie als Datenschutzbeauftragter die hohen Risiken und wirken Sie darauf hin, dass alle im Unternehmen die dargestellten „Minimalprozesse“ einhalten.

Schatten-IT. Welche Risiken müssen Sie kennen und welche Maßnahmen fordern?

Wenn Mitarbeiter mit den ihnen zur Verfügung stehenden IT-Systemen oder Verfahren unzufrieden sind, neigen sie dazu, sich eigene Lösungen zu schaffen. Sei es, dass sie dienstliche E-Mails auf private Smartphones umleiten oder private Cloud-Speicher dazu nutzen, Dateien für das Arbeiten im Homeoffice bereitzustellen.

Auch und gerade in der Krise müssen Sie als Datenschutzbeauftragter damit rechnen, dass Mitarbeiter im Homeoffice sich eine „eigene“ Arbeitsumgebung schaffen. Solche Arbeitsumgebungen bezeichnet man gemeinhin als Schatten-IT.

Achtung: Die Risiken solcher privaten Lösungen sind erheblich! Sie wissen nicht, wo die Daten abgelegt sind, welche Sicherheitsmaßnahmen vorhanden sind, wer auf die Daten zugreifen kann, ob die Daten nach den Vorgaben der DSGVO und weiterer gesetzlicher Anforderungen gespeichert sind.

Hier drohen nicht nur hohe Bußgelder, sondern regelmäßig Datenpannen, Datenverluste und Missbrauch von Daten. Sie müssen demnach schnellstmöglich darauf hinwirken, dass nachfolgende Maßnahmen umgesetzt werden.

Schatten-IT stellt tatsächlich ein sehr hohes Risiko dar. Denn die Daten verlassen völlig unkontrolliert das Unternehmen. Datenpannen sind in der Regel die Folge. Sprechen Sie auch mit Ihrer IT-Abteilung und versuchen Sie gemeinsam, mögliche Ursachen für Schatten-IT zu ergründen. So können Sie Schatten-IT identifizieren und beseitigen.

CHECKLISTE: Maßnahmen gegen Schatten-IT

Maßnahme	Umgesetzt?
Verbot des Einsatzes privater Software, privater E-Mail-Adressen, privater Endgeräte und privater Cloud-Services	☐ Ja ☐ Nein
Sensibilisierung der Mitarbeiter	☐ Ja ☐ Nein
Ausarbeitung von Maßnahmen zur Verbesserung der Situation (risikoorientiert und pragmatisch).	☐ Ja ☐ Nein
Einrichtung von Cloud-Services	☐ Ja ☐ Nein
Bereitstellung betrieblicher Endgeräte	☐ Ja ☐ Nein

Fazit
Als Datenschutzbeauftragter sollten Sie der Unternehmensleitung verdeutlichen, dass die Anschaffung von betrieblichen Endgeräten oder z. B. entsprechender Cloud-Services unter Risikogesichtspunkten kostengünstiger ist als die Schäden durch Datenverluste, Bußgelder oder Datenmissbrauch.

Dokumentationspflichten. Was müssen Sie beachten?

Die in der DSGVO geforderten Dokumentationspflichten müssen auch nach der Krise erfüllt werden. Als Datenschutzbeauftragter haben Sie die Aufgabe, darauf hinzuwirken, dass die Dokumentationen bei geänderten Prozessen oder neuen Verarbeitungssystemen aktualisiert werden. So müssen z. B. neue Cloud-Services auch im Verzeichnis der Verarbeitungsverfahren aufgeführt werden. Ggf. sind DSFA zu erstellen und vieles mehr. Nach der Krise sind diese Dokumentationen auf ihre Aktualität hin zu prüfen und eventuell anzupassen.

Fazit
Nach der Krise müssen Sie darauf hinwirken, dass alle Prozesse wieder in den Normalzustand vor der Krise zurückgeführt werden. Die in Kapitel 2 genannte Dokumentation über Verfahrensänderung gibt Ihnen die Möglichkeit zu prüfen, ob tatsächlich alle Verfahren zurückgeführt wurden. Ist dies nicht der Fall, müssen Sie ermitteln, inwieweit diese Verfahrensänderungen Datenschutzrelevanz haben und ob weitere Maßnahmen umzusetzen sind. Bedenken Sie auch, dass der Status quo vor der Krise nicht unbedingt der erstrebenswerte war. Nutzen Sie die Gelegenheit, überfällige Maßnahmen wie z. B. die Überarbeitung oder den Abschluss von Verträgen zur Auftragsverarbeitung anzugehen.

Organisation. Welche organisatorischen Maßnahmen müssen Sie ergreifen?

Datenschutz in Krisenzeiten ist eine große Herausforderung. Das gesamte Unternehmen befindet sich in einer Ausnahmesituation. Sowohl die Fachbereiche als auch die Mitarbeiter sind in einem hohen Maße gefordert, um die kritischsten Unternehmensprozesse am Laufen zu halten. Maßnahmen zum Datenschutz und zur Datensicherheit werden dabei regelmäßig entpriorisiert oder Vorgaben werden ignoriert.

Mein Tipp
Sie sollten mit Ihrer Unternehmensleitung sprechen und auf die Risiken hinweisen, die derzeit auch in Hinblick auf den Datenschutz und die Datensicherheit bestehen. Wirken Sie darauf hin, dass Sie in der Krise eine Hilfskraft bekommen, die Sie bei Ihren vielfältigen Aufgaben unterstützt. Ebenso sollten Sie – falls nicht schon vorhanden – die Möglichkeit erhalten, Videokonferenzen abzuhalten und mobil arbeiten zu können.

Als Datenschutzbeauftragter müssen Sie dafür sorgen, dass Sie als Ansprechpartner für alle Unternehmensbereiche auch in der Krise zur Verfügung stehen. Sie sollten sich einen Plan machen, wie Sie präsent bleiben und wie Sie mit den vielen Anfragen aus dem Unternehmen umgehen können. Das Spektrum reicht von einer regelmäßigen Sprechstunde über ein zentrales E-Mail-Postfach bis hin zu regelmäßigen Videokonferenzen. So zeigen Sie Ihr Engagement für die Mitarbeiter und den Datenschutz.

Datenschutz im Unternehmen kann nur wirksam sein, wenn die Mitarbeiter sensibilisiert und motiviert sind. Denn Datenpannen resultieren in den meisten Fällen aus Fehlhandlungen oder aus Unkenntnis der Mitarbeiter. Daran müssen Sie täglich arbeiten und dafür müssen Sie auch im Unternehmen präsent sein.

In Krisenzeiten können Sie auf ein vielfältiges Angebot von virtuellen Medien zurückgreifen. Nutzen Sie diese Medien und Sie werden die Mitarbeiter auch im Home-Office oder im Unternehmen erreichen. Sie können weiterhin persönliche Gespräche führen und vor allem auch direkte Unterstützung anbieten. Mit Videokonferenzen, Webwaren oder auch Videos können Sie den Mitarbeitern auch die neuen Richtlinien für das Arbeiten im Home-Office oder den Umgang mit Kontaktlisten (Covid-19) nahe bringen. Das ist letztlich auch eine Chance zu beweisen, dass der Datenschutz ein Vorreiter der Digitalisierung ist. Denn ohne Datenschutz und Datensicherheit wird die Digitalisierung scheitern. Privacy by Design und Security by Design sind die Garanten für eine erfolgreiche Digitalisierung.

Fazit
Schaffen Sie sich einen organisatorischen Rahmen für die Bewältigung der Krise. Als Datenschutzbeauftragter müssen Sie präsent sein und versuchen, alle erforderlichen Informationen zu erhalten. Ebenso müssen Sie dafür Sorge tragen, dass die Mitarbeiter alle Maßnahmen umsetzen, um den Datenschutz zu wahren. Regelmäßige Telefon- oder Videokonferenzen sind derzeit ein probates Mittel für einen solchen organisatorischen Rahmen. So bleiben Sie auch in der Krise am Ball.

Clean Desk. Was heißt das im Homeoffice?

Ich muss stets verhindern, dass während meiner Abwesenheit Unbefugte Zugriff auf vertrauliche Informationen erhalten. Die nachfolgenden Punkte muss ich hier beachten:

› **Büroraum im privaten Umfeld**
- ☐ Ich bewahre (streng) vertrauliche Daten sicher auf (abschließbarer Schrank usw.).
- ☐ Ich schließe ggf. den Raum ab, wenn ich ihn verlasse.

› **IT-Systeme**
- ☐ Ich sperre meine IT-Systeme beim Verlassen (WIN- und L-Tasten).
- ☐ Ich fahre meine IT-Systeme am Ende des Arbeitstags herunter.
- ☐ Ich verwende sichere Anmeldepasswörter für meine Accounts.

› **Mobile Geräte**
- ☐ Ich verwende starke Passwörter (PIN-Code mindestens sechs Zeichen).
- ☐ Ich aktiviere die Geräteverschlüsselung.
- ☐ Ich verschlüssele die Daten auf mobilen Datenträgern.
- ☐ Ich lasse IT-Geräte nur bei vertrauenswürdigen Stellen reparieren.

› **Entsorgung von Daten/Informationen**
- ☐ Ich schreddere vertrauliche Papiere.
- ☐ Ich vernichte nicht mehr benötigte Datenträger datenschutzkonform (Schredder, Entsorger).

Wichtig: Auch Reinigungskräfte, Besucher oder Familienmitglieder können Unbefugte sein. Ich muss also dafür sorgen, dass Unterlagen mit personenbezogenen Daten oder der PC auch bei kurzer Abwesenheit vor unbefugtem Zugang geschützt werden. Denn ich kann nicht ausschließen, dass jemand mein privates Büro betritt.

Cybersecurity. Welche besonderen Gefahren lauern im Homeoffice?

Die Corona-Krise nimmt Einfluss auf die Methoden von Cyberkriminellen. So warnt die Verbraucherzentrale Nordrhein-Westfalen z. B. vor gefälschten E-Mails der Sparkasse, worin Kundinnen und Kunden zur Eingabe ihrer persönlichen Daten aufgefordert werden. Die E-Mail gibt vor, dass die Übermittlung persönlicher Daten an die Sparkasse notwendig sei, um in Zeiten der Corona-Krise auch per Chat mit der Bank in Verbindung bleiben zu können. Über einen Link werden Betroffene auf eine authentisch aussehende Eingabemaske geleitet, die die Daten nach der Eingabe direkt an Betrüger sendet.

Mit solchen Angriffen muss ich auch an meinem Arbeitsplatz im Homeoffice rechnen. Die nachfolgenden Punkte zeigen mir, wie ich diese Gefahren abwehren kann:

E-Mail: Was muss ich denn konkret beachten?

Ganz grundsätzlich vermeide ich großen Ärger, indem ich unbekannte Dateien nicht öffne, den Ursprung von E-Mails überprüfe und sowohl Absender als auch enthaltene Verlinkungen gründlich hinterfrage. E-Mails sind nicht sicher. Ich kann nicht wissen, ob eine Absenderadresse gefälscht ist, ob ein Link mich zu einem Trojaner führt oder ein Dateianhang Trojaner enthält. Die nachfolgenden Regeln muss ich daher unbedingt beachten:

› Ich bin bei Werbemails (Spam) und falschen Virenmeldungen sehr vorsichtig.
› Ich antworte nie auf Spam.
› Ich abonniere Newsletter nur von seriösen Anbietern.
› Ich lasse vor Viren, Trojanern, Würmern etc. Vorsicht walten.
› Ich lösche E-Mails mit unseriösem Betreff sofort.
› Ich öffne keine Anhänge, die ich nicht angefordert habe.
› Zukünftig könnten auch Anrufe getätigt werden, in denen angeblich öffentliche Stellen Daten über die Ausbreitung der Epidemie erfassen wollen und dazu personenbezogene Informationen zu Anmeldedaten oder Zugängen zu Banken bzw. zu unserem Unternehmensnetzwerk abfragen. Ich werde bei solchen Anrufen sehr vorsichtig vorgehen und keine sensiblen Informationen preisgeben oder gar Zahlungen ausführen.
› Ich mache niemals telefonisch Angaben zu sensiblen Informationen, ohne die Identität des Anrufers zweifelsfrei festgestellt zu haben. Ich weiß, dass Behörden, Banken und anderen Institutionen diese niemals auf diese Weise abfragen.
› Zudem werden betrügerische Webportale versprechen, Lösungen für Corona-bezogene Probleme bereitzustellen und dafür Produkte oder Dienstleistungen anbieten. Ich lasse mich nicht von dieser Verlockung täuschen. Sollten wirksame Medizinprodukte auf den Markt gelangen, wird das Bundesministerium für Gesundheit darüber informieren.
› Werbe- und Pop-up-Fenster können plötzlich erscheinen, um mir entweder Heilmittel, Impfungen und Behandlungen anzupreisen oder vorzugeben, ein sicherheitsrelevantes Programm meines Arbeitgebers installieren zu wollen. Ich verzichte grundsätzlich darauf, derartige Werbefenster anzuklicken. Solche Banner oder Pop-ups können Schadsoftware enthalten, unabhängig von den Produkten, für die sie werben.

Achtung: Ist es trotz allem dazu gekommen, dass ich sensible Informationen eventuell an Betrüger versendet habe, ändere ich sofort mein Passwort. Ging es bei diesen Informationen um betriebliche Angelegenheiten, muss ich den Vorgang meiner IT-Abteilung melden. Habe ich zudem Passwörter übermittelt, die ich für mehrere Accounts verwende, werde ich sofort bei all diesen Zugängen die Passwörter zu ändern.

Insbesondere bei Links in E-Mails muss ich mich vergewissern, dass diese nicht auf gefährliche Internetseiten führen. Aber wie erkenne ich, wohin mich ein Link wirklich führt?

Wichtig: So erkenne ich den „Wer-Bereich" eines Links

Der „Wer-Bereich" bezeichnet die Domäne, auf die ein Link zeigt (Wer steckt hinter dem Link?). Diesen „Wer-Bereich" kann ich mit einer einfachen Zählmethode ermitteln. Ein Link ist immer gleich aufgebaut: http://www.Beispiel.de/home. Ich muss einfach die im Link enthaltenen „/" von links beginnend zählen. Der „Wer-Bereich" befindet sich links neben dem dritten „/", hier also „Beispiel.de".

Beispiele:

- Identifizieren Sie die tatsächliche Webadresse hinter diesem Link. Achten Sie nur auf den „Wer-Bereich"!
  http://www.amazon.de/account
  Richtig! Dieser Link führt zu Amazon.
- Lassen Sie sich nicht von Webadressen in die Irre führen, bei denen die Institution außerhalb des „Wer-Bereichs" steht.
  http://www.amazon.shop24.de/account
  Richtig! Dieser Link führt Sie NICHT zu „amazon.de", sondern zu „shop24.de". Dahinter steckt bestimmt ein Betrüger!
- Prüfen Sie den „Wer-Bereich" auch in Bezug auf Tippfehler und Buchstabendreher.
  http://www.mircosoft.com/login
  Richtig! Dieser Link führt ganz bestimmt nicht zu „microsoft.de". Auch hinter diesem Link stecken Betrüger.
- Prüfen Sie den „Wer-Bereich" genau hinsichtlich der Verwendung von ähnlich aussehenden Zeichenfolgen oder auch Zahlenfolgen.
  http://www.mediarnarkt.de/einkaufen
  Richtig! Schon wieder ein betrügerischer Link.

UYOD. Was muss ich bei betrieblichen Daten auf meinen privaten Geräten beachten?

Grundsätzlich sollte ich keine betrieblichen Daten auf privaten Endgeräten speichern oder verarbeiten. Ist es in dieser Krisensituation dennoch erforderlich, dass ich z. B. im Homeoffice mit meinem privaten PC, Notebook oder Smartphone arbeite, muss ich die nachfolgenden Richtlinien beachten:

- Ich trenne geschäftliche und private Daten in geeigneter Form (verschiedene Ordner usw.).
- Ich achte darauf, dass ich die Firewall aktiviert habe, meine Systeme und Anwendungen regelmäßig mit Sicherheitsupdates versorge, meine Antivirensoftware täglich aktualisiere und keine Software aus zweifelhaften Quellen installiere.
- Ich nutze, wenn möglich eine Zwei-Faktor-Authentisierung (2FA) und sichere Passwörter.
- Ich verschlüssele meinen PC, mein Notebook oder mein Smartphone.
- Ich richte für jeden Nutzer des Rechners einen eigenen Nutzer ein. So kann ich verhindern, dass andere Nutzer auf betriebliche Daten zugreifen.
- Ich arbeite nicht mit einem Administrator-Account.
- Ich bin besonders vorsichtig bei der Nutzung des Internets und E-Mail. Hier lauern die größten Gefahren, denn Links oder Dateianhänge können zu Schadsoftware führen.

Dokumentation. Welche besonderen Anforderungen gibt es für mich in der Krise?

Selbst in der Krise muss ich alle Dokumentationsanforderungen erfüllen, die ich auch vor der Krise einhalten musste. Demnach muss ich entweder geeignete organisatorische oder technische Maßnahmen ergreifen, um diese Anforderungen zu erfüllen. Wenn mir kein Drucker zur Verfügung steht, um Akten anzulegen oder Dokumente abzulegen, muss ich entsprechend strukturierte Verzeichnisse in den jeweiligen Speichersystemen erstellen und die Dokumente in elektronischer Form ablegen. Auch in meinem E-Mail-Postfach kann ich solche Ordner anlegen, um meine E-Mails strukturiert abzulegen.

Kann ich meinen Dokumentationspflichten nicht nachkommen, muss ich mich an meinen Vorgesetzten wenden und um eine Lösung bitten. Denn es ist besser meinen Vorgesetzten um Hilfe zu bitten, als wichtige Aufgaben nicht zu erfüllen. Ich zeige damit ja auch, dass mir diese Aufgaben wichtig sind.

Daten. Was muss ich beachten, wenn ich wieder im Unternehmen arbeite?

Im Homeoffice habe ich eventuell Daten auf dem betrieblichen oder privaten Endgerät gespeichert oder auch Akten verwahrt.

Sowohl die Geräte als auch die Daten und Akten müssen ins Unternehmen zurückgebracht werden. Ich achte beim Transport auf den Datenschutz und lasse keine Akten oder Systeme unbeobachtet im Zug oder Auto.

Löschen. Was muss ich konkret löschen und wie stelle ich das an?

Ich muss alle Daten löschen, die nicht mehr benötigt werden. Das betrifft alle privaten und betrieblichen Systeme, auf denen personenbezogene oder vertrauliche Informationen gespeichert wurden. Ebenso sind Akten zu vernichten, die nicht mehr benötigt werden oder bereits im Unternehmen gespeichert wurden.

Bei betrieblichen Notebooks oder Speichersystemen wird die IT-Abteilung die Daten löschen oder vernichten. Daher gebe ich die Geräte dort ab. Gleiches gilt für Akten. Diese sollte ich im Unternehmen ordnungsgemäß vernichten lassen (Shreddern, Papierentsorgung).

Bei privaten Endgeräten muss ich dafür sorgen, dass die betrieblichen Daten gelöscht werden. Auf dem PC lösche ich die entsprechenden Ordner und anschließend auch den Papierkorb. Ich denke daran, dass auch eventuelle Datensicherungen gelöscht werden. Das private Smartphone setze ich am besten auf den Auslieferungszustand zurück. Ich führe aber vorher eine Sicherung meiner privaten Daten durch.

Habe ich in Ausnahmefällen auch meinen privaten E-Mail-Account für die betriebliche Kommunikation genutzt, muss ich diese E-Mails ebenfalls löschen. Dies gilt nicht nur für mein lokales E-Mail-Postfach auf dem Rechner, sondern auch für die E-Mails bei meinem Provider (Webmail-Postfach). Denn personenbezogene Unternehmensdaten darf ich dort nicht speichern.

E-Mail, Teamlaufwerke. Was muss ich prüfen, wenn ich wieder im Büro bin?

Wenn ich wieder vom Homeoffice in mein Büro zurückkehre, muss ich prüfen, ob es eventuell wichtige unbearbeitete E-Mails in meinem Postfach gibt (falls diese nicht in das Homeoffice umgeleitet wurden). Ebenso muss ich prüfen, ob alle Dateien, die ich im Homeoffice bearbeitet habe, tatsächlich in den zentralen Teamlaufwerken vollständig enthalten sind. Eventuell wurden Dateien auf Cloud-Speichern verarbeitet und noch nicht in die zentralen Laufwerke überführt.

Ich prüfe, inwieweit meine E-Mails noch an Vertretungen umgeleitet werden und ob diese Umleitung tatsächlich noch erforderlich ist. Genauso prüfe ich, ob eventuell andere Mitarbeiter auf Dateien zugreifen können, obwohl dies nach der Krise nicht mehr erforderlich ist. Denn jeder darf nur auf die Daten zugreifen, die er benötigt.

Wieder im Büro. Wofür muss ich jetzt sorgen?

Wenn ich wieder im Büro bin, sollte ich zunächst prüfen, ob ein Kollege in der Zwischenzeit in meinem Büro gearbeitet hat. Dies ist oft der Fall, weil die Unternehmen Mitarbeiter auf Einzelbüros verteilen mussten. Ich schaue nach, ob derjenige sensible Informationen wie Passwörter usw. unter meiner Schreibtischunterlage oder an anderen Stellen abgelegt hat. Ich vernichte diesen Zettel und benachrichtige den Kollegen, falls ich weiß, wer es ist. Ich informiere auch die IT-Abteilung, damit der Account gesperrt wird. Denn wer weiß, wer dieses Passwort außer mir noch gefunden hat.

Ebenso sollte ich in meinem Schrank nachschauen, ob dort Akten meiner Kollegen stehen oder Post liegt, die diese noch nicht abgeholt haben. Sollte es sich um vertrauliche Informationen handeln, darf ich diese nicht einsehen. Ich lasse die Akten kurzfristig abholen. Ich prüfe, ob jemand auf meinem PC Daten lokal gespeichert hat, und unterrichte die IT-Abteilung.

Videokonferenzen. Wie soll ich mich konkret verhalten und worauf muss ich besonders achten?

Ich beachte bei der Nutzung von Videokonferenzsystemen die nachfolgenden Punkte:

- Videokonferenzsoftware darf ich nicht automatisch beim Hochfahren des Computers starten.
- Ich schalte beim Betreten eines Videokonferenzraums das Mikrofon automatisch stumm.
- Ich überprüfe vorab mein eigenes Videobild, ob es Objekte enthalt, die nicht gesehen werden sollten.
- Ich wähle meine Meeting-ID bzw. Meeting-URL möglichst kryptisch und keinesfalls sprechend (z. B. meinen Namen oder meine Telefonnummer), damit mich niemand erraten kann.
- Ich geben die Zugangsdaten zu dem Meeting nur an die geplanten Teilnehmer weiter.
- Ich beobachte als Veranstalter des Meetings die Teilnehmer. Ich reagiere sofort, wenn ein nicht eingeladener Teilnehmer erscheint.
- Ich halte die Videokonferenzsoftware (oder den Browser, mit dem ich an der Videokonferenz teilnehme) aktuell.
- Ich hole für die Aufzeichnung einer Videokonferenz die Zustimmung aller Teilnehmer ein.
- Wenn ich parallel zur Videokonferenz in der Software einen Chat-Kanal benutze, sollte ich mich nur so äußern, dass eine versehentliche Veröffentlichung des Chats keinen Schaden für mich oder mein Unternehmen anrichtet.
- Ich kläre vor der Einladung zu einem Meeting, ob die zu erwartenden Inhalte der Konferenz für das Medium geeignet sind. Insbesondere bei Gesprächen aus dem Personalbereich (z. B. Vorstellungsgespräche, Mitarbeitergespräche) muss ich klären, ob das zulässig ist. Ich frage in Zweifelsfällen unseren Datenschutzbeauftragten.
- Als Organisator einer Videokonferenz obliegt mir auch die Verantwortung für die ordnungsgemäße Durchführung der Videokonferenz. Ich muss jederzeit wissen, wer sich in der Videokonferenz aufhält und welche Daten/Informationen ausgetauscht werden.

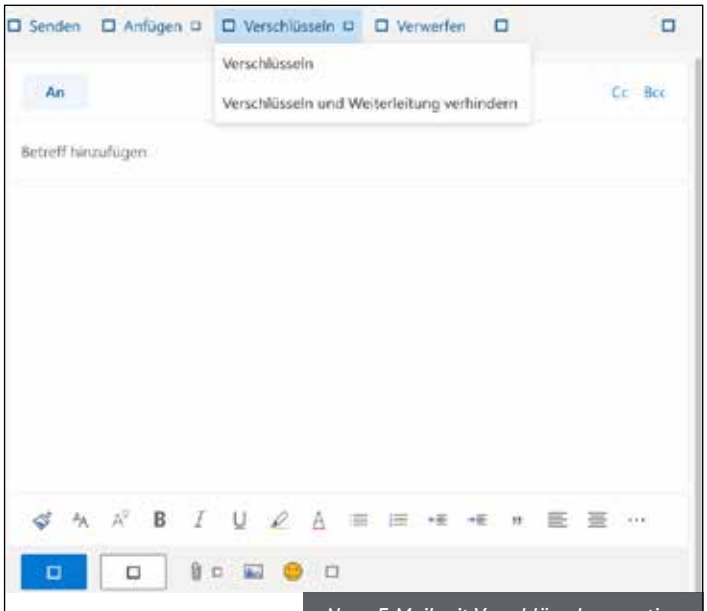
Datenschutz und Microsoft 365. Was muss ich konkret bei meiner Arbeit beachten?

Microsoft verfolgt seit einigen Jahren eine weitreichende Cloud-Strategie. Insbesondere das Produkt Office 365 hat Microsoft den Weg in viele Unternehmen geebnet, bietet Office 365 doch eine Vielzahl von Services, die weit über die bekannten MS-Office-Produkte wie Word oder Excel hinausgehen. Insbesondere Services wie Sharepoint, Teams, Exchange und Online-Varianten der bekannten MS-Office-Produkte schaffen für Firmenkunden einen enormen Mehrwert. Für mich als Nutzer gilt es jedoch, einige grundlegende Anforderungen zum Schutz der Daten zu beachten.

Outlook in Office 365. Was muss ich bei meiner täglichen Arbeit konkret beachten?

Outlook unterscheidet sich in der Online Variante kaum von der lokal installierten Office-Version. Allerdings bietet die Office-365-Variante ab der Lizenz E5 die Möglichkeit, E-Mails sicher zu verschlüsseln und das auch mit Partnern außerhalb des Unternehmens. Die Partner müssen noch nicht einmal Office 365 nutzen. Das ist ein enormer Mehrwert für den Datenschutz und die Datensicherheit. Wenn ich bei einer neuen E-Mail die Option „Verschlüsseln“ im Menüband auswählen kann, steht mir diese Funktion zur Verfügung.

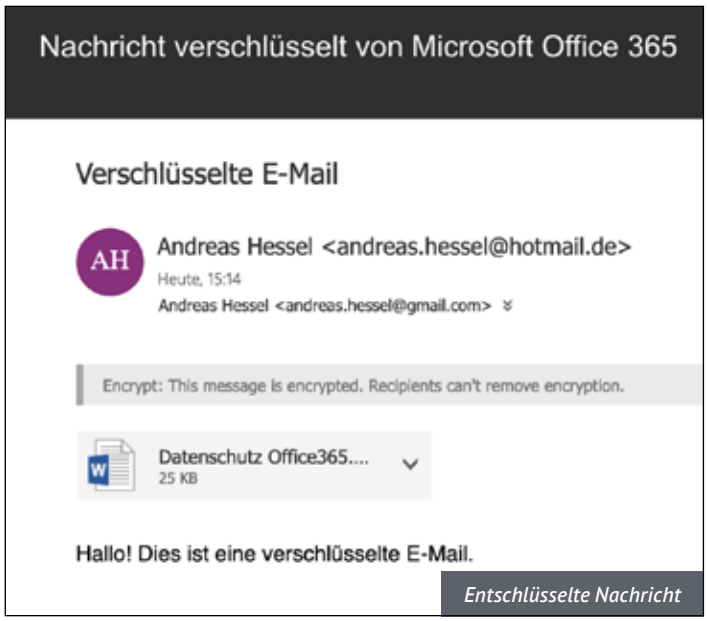
Wähle ich „Verschlüsseln“, wird die E-Mail inklusive Anhang sicher verschlüsselt. Der Empfänger erhält eine E-Mail mit einem Link auf die verschlüsselte E-Mail. Der Empfänger muss sich nun authentifizieren, entweder mit einem Google Account oder einem temporären Account. Wähle ich den temporären Account, erhält der Empfänger eine E-Mail mit einem Zifferncode, den er in das Anmeldefenster eingeben muss.



Neue E-Mail mit Verschlüsselungsoption

Eingabe des Codes

Dann steht ihm die Nachricht zur Verfügung.



Entschlüsselte Nachricht

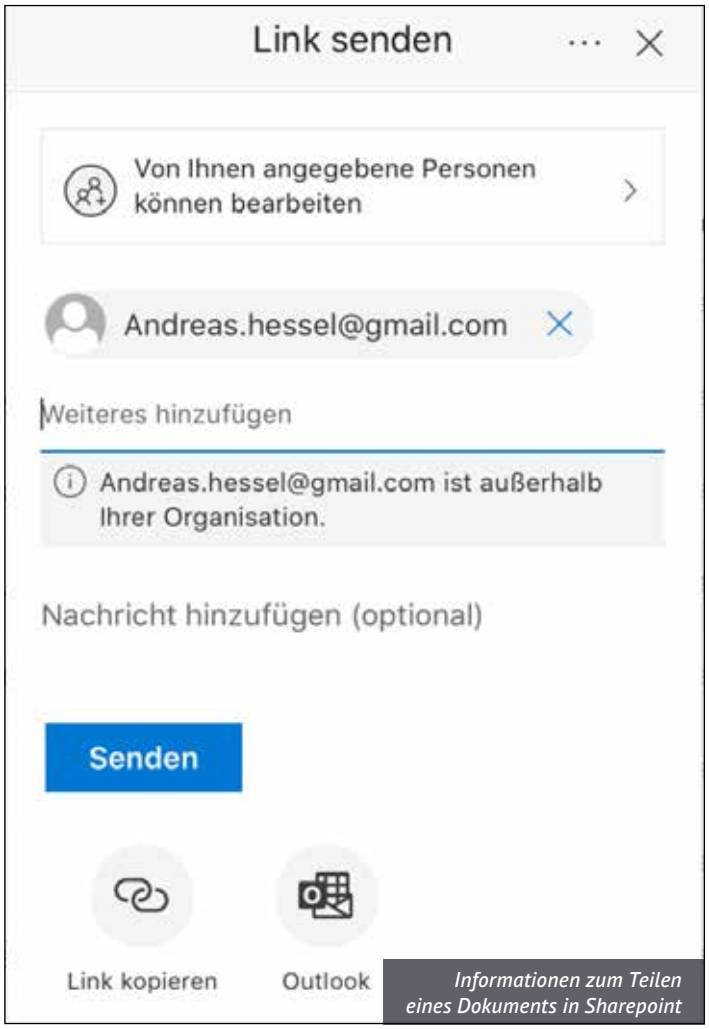
Dieses Verfahren ist sowohl für mich als auch den Empfänger einfach zu bedienen. So kann ich ebenso vertrauliche Informationen sicher übertragen.

Sharepoint und OneDrive: Was muss ich beim Teilen von Dateien beachten?

Das Teilen von Dateien in Sharepoint oder OneDrive ist ein sehr effektives Mittel, um anderen Personen schnell Informationen zur Verfügung zu stellen. Doch gilt es, einige Regeln zu beachten, denn sonst geraten die Informationen schnell in die falschen Hände oder stehen schlimmstenfalls für jedermann frei im Internet zur Verfügung. Wenn mir mein Administrator erlaubt hat, Daten auch außerhalb unseres Unternehmens zu teilen, sollte ich nachfolgende Regeln beachten.

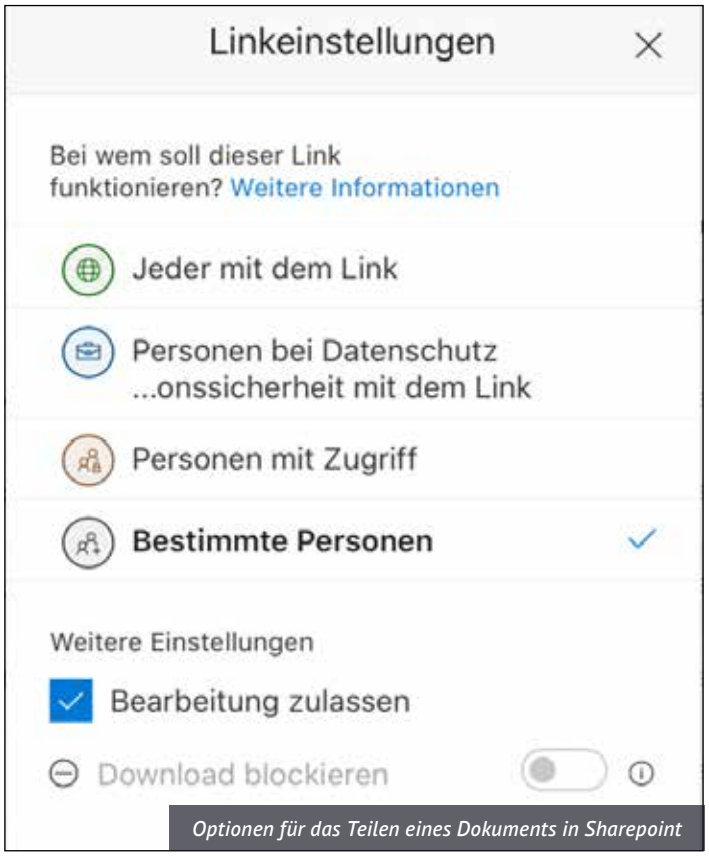
Denn gerade das Teilen von Inhalten mit Externen birgt erhebliche Risiken. Schnell habe ich eine E-Mail-Adresse verwechselt und die Daten einer falschen Person ausgehändigt. Oder ich habe zu schnell auf Teilen geklickt und die Daten stehen jedem zur Verfügung. Das kann schlimme Folgen haben.

Wenn ich eine Datei teilen möchten, bekomme ich zunächst das oben rechts abgebildete Fenster angezeigt:



Informationen zum Teilen eines Dokuments in Sharepoint

Ich prüfe zunächst die Option „Von Ihnen angegebenen Personen können bearbeiten“ im Detail. Hierzu klicke ich auf die entsprechende Schaltfläche.



Optionen für das Teilen eines Dokuments in Sharepoint

CHECKLISTE: Das muss ich konkret zu den Optionen wissen

Option	Auswirkung	Datenschutzempfehlung	Geprüft?
„Jeder mit dem Link“	Jeder, der den Link erhält, kann die Datei bearbeiten. Wird die E-Mail abgefangen oder an andere Personen weitergeleitet, habe ich keinerlei Kontrolle mehr.	nicht empfehlenswert	☐ Ja ☐ Nein
„Personen im Unternehmen“	Nur wer in unserem Unternehmen registriert ist, kann die Datei abrufen.	› empfehlenswert, wenn interne Informationen im Unternehmen verteilt werden sollen › nicht empfehlenswert im Unternehmen, wenn es sich um personenbezogene Daten handelt	☐ Ja ☐ Nein
„Personen mit Zugriff“	nur Personen, denen ich oder ein Administrator Zugriff auf die Datei gegeben habe/hat (z. B. Teams oder Abteilungen)	empfehlenswert	☐ Ja ☐ Nein
„Bestimmte Personen“	alle Personen, die ich per E-Mail-Adresse eingetragen habe	empfehlenswert, unkritisch, wenn der Personenkreis fest definiert wurde	☐ Ja ☐ Nein
„Bearbeitung zulassen“	Der Empfänger des Links kann die Datei herunterladen und damit in seinen Einflussbereich bringen. Ich habe keine Kontrolle mehr.	› empfehlenswert, wenn es sich um eine Datenübermittlung handelt › nicht empfehlenswert, wenn es sich nur um Informationen zu sensiblen Vorgängen handelt	☐ Ja ☐ Nein
„Download blockieren“	Der Empfänger kann die Datei nicht downloaden.	empfehlenswert bei sensiblen Daten, über die lediglich informiert werden soll	☐ Ja ☐ Nein

Habe ich die entsprechende Option ausgewählt, kann ich das Fenster mit der Schaltfläche „Übernehmen“ schließen und im folgenden Fenster entweder direkt mit der Schaltfläche „Senden“ den Link verschicken oder über die Schaltfläche „Link kopieren“ lediglich kopieren. Diesen Link kann ich ggf. in eine individuelle E-Mail an die entsprechenden Empfänger einfügen.

Mein Tipp
Beim Teilen von Dateien sollte ich mir immer Zeit nehmen und die oben stehende Tabelle durchgehen. Nur wenn ich alle Optionen geprüft habe, sollte ich die Informationen freigeben und den Link verschicken. Das Risiko, dass sensible Informationen über solche Freigaben in die falschen Hände geraten, ist hoch. Ich investiere also besser ein paar Minuten.

Wichtig: Über die Option „Zugriff verwalten“ kann ich in Sharepoint anzeigen lassen, welche Personen Zugriff auf die Datei und welche Personen über einen Link Zugriff erhalten haben. Über den Link „Nicht mehr teilen“ kann ich den Personen den Zugriff über diesen Link wieder entziehen. Das funktioniert auch mit Verzeichnissen.

Ich sollte regelmäßig prüfen, ob diese Zugriffsberechtigungen noch aktuell sind. Denn oftmals ändern sich Zuständigkeiten oder auch die Ansprechpartner in anderen Unternehmen.

Sonderfall Teams. Was muss ich hier beachten?

Ich kann auch in Microsoft Teams Dateien teilen. Hier wird immer ein Link erzeugt, den ich dann per E-Mail weiterleiten kann. Das funktioniert aber nur bei registrierten Mitgliedern der Teams. Demnach ist das Teilen nicht so kritisch wie in Sharepoint. Ich muss dennoch beachten, dass auch hier das Minimalprinzip gilt. Nicht jeder darf auf alle personenbezogenen Daten in gleichem Maße zugreifen. Also prüfe ich auch hier vor dem Teilen, ob wirklich alle Teammitglieder diese Informationen erhalten dürfen.

Ich beachte auch, dass die Datei beim Teilen bei Microsoft zwischengespeichert wird. Je nach Sensibilität des Inhalts muss ich diese Datei eventuell vor dem Teilen verschlüsseln.

Teams ist ein sehr mächtiges Tool, das vor allem die Zusammenarbeit verbessern kann. Allerdings bringt diese Freiheit in der Zusammenarbeit auch datenschutzrechtliche Risiken mit sich. Ich denke immer daran, dass jeder im Team uneingeschränkt auf alle Informationen in diesem Team zugreifen kann. Das gilt für Dateien, Chats, Wikis usw.

Zudem kann in der Regel jedes Teammitglied beliebige andere Personen innerhalb oder auch außerhalb unseres Unternehmens in das Team einladen. Da geht der Überblick oftmals allzu leicht verloren. Ich schaue also regelmäßig nach, wer alles in meinem Team ist und ob wirklich alle Mitglieder auf die jeweiligen Informationen zugreifen dürfen.

Fazit
Office 365 stellt eine Vielzahl von Services bereit, die insbesondere die Zusammenarbeit und den Datenaustausch erleichtern. Hier gilt es aber, immer im Auge zu behalten, dass der Zugriff auf personenbezogene Daten nach dem Minimalprinzip erfolgen muss. Ich prüfe immer, welche Rechte ich den Empfängern einräume und ob der Zugriff auf die Daten überhaupt erforderlich ist. Nicht jeder benötigt nämlich alle Daten. Dann bin ich auch mit Office 365 auf der sicheren Seite.

Diese Muster helfen Ihnen als Datenschutzbeauftragtem im Alltag

Mit den nachfolgenden Checklisten und Musterformularen haben Sie das nötige Rüstzeug, um in diesen Krisenzeiten gegen die meisten Herausforderungen gewappnet zu sein. Sie können tatsächlich mit der Erledigung der zentralen Aufgaben beginnen und die meisten Datenschutzrisiken, die sich in Zeiten von Covid-19 ergeben minimieren. Mit diesen Best-Practice Hilfsmitteln haben Sie alles Griff. Ich wünsche Ihnen viel Erfolg bei Ihrer Arbeit.

☑ ÜBERSICHT: Änderung an Prozessen und Richtlinien

Prozess	**Berechtigungsmanagement**
Betroffene Richtlinien	Berechtigungsmanagement, Grundlagen des IT-Berechtigungsmanagements
Betroffene Arbeitsanweisungen	User-Anlage / IT-Berechtigungen bearbeiten
Verantwortliche Fachbereiche:	IT
Betroffene Fachbereiche:	Alle
Freigeber:	Leiter Notfallstab
Datum Änderung:	23.03.2020
Datum Einsatz:	23.03.2020
Datum Ende der Änderung:	Bis auf weiteres
Anmerkungen	
Informationssicherheitsbeauftragter	abgestimmt
Datenschutzbeauftragter	abgestimmt
Interne Revision	abgestimmt
Leiter Notfallstab	genehmigt

Kurzbeschreibung:

- Berechtigungen werden per E-Mail beantragt und von den jeweiligen Führungskräften freigegeben.
- Die Änderung wird an den jeweiligen Administrator zur Umsetzung gegeben.
- Das Verfahren wird zentral dokumentiert.
- Solange für dieses Verfahren genügend Mitarbeiter vorhanden sind, wird ein etablierte 4-Augen-Prinzip umgesetzt. Ist dies nicht mehr gegeben, wird auf ein vereinfachte 2-Augen-Prinzip umgestellt. Es erfolgt eine Information an den Informationssicherheits- und Datenschutzbeauftragten.
- Für fachliche Administrationen in Anwendungen (z. B. Produkteinstellungen oder -veränderungen, Konditionenfreigabe oder bei sonstigen Anpassungen in Workflows) kann bis auf weiteres im Bedarfsfall vom 4-Augen-Prinzip abgewichen werden. Änderungen sind zu dokumentieren und im Nachgang zu prüfen.

Anmerkung:
Derzeitige 4-Augen-Prinzipien sind in den entsprechenden Fachbereichen dahingehend zu überprüfen, dass bei Ausfall eines Mitarbeiters noch die technische Möglichkeit besteht, ein 4-Augen-Prinzip zu deaktivieren. Hierzu erforderliche Benutzer sind kurzfristig nach dem beschriebenen Verfahren zu beantragen, freizugeben und einzurichten. Eventuell erforderliche Notfallkennwörter für diese User sind sicher zu verwahren. Hierbei ist ebenfalls auf eine Vertretungsregelung zu achten.

☑ CHECKLISTE: Sicherheitsrisiken Cloud-Dienste

Sicherheitsrisiko	Kurzbeschreibung	Maßnahme	Umgesetzt?
Datenverluste	Cloud-Provider sind gem. Art. 32 DSGVO zum Einhalten gängiger Sicherheitsstandards (ISO 27001 usw.) verpflichtet. Werden sie nicht eingehalten und es kommt zu Datenverlusten, drohen hohe Bußgelder und empfindliche Reputationsverluste. Allerdings sind nicht nur die Provider für den Schutz der Daten verantwortlich, sondern auch die Auftraggeber.	Multifaktor-Authentifizierung und Verschlüsselung	☐ Ja ☐ Nein
Unzureichendes Identitäts-, Zugangs- und Zugriffsmanagement	Datenverluste und Hackerangriffe werden begünstigt durch ein fehlendes oder mangelhaftes Identitätsmanagement-System.	Multifaktor-Authentifizierung, starke Passwörter, automatischer Austausch von Schlüsseln, Kennwörtern und Zertifikaten	☐ Ja ☐ Nein
Unsichere Bedienoberflächen und APIs	Schnittstellen sind besonders gefährdet, da sie zum einen die Verbindung zur Software von Drittanbietern herstellen und zum anderen meist übers Internet erreichbar sind.	Kontrolle des Codes (Code Review, Privacy by Design), kontinuierliche Überwachung.	☐ Ja ☐ Nein
Systemschwachstellen	Sicherheitslücken sind ein bekanntes Phänomen, in der Cloud werden ihre Auswirkungen potenziert.	regelmäßige Scans auf Schwachstellen, schnelle Reaktion auf bekanntgewordene Sicherheitslücken, unverzügliche Installation von Security-Patches und Updates	☐ Ja ☐ Nein
Account Hijacking	Der Diebstahl von Account-Daten birgt bei Cloud-Diensten zusätzliche Gefahren in sich, da die Angreifer die Aktivitäten und Transaktionen des rechtmäßigen Besitzers überwachen, Daten verändern, falsche Informationen verbreiten und ihn auf manipulierte Seiten führen können.	kontinuierliches Monitoring der Benutzeraktivitäten, das gilt auch für die Service-Accounts.	☐ Ja ☐ Nein
Kriminelle Insider	Sie können in einer Cloud-Umgebung besonders viel Schaden anrichten.	Cloud-Kunden müssen die Datenverschlüsselung unter eigener Kontrolle behalten und Zuständigkeiten auf mehrere Personen aufteilen	☐ Ja ☐ Nein
Advanced Persistent Threads	Angriffe, bei denen Unternehmen über längere Zeit hinweg ausgespäht werden, haben in den vergangenen Jahren zugenommen.	Cloud-Kunden müssen sich kontinuierlich über aktuelle Bedrohungen informieren und ihre Mitarbeiter entsprechend schulen.	☐ Ja ☐ Nein
Datenverluste	Daten können nicht nur durch Hackerattacken verlorengehen, sondern auch durch versehentliche Löschungen, Naturkatastrophen und Ähnliches.	Cloud-Kunden müssen sich über die Sicherheitsmaßnahmen ihres Providers informieren und bei besonders kritischen Daten eventuell das Vorhalten einer lokalen Kopie erwägen.	☐ Ja ☐ Nein
Nicht erfüllte Sorgfaltspflicht	Die mangelhafte Recherche der Kunden über die Rahmenbedingungen des Cloud-Computing und die mangelhaften vertraglichen Regelungen führen zu Datenschutzverstößen.	Explizite Sicherheitsanforderungen in Verträgen, Prüfungen, regelmäßige Pen Tests, Auswertung von Sicherheits- und Datenschutzberichten des Cloud-Providers.	☐ Ja ☐ Nein
Missbrauch von Cloud-Services	Aufgrund der hohen Rechenleistung und des nahezu unbegrenzten Speicherplatzes werden Cloud-Services regelmäßig auch für kriminelle Aktivitäten verwendet, wie etwa das Knacken von Passwörtern oder DDoS-Attacken.	Cloud-Provider benötigen Mechanismen, um solchen Missbrauch zu entdecken, sowie eine Möglichkeit, damit Kunden und andere Anwender entsprechendes Feedback liefern können.	☐ Ja ☐ Nein
DoS-Attacken	Denial-of-Service-Angriffe können ganze Cloud-Systeme abbremsen oder sogar komplett in die Knie zwingen.	Monitoring der Systeme sowie bereits vorbereitete und ständig erreichbare Abwehrmaßnahmen	☐ Ja ☐ Nein
Schwachstellen in geteilten Systemen	In der Cloud teilen sich mehrere Anwender die gleiche Infrastruktur, Plattform oder Applikation. Eine Schwachstelle kann daher das gesamte Cloud-Angebot eines Providers betreffen.	umfassende Sicherheitsstrategie, Multifaktor-Authentifizierung, host- und netzwerkbasierte Intrusion-Detection-Systeme (IDS), Security Incident and Event Management (SIEM), CERT	☐ Ja ☐ Nein

☑ CHECKLISTE: Home-Office Arbeitsplätze

Fragen	Sachverhalt	Erläuterungen	Eintritts-wahrsch.	Erfüllungs-grad
Nutzung der Home-Office Arbeitsplätze				
Werden an den Home-Office Arbeitsplätzen personenbezogene Daten erhoben, verarbeitet oder genutzt?	☐ Ja ☐ Nein			
Welche Datenverarbeitungsverfahren mit einer Verarbeitung oder Nutzung von personenbezogenen Daten werden an den Home-Office Arbeitsplätzen eingesetzt bzw. genutzt?				
Ausstattung der Home-Office Arbeitsplätze				
Wie sind die Home-Office Arbeitsplätze ausgestattet (Geräte und Einrichtungen)?	☐ PC ☐ Notebook ☐ Drucker/Multif. ☐ betr. Telefon ☐ Sonstiges			
Sind diese Geräte betriebssicher installiert und ist die Funktionsfähigkeit gewährleistet bzw. getestet?	☐ Ja ☐ Nein			
Handelt es sich bei diesen Geräten um betriebliche oder um private Geräte, ggf. welche Geräte sind Privateigentum des Beschäftigten?	☐ nur betr. Geräte ☐ zum Teil privat Ggf. welche?			
Ist eine Nutzung der betrieblichen Geräte für private Zwecke erlaubt?	☐ Ja ☐ Nein			
Werden auf den Geräten personenbezogene Daten auch gespeichert, ggf. welche und aus welchen Verfahren?	☐ Ja ☐ Nein			
Technische und organisatorische Maßnahmen				
Werden die personenbezogenen oder sonstige vertrauliche Daten sicher verschlüsselt, ggf. wie?	☐ Ja ☐ Nein Verschlüsselungs-verfahren?			
Sind die Arbeitsplätze gegen Zugang/Einsichtnahme durch unbefugte Personen geschützt, ggf. wie?	☐ gesonderter Raum ☐ absperrbar ☐ sonstiger Schutz, wie? ☐ Nein			
Ist eine Nutzung der Geräte durch Unbefugte, auch Familienangehörige, ausgeschlossen, ggf. für welche Geräte und auf welche Weise?	☐ Ja ☐ Nein			
Sind ausreichende technische und organisatorische Maßnahmen zum Datenschutz vorhanden, insbesondere zur Zugangs-, Zugriffs-, Eingabe- und Weitergabekontrolle (siehe Checklisten zu den technischen und organisatorischen Maßnahmen)?	☐ Ja ☐ Nein			
Entsprechen diese Maßnahmen dem Sicherheitsstandard des Unternehmens?	☐ Ja ☐ Nein			
Unterliegt die Protokollierung der Nutzung der Geräte des Telearbeitsplatzes dem allgemeinen Protokollierungsstandard des Unternehmens?	☐ Ja ☐ Nein			
Verfügen PC und/oder Notebook des Telearbeitsplatzes über Anschlüsse für externe Geräte/Datenträger oder Laufwerke, z. B. DVD-Brenner, USB-Geräte etc.?	☐ Ja ☐ Nein			
Sind diese Anschlüsse erforderlich, ggf. für welche Zwecke?	☐ Ja ☐ Nein			
Werden auf mobilen Datenträgern wie USB-Sticks oder Plattenlaufwerken personenbezogene Daten gespeichert, ggf. welche und für welche Zwecke?	☐ Ja ☐ Nein			
Handelt es sich bei den mobilen Datenträgern ausschließlich um betriebliche Datenträger oder ist auch die Nutzung von privaten Geräten zugelassen?	☐ nur betr. Geräte ☐ auch priv. Geräte ☐ nicht geregelt			

☑ CHECKLISTE: Home-Office Arbeitsplätze (Fortsetzung)

Fragen	Sachverhalt	Erläuterungen	Eintrittswahrsch.	Erfüllungsgrad
Sind Einrichtungen vorhanden, die eine zugangs- und zugriffsgeschützte Verwahrung von vertraulichen Unterlagen ermöglichen, ggf. welche?	☐ Ja ☐ Nein Welche?			
Ist ein sicherer bzw. zugriffsgeschützter Transport von vertraulichen/personenbezogenen Unterlagen eingerichtet, ggf. wie?	☐ Ja ☐ Nein Wie?			
Wie ist die sichere Vernichtung/Entsorgung von vertraulichen Unterlagen geregelt?				
Sind ein sicherer Zugang und Verbindung/Datenübertragung zu und von den betrieblichen Datenverarbeitungssystemen gewährleistet, ggf. wie?	☐ Ja ☐ Nein Wie?			
Gibt es Telearbeitsplatzrichtlinien (Wahrung des Datenschutzes, technische und organisatorische Maßnahmen, Betretungsrecht der Wohnung u. a.)?	☐ Ja ☐ Nein Aufgabenbereiche? ☐ entfällt			
Ist, soweit erforderlich, zur Wartung/Durchführung und Kontrolle von technischen und organisatorischen Maßnahmen oder Datenschutzkontrollen das Betretungsrecht der Wohnung geregelt?	☐ Ja ☐ Nein Wie?			

Erfüllungsgrad der Maßnahmen:

Anmerkungen:

Revisionshistorie

Laufende Nr.: _____

Datum	erfasst/geändert durch	Datum Prüfung durch DSB	Maßnahmen ausreichend?	Anmerkungen
			☐ Ja ☐ Nein	
	Unterschrift	Unterschrift		Termin nächste Überprüfung

☑ MUSTER: Datenschutzerklärung Home-Office

Herrn ……,

Datenschutzverpflichtung

Der Arbeitnehmer verpflichtet sich, die nachfolgenden Maßnahmen zum Schutz der ihm anvertrauten Informationen bei seiner Tätigkeit im Home-Office umzusetzen.

1. Der Arbeitnehmer stellt sicher, dass Dritte – auch Familienangehörige – am häusli-chen Arbeitsplatz keinen Zugang zu dienstlichen Informationen erhalten.
2. Alle Arbeitsmittel (Notebook usw.) und Unterlagen sind so zu verwahren, dass sie vor Diebstahl oder Missbrauch geschützt sind.
3. Der Büroraum muss beim Verlassen verschlossen werden.
4. Passwörter und Zugangskennungen sind vor Missbrauch zu schützen und verschlossen aufzubewahren.
5. Es ist untersagt Akten oder Dokumente im Original außerhalb des Unternehmens aufzubewahren.
6. Unterlagen sind im Home-Office in verschließbaren Schränken aufzubewahren.
7. Unterlagen und Datenträger sind vor der Entsorgung immer mit dem zur Verfügung gestellten Aktenvernichter datenschutzkonform zu vernichten.
8. Betriebliche Informationen und Unterlagen sind strikt von privaten zu trennen und dürfen z.B. nicht in den gleichen Schränken aufbewahrt werden.
9. Im Übrigen verpflichtet sich der Arbeitnehmer die internen Richtlinien zum Schutz der Vertraulichkeit von Informationen auch in seinem Home-Office zu beachten.
10. Der Datenschutzbeauftragte, die Fachkraft für Arbeitssicherheit, ein/e Vertreter/in des Personalrats und der IT-Sicherheitsbeauftragte erhalten das Recht, die Einhaltung der datenschutzrechtlichen Vorschriften sowie der arbeitssicherheitsrechtlichen Vor-schriften am häuslichen Arbeitsplatz zu kontrollieren. Mit dieser Kontrollbefugnis erklärt sich der Mitarbeiter ausdrücklich einverstanden.

……, den ……

Plötzlich im Homeoffice? – Datenschutz und die Informationssicherheit gelten auch im Homeoffice!

Im Zuge der Corona-Pandemie hat sich vieles im Alltagsleben sehr schnell verändert. Dazu gehört auch das Arbeiten von Zuhause (Homeoffice, Telearbeit). Üblicherweise ist die Einrichtung eines Heim-Arbeitsplatzes mit viel Vorbereitung verbunden, um zum Beispiel auch den Datenschutz am heimischen Arbeitsplatz in gleichem Maße wie im Büro zu gewährleis-ten.

Da Sie sehr spontan ins Homeoffice wechseln mussten, haben wir einige einfache Regeln und Hinweise für den Umgang mit personenbezogenen Daten, die Sie auch sofort umsetzen können.

Arbeitsplatz im Homeoffice einrichten

Achten Sie bei der Einrichtung ihres Arbeitsplatzes in den eigenen vier Wänden nicht nur darauf, dass Sie ungestört, angenehm und effektiv arbeiten können:

- Am besten ist ein Arbeitsplatz in einem eigenen Raum oder in einer eigenen Ecke. Wählen Sie den Platz so, dass andere nicht den Bildschirm sehen können – auch nicht durch ein Fenster. Eine Sichtschutzfolie für den Monitor kann dies unterstützen.
- Da Sie Ihren privaten Internet-Anschluss verwenden: Richten Sie Ihren Computer so ein, dass er mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden ist. Ihr WLAN sollte ohnehin so eingerichtet sein, dass man sich nur mit einem Passwort einwählen kann.
- Achten Sie auch darauf, dass Ihre Geräte nicht zugänglich sind, wenn Sie den Raum verlassen, z. B. abends nach getaner Arbeit.

Nachdem Sie dies alles beachtet haben, überlegen Sie noch einmal selber, wo Risiken lauern können.

Mit Vorgesetzten klären

Der Arbeitsplatz zu Hause bringt einige Fragestellungen mit sich, die mit den Vorgesetzten geklärt werden müssen. Bei spontan eingerichteten Homeoffice-Arbeitsplätzen ist mindes-tens Folgendes zu beachten:

- Dokumente, an denen Sie arbeiten, und Ihre Arbeitsergebnisse speichern Sie aus-schließlich im Netz der SaarLB. So kann auch die übliche Datensicherung (Backup) gewährleistet werden.
- Legen Sie gemeinsam fest, wie Sie untereinander und nach außen erreichbar sind und wie Sie Datenschutzrisiken vermeiden.
  - ☐ Sollen beispielsweise private Telefone verwendet werden, müssen Sie si-cherstellen, dass automatisch gespeicherte Anrufkontakte regelmäßig ge-löscht werden. Zumeist ist es sinnvoll, dass Ihre private Nummer bei Ihren Anrufen nicht übertragen wird, weil sonst Kundinnen und Kunden Ihre Privat-nummer des Handys oder Ihres Haushalts auch in späteren Kontakten nutzen könnten.
  - ☐ Für den Fall eines Datenverlusts (z. B. Verlust eines Notebooks) oder eines Datenschutzverstoßes (z. B. Zugang von Unbefugten an den Computer) be-steht eine Meldepflicht. Hier muss auch für das Arbeiten im Homeoffice klar sein, dass Sie dies unverzüglich melden müssen.

Beim Arbeiten im Homeoffice beachten

Bei der Arbeit im Homeoffice sollten Sie die gleichen Sicherheitsanforderungen wie an Ih-rem Arbeitsplatz im Büro berücksichtigen. Sie sollten sich an folgenden Maßnahmen orien-tieren:

- Organisieren Sie Ihren Arbeitsplatz so, dass sich private und dienstliche Daten nicht mischen.
- Wenn Sie Ihren Arbeitsplatz kurzfristig verlassen, aktivieren Sie den Bildschirmscho-ner mit Kennwortschutz, damit niemand unberechtigt auf Ihre dienstlichen Daten zugreifen kann.
- Achten Sie beim Verlassen des Arbeitsplatzes darauf, dass Türen und – vor allem im Erdgeschoss – Fenster verschlossen bzw. geschlossen sind, um eine unbefugte Kenntnisnahme, einen Verlust oder eine Veränderung von Daten zu verhindern.
- Wenn Sie am häuslichen Arbeitsplatz dienstlich telefonieren müssen, dann achten Sie da-rauf, dass Sie dafür einen ungestörten Bereich aufsuchen, damit andere Per-sonen im Haushalt keine Kenntnis von Ihrem Telefonat nehmen können.

Bei Fragen wenden Sie sich an Ihren Vorgesetzten.

Homeoffice-Richtlinie

Im Homeoffice sind zum Schutz der personenbezogenen Daten alle Richtlinien und Anweisungen einschließlich der Regelungen zum Datenschutz und zur IT-Sicherheit in ihrer jeweiligen aktuellen Fassung einzuhalten. Ergänzend zu diesen Richtlinien und zur IT-Sicherheitsrichtlinie gelten die nachstehenden Regelungen.

1. Geltungsbereich
Diese Richtlinie gilt für alle Standorte und Niederlassungen der <Firmenname> und für alle Beschäftigten, die personenbezogene Daten in einem Homeoffice verarbeiten.

2. Schutzmaßnahmen beim Transport von Geräten, Daten und Datenträgern
Geräte mit vertraulichen Daten, mobile Datenträger und vertrauliche Unterlagen, z. B. Akten u. a. dürfen nur in sicher verschließbaren Behältnissen und geschützt (z. B. nicht unbeobachtet auf dem Beifahrersitz oder dem Rücksitz des Pkw transportiert werden. Bei Verlassen des Pkw sind die Geräte, Datenträger und Unterlagen im Kofferraum einzusperren.
Für den Transport ist der unmittelbare und direkte Weg zwischen der betrieblichen Arbeitsstätte und dem Homeoffice zu wählen. Umwege und Unterbrechungen, z. B. für Besuche oder um Einkäufe zu erledigen, sind unzulässig.

3. Aufbewahrung von Geräten, Unterlagen und Datenträgern
Geräte, Datenträger und sonstige Unterlagen mit personenbezogenen oder sonstigen vertraulichen Daten dürfen nicht unbeaufsichtigt sein und sind während der arbeitsfreien Zeiten und bei Abwesenheit vom Homeoffice verschlossen zu verwahren.

4. Passwort
Aufgrund der besonderen Umstände eines Homeoffice ist ein sicheres und vertrauliches Passwort von besonderer Bedeutung. Es sind deshalb nur sichere Passwörter nach den Regelungen der IT-Sicherheitsrichtlinie zu verwenden und auch den Familienangehörigen gegenüber vertraulich zu behandeln.

5. Sichere Verbindung, WLAN
Die Verbindung zwischen den mobilen Geräten und den zentralen Verarbeitungssystemen darf nur über eine sichere Leitung hergestellt werden, z. B. über VPN. Unsichere WLANs vor Ort dürfen für eine Verbindung mit den zentralen Systemen und der lokalen Geräte untereinander ebenfalls nicht genutzt werden. Personenbezogene Daten sind bei jeder Form der elektronischen Übertragung, Übermittlung oder Versand nach den geltenden Sicherheitsrichtlinien zu verschlüsseln. Eine betriebliche Kommunikation über private E-Mail-Konten und ein Zugriff auf eine betriebliche Cloud mit privaten Geräten sind unzulässig.

6. Vertraulichkeit des Arbeitsplatzes
Der Mitarbeiter hat bei der Ausübung der Homeoffice-Tätigkeit darauf zu achten, dass die Vertraulichkeit der personenbezogenen Daten gewahrt bleibt und die Daten und Unterlagen vor einem Einblick durch Dritte, auch durch Familienangehörige, geschützt werden. Auf Bildschirmen sind Sichtschutzfolien zu verwenden.

7. Arbeitspausen und Verlassen des Homeoffice
Bei Pausen oder sonstigen kurzzeitigen Arbeitsunterbrechungen mit Abwesenheit vom Arbeitsplatz ist das Arbeitsmittel abzuschalten oder der Zugang zum Arbeitsmittel durch eine passwortgesicherte Pausenschaltung zu sperren. Bei Verlassen der Wohnung sind die Unterlagen und Arbeitsmittel mit personenbezogenen Daten, wie Akten, Notebook u. a. Datenträger, zugriffsgeschützt zu verwahren.

8. Vernichtung von vertraulichen Unterlagen
Ein Ausdruck von vertraulichen Daten im Homeoffice sollte soweit wie möglich vermieden werden. Sind Ausdrucke erforderlich, ist auf eine vertrauliche Umgebung am Drucker zu achten und die Ausdrucke sind vor einem Einblick und Zugriff durch Dritte, auch durch Familienangehörige, zu schützen. Die Ausdrucke sind geschützt, z. B. in einem abschließbaren Schrank, zu verwahren und bei nächster Gelegenheit zum betrieblichen Arbeitsplatz zu verbringen oder, sobald sie nicht mehr erforderlich sind, datenschutzgerecht mit einem Aktenvernichter mit mindestens Sicherheitsstufe P-3 nach DIN 66399-2 zu vernichten.

9. Speicherung von personenbezogenen Daten, Verschlüsselung
Nach Möglichkeit dürfen auf dem Notebook und auf sonstigen mobilen Datenträgern im Homeoffice keine personenbezogenen Daten gespeichert werden. Ist im Einzelfall eine Speicherung erforderlich, z. B. weil der Arbeitsablauf dies verlangt oder die Datenleitung zu den zentralen Verarbeitungssystemen nicht zur Verfügung steht, sind die Daten zu verschlüsseln und bei nächster Gelegenheit auf dem zentralen System zu sichern. Festplatten und mobile Datenträger, z. B. USB-Sticks, sind nach den betrieblichen Richtlinien zu verschlüsseln.

10. Private Nutzung
Die Privatnutzung der überlassenen Arbeitsmittel durch den Mitarbeiter sowie die Überlassung an andere Personen, auch an diejenigen, die im Haushalt des Mitarbeiters leben („Dritte"), ist untersagt. Ebenso ist die betriebliche Nutzung von privaten Arbeitsmitteln, z. B. von USB-Sticks, streng untersagt. Der Mitarbeiter wird durch geeignete Maßnahmen sicherstellen, dass Dritte keinen Zugriff auf die überlassenen Arbeitsmittel erhalten.

11. Firewall und Virenschutz
Um einen ständigen Schutz der Geräte zu gewährleisten, muss und darf nur die freigegebene und installierte Sicherheitssoftware installiert und betrieben werden. Die Einstellungen der Schutzsoftware dürfen nicht verändert oder die Schutzsoftware deaktiviert oder deinstalliert werden. Insbesondere dürfen die automatische Aktualisierung der Schutzsoftware nicht deaktiviert oder verändert und die Geräte nicht ohne aktuellen Schutz am Internet betrieben werden.

☑ MUSTER: Zusatzvereinbarung zum Arbeitsvertrag (Datenschutz und Datensicherheit)

Zusatzvereinbarung zum Arbeitsvertrag vom ..... über die Einrichtung eines Homeoffice-Arbeitsplatzes

zwischen
<Name Arbeitgeber>
und
<Name Mitarbeiter>

§ 1 Arbeitsort/häusliche Arbeitsstätte
Die Vertragsparteien vereinbaren eine <Telearbeit/alternierende Telearbeit oder mobile Telearbeit>. Der Mitarbeiter wird seine Arbeitsleistung ganz/zeitweise in seiner Wohnung („häusliche Arbeitsstätte“) und im vereinbarten Umfang am betrieblichen Arbeitsplatz erbringen. Soweit aus betrieblichen Gründen erforderlich, kann der Arbeitgeber die Anwesenheit im Unternehmen anordnen.

§ 2 Beschaffenheit des Homeoffice-Arbeitsplatzes
Der Mitarbeiter stimmt mit dem Arbeitgeber im erforderlichen Maße die Beschaffenheit des Homeoffice-Arbeitsplatzes, soweit diese datenschutz- oder sicherheitsrelevant ist, ab. ~~Er gewährt dazu dem Arbeitgeber oder einem Beauftragten des Arbeitgebers Zutritt zum Homeoffice-Arbeitsplatz und verpflichtet sich, nach erfolgter Einrichtung des Arbeitsplatzes diesen nicht in einem Sinne zu verändern, der zu einer Verschlechterung des Schutzes der personenbezogenen Daten führen kann. Veränderungen, die insoweit keine Auswirkungen nach sich ziehen, sind zulässig. Im Zweifel stimmt der Mitarbeiter Veränderungen des Homeoffice-Arbeitsplatzes mit dem Arbeitgeber ab.~~

§ 3 Arbeitsplatz
Die häusliche Arbeitsstätte befindet sich in <Wohnort oder abweichende Adresse>.

~~Der Mitarbeiter ist verpflichtet, jeden bevorstehenden Wohnungswechsel oder einen Wechsel des Homeoffice-Arbeitsplatzes vor der Aufnahme der Tätigkeit unverzüglich schriftlich mitzuteilen.~~

Der Mitarbeiter versichert, dass sich die häusliche Arbeitsstätte in einer abschließbaren Wohnung mit einer vertraulichen Umgebung befindet, die einen ausreichenden Schutz vor Einblick anderer Personen ermöglicht.

Alternativ: Der Mitarbeiter stellt einen abschließbaren Büroraum einschließlich Mobiliar zur Verfügung.

Der Mitarbeiter stellt sicher, dass der zur Verfügung gestellte Heimarbeitsplatz einschließlich der Büromöbel den jeweiligen Arbeitsschutzvorschriften entspricht.

§ 4 Arbeitsmittel
Für den Betrieb der häuslichen Arbeitsstätte stellt der Arbeitgeber folgende Arbeitsmittel kostenlos zur Verfügung:
<Beschreibung der Arbeitsmittel>

Der Mitarbeiter wird das Unternehmen unverzüglich über technische und sonstige Störungen sowie Mängel und Schäden an den überlassenen Arbeitsmitteln unterrichten. Bei einer Beschädigung oder einem Verlust von Arbeitsmitteln haftet der Beschäftigte nach arbeitsrechtlichen Grundsätzen.

§ 5 Zutrittsrecht zur Wohnung
Der Mitarbeiter verpflichtet sich, dem Arbeitgeber und Personen, die vom Arbeitgeber beauftragt werden, z. B. dem Arbeitsschutz- oder dem Datenschutzbeauftragten, sowie Personen oder Behörden, die aufgrund gesetzlicher Verpflichtungen Zugang zur häuslichen Arbeitsstätte haben müssen, nach vorheriger Abstimmung in zumutbarem Rahmen vor der Aufnahme und während der Tätigkeit in der häuslichen Arbeitsstätte Zugang zur häuslichen Arbeitsstätte zu gewähren. In dringenden Fällen ist der Zugang auch ohne vorherige Abstimmung zu gewähren.

Der Mitarbeiter bestätigt, dass die mit ihm in häuslicher Gemeinschaft lebenden Personen mit dieser Regelung einverstanden sind.

~~Alternativ: Der Mitarbeiter besorgt von den Mitbewohnern eine Einwilligung zum Betreten der Wohnung im o. g. Umfang.~~

§ 6 Schutz von Daten und Informationen, Datensicherheit
Die Verarbeitung von besonders sensiblen oder besonderen Datenarten i. S. v. Art. 9 Abs. 1 DSGVO ist mit dem Arbeitgeber abzustimmen.

Der Schutz von Daten und Informationen sowie die Datensicherheit richten sich nach den vorhandenen betrieblichen Regelungen in ihrer aktuellen Fassung sowie den einschlägigen gesetzlichen und unternehmensinternen Regelungen in der jeweils gültigen Fassung. Der Mitarbeiter ist verpflichtet, diese Regelungen entsprechend einzuhalten.

Der Mitarbeiter ist verpflichtet, geeignete Maßnahmen zu ergreifen, um die Einsicht und den Zugriff Dritter auf Daten und Informationen zu verhindern. Insbesondere dürfen Passwörter und Zugangswege zum Datennetz des Unternehmens nicht an Dritte weitergegeben werden. Näheres regelt die Homeoffice-Richtlinie.

§ 7 Datenschutzvorfälle
Datenschutzvorfälle, insbesondere Vertraulichkeitsverluste durch eine unbefugte Einsichtnahme oder Kenntnisnahme von personenbezogenen Daten durch Dritte, oder eine unbefugte Nutzung eines Arbeitsmittels sind umgehend zu melden. Der Mitarbeiter verpflichtet sich, vom Arbeitgeber zur Aufklärung des Vorfalles eventuell beauftragte externe Sachverständige im erforderlichen Umfang Zutritt zum Homeoffice zu gewähren.

§ 8 Mitgeltende Regelungen
Ergänzend zu dieser Vereinbarung findet der zwischen den Parteien bestehende Arbeitsvertrag, <soweit ein Betriebsrat eingerichtet ist, die anwendbaren Betriebsvereinbarungen> sowie alle Richtlinien und Anweisungen einschließlich der Regelungen zum Datenschutz und zur IT-Sicherheit in ihrer jeweiligen aktuellen Fassung entsprechend Anwendung.

☑ CHECKLISTE: Wahrung des Datenschutzes bei der mobilen Arbeit und Im Home-Office

Bereich	Maßnahme	Inhalt	Erledigt?
1. Organisation	Erstellung einer Sicherheitsrichtlinie bzw. Regelungen für die mobile IT-Nutzung, Telearbeit und Home-Office	› Kommunikationsarten (E-Mail, Internet, Fax, Mobiltelefon, Video- und Telefonkonferenzen) › Datenklassifizierung: Welche Daten dürfen wie das Unternehmen verlassen? › Sicherheitsanforderungen festlegen (z. B. Regelungen zu Datensicherung, Virenschutz, Firewall, Verschlüsselungsoption (in jedem Fall bei sensiblen Daten) › Wege der Datenübermittlung oder des Zugriffs: VPN, E-Mail, mobile Datenträger (USB), Ausdrucke › Passwortregeln, Token usw. › Absicherung privater WLANs › Nutzung von Cloud-Speichern › Nutzung privater Software › Nutzung privater Endgeräte (BYOD) › Nutzung privater Drucker › Vernichtung Papier und elektronische Datenträger › Umgang mit mobilen Datenträgern (USB-Schnittstellen) › Umgang mit Smartphones › Einsatz von Blickschutzfiltern › ggf. Regelungen zu Fernwartung › Clean Desk Policy mobiler Arbeitsplatz und Home-Office › Umgang mit Akten › Anforderungen an einen Home-Office Arbeitsplatz › Transport von sensiblen Informationen › Aushändigung der Richtlinie an betroffene Mitarbeiter	☐ Ja ☐ Nein
	Erstellung Betriebsvereinbarung zu Telearbeit und/ oder Home-Office	› Grundsätzliche Rechte und Pflichten des Mitarbeiters und des Arbeitgebers › Kontrollbefugnisse des Arbeitgebers vor Ort	☐ Ja ☐ Nein
	Erstellung Zusatzregelungen zum Arbeitsvertrag zum Home-Office	› Dauer des Einsatzes › Arbeitszeiten, Arbeitsplatz, Arbeitsmittel usw.	☐ Ja ☐ Nein
	Erstellung eines Sicherheitskonzepts für Tele- bzw. Home-Office	› Benennung von Sicherheitszielen › Bedrohungsanalyse (Datenverlust, Spionage, Missbrauch usw.) › Schutzbedarf der bearbeiteten Informationen und diesbezüglichen Risiken	☐ Ja ☐ Nein
2. Personalsicherheit	Einweisung und Schulung der Mitarbeiter	› Einweisung der Mitarbeiter in die mobile Arbeit › Mitarbeiterschulungen, Sensibilisierungen z. B. zum Umgang mit ausgedruckten Dokumenten	☐ Ja ☐ Nein
3. Asset Management	Dokumentation der Ausgabe und Rücknahme von unternehmenseigener IT (z. B. Laptop, Drucker) an und von dem jeweiligen Mitarbeiter Ggf. Vereinbarung eines Zutrittsrechts zu den privaten Räumen zur Durchführung von Kontrollen und Zugriff auf Dokumente (s. a. BV)		☐ Ja ☐ Nein
4. Zugriffskontrolle	Identifizierungs- und Authentisierungsmechanismus	2FA, Passwort, PIN, Token usw.	☐ Ja ☐ Nein
	Protokollierung	› Authentisierungen › Zugriffe › Veränderungen › Administratortätigkeiten › Fehler	☐ Ja ☐ Nein
	Sonderrechte	Vertretungsregelungen (Genehmigungsverfahren, Dokumentation)	☐ Ja ☐ Nein
	Administrationsrechte	› Regelungen und Kontrolle › Einschränkung der Benutzerumgebung für den Mitarbeiter	☐ Ja ☐ Nein

Übersatz von Seite 30

Die Regelungen dieser Richtlinien und die Betriebsvereinbarungen sind, soweit sie für die Verhältnisse eines Homeoffice zutreffen, einzuhalten. Zusätzlich gilt die Homeoffice-Richtlinie zum Datenschutz mit ihren speziellen Regelungen zum Datenschutz und zur Sicherheit der Verarbeitung.

……
Ort, Datum

…… ……
Unterschrift Arbeitgeber Unterschrift Mitarbeiter

☑ CHECKLISTE: Wahrung des Datenschutzes bei der mobilen Arbeit und Im Home-Office (Fortsetzung)

Bereich	Maßnahme	Inhalt	Erledigt?
5. Krypto-graphie	Verschlüsselung	› Mobile Endgeräte › Mobile Datenträger › E-Mails	☐ Ja ☐ Nein
6. Physische und Umgebungs-sicherheit	Arbeitsplatz-Sicherungs-maßnahmen	› Wer ist zutrittsberechtigt? › Welche Sicherungsmaßnahmen gibt es?	☐ Ja ☐ Nein
	Clean-Desk-Policy	Gedruckte Dokumente vor Einsicht Unbefugter schützen	☐ Ja ☐ Nein
	Arbeitsplatzrechner	Einstellung passwortgeschützter automatischer Bildschirmschoner	☐ Ja ☐ Nein
7. Betriebs-sicherheit	Updates	Installiert und aktuell	☐ Ja ☐ Nein
	Virenschutz	Installiert und aktuell	☐ Ja ☐ Nein
	Firewall	Aktiviert	☐ Ja ☐ Nein
	Bootschutz	Aktivierung empfehlenswert	☐ Ja ☐ Nein
	Datensicherung	Regelungen und Kontrolle	☐ Ja ☐ Nein
8. Kommuni-kations-sicherheit	Trennung von Daten	Trennung privater Daten von unternehmenseigenen Daten	☐ Ja ☐ Nein
9. Compliance	Beauftragung von Freien Mitarbeitern	Ggf. Abschluss eines AV Vertrags, Verschwiegenheitserklärung usw.	☐ Ja ☐ Nein
10. Dokumen-tation	Technische und organisa-torische Maßnahmen	› Änderung von Prozessen › Außer Kraft Setzung von Richtlinien › Kompetenzregelungen (Notfallstab usw.) › Maßnahmen, die nicht durchgeführt werden konnten (Schulungen, Prüfungen, Verträge usw.)	☐ Ja ☐ Nein

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de

Ein Unternehmensbereich des
VNR Verlag für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn