Geschäftsstelle Dresden:
Königsbrücker Landstraße 40
01109 Dresden
Tel: 0351 8881251

Niederlassung Böblingen:
Otto-Lilienthal-Straße 36
71034 Böblingen
Tel: 07031 7145660

mail@sodalitas-gmbh.de
www.sodalitas-gmbh.de
Fax: 0351 8881252

IT-Ticker 02/2020

Der IT-Ticker 02/2020 informiert Sie über folgende Themen:

Chancen nutzen und jetzt Videokonferenzen auch für die Zukunft etablieren!

Die Corona-Krise hat einen regelrechten Boom der Digitalisierung ausgelöst und viele Unternehmen setzen heute Videokonferenzen in einem Umfang ein, den sie noch Anfang des Jahres für unmöglich hielten. Nach den häufig im ad-hoc-Verfahren beschlossenen Einführungen der Tools, müssen nun die Weichen für die Zukunft gestellt werden und die gesetzlichen Anforderungen umgesetzt werden (z.B. im Datenschutz, hinsichtlich der Lizenzen oder bezogen auf interne Nutzungsvorgaben).

An die Stelle von Dienstreisen und Telefonkonferenzen sind in vielen Unternehmen Videokonferenzen getreten, bekannte Anbieter sind Microsoft Teams, Zoom, Skype for Business und WebEx (um nur einige der zahlreichen Anbieter zu nennen). Mitarbeiter können aus dem Home-Office teilnehmen und verlieren nicht den Kontakt zu einander oder zum Kunden. Bei der Nutzung von Online- und Videokonferenzen müssen jedoch, trotz Krisenzeiten, die Vorgaben der DS-GVO eingehalten werden, sofern diese im geschäftlichen Umfeld zum Einsatz kommen. Folgende Stellungnahmen von deutschen Aufsichtsbehörden im Zusammenhang mit Videokonferenzen sind besonders hilfreich: Baden-Württemberg, Hamburg, Rheinland-Pfalz und Niedersachsen. Berlin hat ebenfalls eine Stellungnahme veröffentlicht, in der einzelne Anbieter wie Microsoft und Zoom kritisiert werden. Microsoft hat daraufhin eine eigene Stellungnahme veröffentlich und sucht aktuell das Gespräch mit der Behörde.

Nachfolgend finden Sie eine Checkliste zu den relevanten Fragen beim Einsatz von Online- und Videokonferenzen, welche vor dem Einsatz des Systems sichergestellt werden müssen.

1. Auswahl des Dienstleisters

- Welche Leistungen muss der Dienstleister ermöglichen? Z.B. reine Videokonferenz, Teilen von Dokumenten (von einer Person oder von mehreren Teilnehmern), etc.
- Darf der Dienst zu geschäftlichen Zwecken genutzt werden? Zum Teil ist die geschäftliche Nutzung nur gegen Bezahlung möglich
- Wo stehen die Server des Dienstleisters? EU-Anbieter sollten Anbietern aus dem Drittland vorgezogen werden, da diese sich im Anwendungsbereich der DS-GVO befinden

- Soll das Tool/die Software nur zur Zeit der Corona-Pandemie genutzt werden oder ist ein Dauerbetrieb geplant?

Für den Fall des Dauerbetriebs sollten nur Tools/Software in den Auswahlprozess einbezogen werden, die die erforderlichen technischen Maßnahmen zur Gewährleistung der Datensicherheit erfüllen

2. Erste Schritte zur Einführung eines Tools/Software für Videokonferenzen

- Zustimmung des Betriebs- oder Personalrats einholen (ggf. Abschluss einer Betriebsvereinbarung)
- Einschaltung des Datenschutzbeauftragten
- Prüfung, ob Datenschutz-Folgenabschätzung erforderlich ist und Dokumentation dieser Vorabprüfung

3. Prüfung Datenschutzniveau bei Anbietern aus Drittländern

Sofern der ausgewählte Anbieter nicht aus der EU kommt, muss sichergestellt werden, dass ausreichende Garantien für ein angemessenes Datenschutzniveau gewährt werden.

- Vorliegen einer Angemessenheitsentscheidung der EU-Kommission
- Privacy-Shield-Zertifizierung im Falle eines US-Anbieters
- Abschluss von Standarddatenschutzklauseln
- Ausnahmetatbestände für bestimmte Fälle nach Art. 9 DS-GVO

4. Notwendige Dokumente zum Einsatz von Videokonferenzen

- Abschluss Vertrag zur Auftragsverarbeitung inklusive TOMs, sofern weisungsgebundene Auftragsverarbeitung vorliegt: Dieser wird von vielen Anbietern zur Verfügung gestellt, muss aber geprüft werden, insbesondere, ob die technischen und organisatorischen Maßnahmen und Subunternehmer passend sind
- Datenschutzhinweise nach Art. 13/14 DS-GVO für die Teilnehmer der Videokonferenz (eigene Mitarbeiter und externe Teilnehmer)
- Aufnahme des Tools/der Software in das Verarbeitungsverzeichnis

5. Prüfung der datenschutzfreundlichen Voreinstellungen

- Bietet der Dienstleister ausreichende datenschutzfreundliche Voreinstellungen (unterschiedlich je nach Nutzung der Plattform) und sind diese eingestellt? Z.B. Ende-zu-Ende-Verschlüsselung von Übertragungen, d. h. Anbieter darf keine Kenntnis von Inhalten der Kommunikation nehmen (nur Megadaten); Einholung von Zustimmungen bei Aufzeichnungen und Freigaben; Löschung von Aufzeichnungen
- Ausschalten von Tracking-Funktionen, sofern diese nicht erforderlich sind
- Wenn möglich sollten keine besonderen Kategorien von Daten besprochen und aufgezeichnet werden
- Strenge Zweckbindung, d. h. keine Nutzung der erhobenen Daten zu anderen Zwecken als zur Ermöglichung der Kommunikation

Praxistipp

Die Nutzung von Videokonferenzen ist datenschutzrechtlich kein Hexenwerk und bietet eine gute Alternative zu Anwesenheits-Meetings. Einmal aufgesetzt können sämtliche Mitarbeiter diese Möglichkeit nutzen und weiterhin Kontakt zu Kunden halten.

Wird jetzt – trotz Krisenzeiten – auf die Einhaltung von datenschutzrechtlichen Vorgaben geachtet, kann dieses System auch nach Corona weiterhin genutzt werden und einige Abstimmungen auch zukünftig effizienter und kostengünstiger ermöglichen. Insofern sollte die Einhaltung der datenschutzrechtlichen Vorgaben derzeit nicht nur als Last gesehen werden, sondern vielmehr als Chance.

Wir haben bereits viele Mandanten bei der Auswahl von Tools und Software unterstützt und insbesondere im Bereich Datenschutz, Sicherheit und Lizenzen umfangreiche Erfahrungen mit vielen Anbietern gesammelt.

Nachfolgend finden Sie noch eine Übersicht von Tools. Diese ist weder vollständig noch als Empfehlung für ein bestimmtes Tool zu verstehen. Vor dem Einsatz eines bestimmten Tools muss

eine rechtliche Prüfung im Einzelfall erfolgen. Viele Anbieter aus den USA oder mit Muttergesellschaften in den USA bieten inzwischen an, dass die Leistungen aus EU-Rechenzentren erbracht werden können. Mitunter werden dann aber Wartungsleistungen aus den USA oder anderen Drittstaaten erbracht:

Name	Land	Wird der Abschluss eines Vertrags zur Auftragsverarbeitung angeboten	Privacy-Shield-Zertifizierung oder Standarddatenschutzklauseln, wenn außerhalb der EU ansässig
Arkadin	Deutschland	Auf Anfrage	
BlueJeans	USA	Nein	Ja
ClickMeeting	Polen	Ja	
Discord	USA	Nein	Ja
Fastviewer	Deutschland	Ja	
GoToMeeting	USA	Ja	Ja
Hangouts/Meet von Google	USA	Ja	Ja
Intercall Unified Meeting	USA	Ja	Ja
meetgreen	Deutschland	Auf Anfrage	
meetyo	Deutschland	Auf Anfrage	
Skype for Business	EU/USA	Ja	Ja
Slack	USA	Ja	Ja
TeamViewer	Deutschland	Auf Anfrage	
Teams von Microsoft	EU/USA	Ja	Ja
Twitch	USA	Nein	Nein
WebEx von Cisco	USA	Ja	Ja
Zoom	EU/USA	Ja	Ja

Rechtlicher Hinweis:

Keine Empfehlung. Welcher Anbieter für Ihr Unternehmen der richtige ist, finden wir am besten in einem persönlichen Gespräch heraus.

Fazit

Die Nutzung von Videokonferenzen ist datenschutzrechtlich kein Hexenwerk und bietet eine gute Alternative zu Anwesenheits-Meetings. Einmal aufgesetzt können sämtliche Mitarbeiter diese Möglichkeit nutzen und weiterhin Kontakt zu Kunden halten.
Auch juristisch einwandfreie Vertragsabschlüsse sind dank digitaler Signaturen kein Problem.
Achten Sie jetzt auf die Einhaltung von datenschutzrechtlichen Vorgaben, können Sie Ihr Videokonferenz-System auch nach Corona weiterhin nutzen. So nutzen Sie die nun gewonnenen Learnings, um in vielen Bereichen auch zukünftig effizienter und kostengünstiger zu arbeiten.
Insofern sollte die Einhaltung der datenschutzrechtlichen Vorgaben derzeit nicht nur als Last gesehen werden, sondern vielmehr als Chance.

Wir unterstützen Sie bei der Implementierung von Videokonferenzen

Allgemeine Bausteine

- Checkliste zu allen rechtlichen Fragen, die vor dem Einsatz eines Videokonferenzsystems in Ihrem Unternehmen geprüft werden müssen
- Konkrete Software-Empfehlung auf Basis eines umfassenden Produktvergleichs
- Durchführung praxisnaher Schulungen
- Bereitstellung von Schulungsunterlagen und Service Cards für interne Schulungen

Datenschutz und Datensicherheit

- Konkrete Bewertung der marktüblichen Videokonferenzsysteme bezüglich allgemein gültiger Datenschutz- und Datensicherheitsanforderungen unter Berücksichtigung der aktuellen Regelungen der deutschen Datenschutzaufsichtsbehörden
- Beurteilung der datenschutzfreundlichen Voreinstellungen im Videokonferenzsystem
- Vollständige Prüfberichte der Auftragsverarbeitungsverträge (AVV) der wichtigsten Videokonferenzanbieter
- Erstellung von direkt einsetzbaren Datenschutzhinweisen/Datenschutzerklärungen für Mitarbeiter und externe Teilnehmer in deutscher und englischer Sprache

Arbeitsrecht

- Individuell abgestimmte Betriebsvereinbarungen, Richtlinien und Arbeitsanweisungen
- Rechtliche Beratung zu Betriebsratsbeschlüssen per Videokonferenz
- Sicherstellung der Arbeitsfähigkeit von Betriebsräten mit Blick auf COVID-19

Lizenzrecht

- Unterstützung bei der Einbindung in die Lizenz- und IT Landschaft Ihres Unternehmens
- Rechtliche Absicherung von Geschäftsgeheimnissen und Know-how gegenüber Anbietern
- Antworten auf IT rechtliche Fragen und lizenzvertragliche Stolpersteine bei der Einbindung in den Unternehmensalltag

Die einzelnen Bausteine bieten wir wahlweise planbar zu voraus vereinbarten Festpreisen oder individuell nach Aufwand an.

Kostentransparenz ist für uns in jedem Fall selbstverständlich.

Sprechen Sie uns an, wir helfen Ihnen gerne weiter.

Weitere interessante Links zum Thema

Folgende Stellungnahmen von deutschen Aufsichtsbehörden im Zusammenhang mit Videokonferenzen sind besonders hilfreich:

Datenschutzfreundliche technische Möglichkeiten der Kommunikation. Informationen des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg:

https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

Datenschutz in Zeiten von Covid-19. Informationen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit:

https://datenschutz-hamburg.de/assets/pdf/Corona-FAQ.pdf

FAQs zu verschiedenen Datenschutz-Fragen im Zusammenhang mit der Corona-Pandemie. Bereitgestellt vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

https://www.datenschutz.rlp.de/de/themenfelder-themen/corona-datenschutz/

Franziska Ladiges, Frankfurt/Main, f.ladiges@skwschwarz.de
Dr. Oliver Hornung, Frankfurt/Main, o.hornung@skwschwarz.de
Nikolaus Bertermann, Berlin, n.bertermann@skwschwarz.de

Homeoffice rechtskonform gestalten: So beachten Sie Datenschutz, Datensicherheit und Arbeitsrecht.

Viele berufstätige Menschen, Arbeitnehmer ebenso wie Selbstständige, hat es im Angesicht der Corona-Pandemie unversehens ins Homeoffice verschlagen. Dabei dürfen Datenschutz und Datensicherheit nicht auf der Strecke bleiben. Wer bisher schon das Arbeiten im Homeoffice zuließ, kann seinen Beschäftigten nun eher Leitlinien an die Hand geben als Unternehmen, bei denen das bislang nicht der Fall war. Was Sie in Sachen Datenschutz unbedingt beachten sollten, und wie Sie die Arbeitsplätze Ihrer Mitarbeiter zuhause rechtskonform gestalten, erfahren Sie hier.

Auf diese Datenschutz-Aspekte sollten Sie als Arbeitgeber achten
Damit die Arbeit im Homeoffice erfolgreich erledigt werden kann, sollten Sie einige datenschutzrechtliche Aspekte beachten und Ihre Angestellten entsprechend ausstatten.

Prüfen Sie Ihre Kundenverträge
Werden Daten für einen Dritten im Auftrag verarbeitet, ist der zugrunde liegende Vertrag über Auftragsverarbeitung zu prüfen, denn nicht jeder lässt die Tätigkeit im Homeoffice zu. Manche Verträge enthalten zumindest Einschränkungen oder fordern bestimmte Sicherheitsvorkehrungen. Nur wenn die Tätigkeit im Homeoffice nicht explizit ausgeschlossen ist und etwaige zusätzliche Sicherheitsvorkehrungen erfüllt werden können, ist die Datenverarbeitung im Auftrag des Kunden durch Mitarbeiter im Homeoffice zulässig. Das betrifft natürlich nur die Fälle, in denen der Arbeitnehmer für den Auftragnehmer tätig ist.

Schützen Sie personenbezogene Daten
Das Datenschutzrecht schützt nur die Verarbeitung von Daten sogenannter natürlicher Personen. Das heißt, Daten, die Informationen über Unternehmen enthalten, wie es insbesondere im B2B-Bereich der Fall ist, sind nicht von datenschutzrechtlichen Pflichten umfasst. Einschränkend gilt jedoch, dass infolge des weiten Anwendungsbereiches auch im B2B-Bereich die Verarbeitung personenbezogener Daten zum Alltag gehört. Bereits die Information, ob eine Person bei einem bestimmten Unternehmen angestellt ist, stellt eine personenbezogene Information dar, auch wenn sie nicht besonders sensitiver Natur ist.
In den meisten Fällen lässt es sich also gar nicht vermeiden, dass zumindest einige personenbezogene Daten genutzt oder verarbeitet werden. Auch vertrauliche Daten ohne Personenbezug, wie z.B. Geschäftsgeheimnisse, müssen im Unternehmen durch ausreichende technische Vorkehrungen geschützt werden. Was als ausreichend anzusehen ist, bestimmt Art. 32 DSGVO, der je nach Art und Umstände der Datenverarbeitung unterschiedliche Pflichten auferlegt. Die datenschutzrechtlichen Pflichten sind nicht einschlägig, wenn nur Daten ohne Personenbezug verarbeitet werden.

Vermischen Sie keine privaten und dienstlichen Daten
Im Homeoffice werden die Daten zwar zumindest teilweise an einem anderen Ort und mit anderen Mitteln verarbeitet als im Büro. Trotzdem ist der Arbeitgeber der Verantwortliche im Sinne des Datenschutzrechts. Deshalb ist es wichtig, dass private und dienstliche Daten nicht vermischt werden. Der Arbeitgeber bleibt auch für die im Homeoffice verarbeiteten Daten verantwortlich und legt auch dort die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten fest. Das gehört zu seinem Weisungsrecht.

Nutzen Sie keine privaten Geräte
Nur wenn die Mitarbeiter für das Homeoffice mit betrieblichen Computern ausgestattet sind, ist ein effektiver Schutz der personenbezogenen Daten möglich. Dadurch ist gewährleistet, dass die betrieblichen Sicherheitsvorkehrungen wie z.B. Betriebssystem, Virenschutz und Firewall tatsächlich aktiv und auf dem aktuellsten Stand sind. Eine Privatnutzung dieser Geräte sollte untersagt werden, weil ansonsten der Zugriff auf gespeicherte Daten durch das Unternehmen erschwert werden kann.

Nutzen Sie professionelle Verschlüsselung
Um eine hinreichende IT-Sicherheit im Homeoffice zu gewährleisten, sollte der Arbeitgeber auf den Speichermedien in den IT-Geräten und auf externen Speichermedien eine hinreichende Verschlüsselung implementieren. Gehen die Speichermedien verloren oder werden sie gestohlen, sind die Daten so trotzdem vor unberechtigtem Zugriff gesichert. Auf Nummer sicher gehen Sie jedoch, wenn Dateien mit personenbezogenen Daten auf den Servern des Unternehmens gespeichert

werden und nicht auf dem Endgerät im Homeoffice. Auch sollten Sie für eine sichere VPN-Verbindung zu Ihren Unternehmens-Servern sorgen.

Arbeitsrecht im Homeoffice

Erstellen Sie eine Homeoffice Richtlinie
Empfehlenswert für ein Unternehmen ist es, alle Vorgaben im Zusammenhang mit der Arbeit zu Hause (Telearbeit) in einer Homeoffice Richtlinie festzulegen. Dort können dann auch alle Vorkehrungen zur Sicherheit beschrieben werden. Auch sollten ein Ansprechpartner für alle Fälle von Datenschutzverletzung oder Phishing festgelegt werden, an den sich die Mitarbeiter wenden können.

Muss der Arbeitsvertrag für die Arbeit im Homeoffice angepasst werden?
Nein. Der Arbeitsvertrag muss nicht angepasst werden. Es reicht eine Zusatzvereinbarung, in der der sogenannte Leistungsort abweichend vom Arbeitsvertrag geregelt wird. Ferner können weitere Pflichten relevant sein, die sich auf die Einhaltung der Schutzmaßnahmen bei der Verarbeitung personenbezogener Daten durch den Arbeitnehmer beziehen. Vorbehaltlich zwingender datenschutzrechtlicher Regeln, ist es die Entscheidung des Arbeitgebers und des Arbeitnehmers, wie weitreichend diese Anpassungen ausfallen. Geregelt werden sollte insbesondere, wie weit die Entscheidungsbefugnis des Arbeitnehmers für die Arbeit im Homeoffice ausfällt.

Gibt es ein Recht auf Homeoffice?
Falls der Arbeitnehmer individualvertragliche Vereinbarungen getroffen hat oder entsprechende Betriebsvereinbarungen bestehen, ist ihm dieses grundsätzlich zuzustehen und er hat ein Recht auf Arbeit im Homeoffice. Soweit dieses nicht der Fall ist, hängt es von der individuellen Situation des Arbeitnehmers und des Arbeitsortes ab.
Zwar hat der Arbeitgeber das Weisungsrecht gegenüber seinen Angestellten, allerdings darf er dieses nicht in einer Weise ausüben, die die rechtlich geschützten Interessen dieser verletzt. Insbesondere ist der Arbeitgeber auch zum Schutz der Gesundheit seiner Angestellten verpflichtet.
Ein „Recht auf Homeoffice“ wird mithin nur dann anzunehmen sein, wenn der Arbeitsort entweder in einer besonders belasteten Region liegt oder der Arbeitnehmer zu einer besonderen Risikogruppe gehört. Soweit die Arbeit problemlos auch von zu Hause aus ausgeführt werden kann, reduziert dieses das Ermessen des Arbeitgebers. Entsprechendes wird anzunehmen sein, wenn der jeweilige Arbeitnehmer auf die Inanspruchnahme öffentlicher Verkehrsmittel angewiesen ist.
Das Bundesministerium für Arbeit und Soziales plant derzeitig einen Gesetzesentwurf „Recht auf Homeoffice“, nach dem einen Rechtsanspruch auf Homeoffice erhalten soll, wenn keine betrieblichen Gründe dagegen sprechen. Inwieweit dieses tatsächlich umgesetzt wird, ist derzeitig jedoch noch nicht absehbar, zumal hierfür eine Reihe von Änderungen von Vorschriften zu Arbeitsschutz und Datenschutz vonnöten wären.

Kann der Arbeitgeber Homeoffice anordnen?
Grundsätzlich reicht das Direktionsrecht des Arbeitnehmers nicht in die Privaträume seiner Angestellten hinein, sodass Homeoffice nicht ohne weiteres angeordnet werden kann. Allerdings sind auch von diesem Grundsatz Ausnahmen anzuerkennen.
Insbesondere dann, wenn es zum Schutz der Belegschaft erforderlich ist, dass der Betroffene nicht mehr in den Betriebsräumen erscheint, etwa weil dieser sich in einem Covid-19-Risikogebiet aufgehalten hat. In diesem Fall ist ein entsprechendes Weisungsrecht anzuerkennen.
Als Grundbedingung muss jedoch gelten, dass der Arbeitnehmer gesund und arbeitsfähig ist und vom Arbeitgeber die erforderlichen Arbeitsmittel zur Heimarbeit zur Verfügung gestellt bekommt. Allein die abstrakte Gefahr einer Infektion begründet das Recht zum Homeoffice jedenfalls nicht.

Unterschied Homeoffice, Telearbeit, flexibler oder mobiler Arbeitsplatz?
Die Begriffe haben keine festgeschriebene rechtliche Bedeutung und bezeichnen für das Arbeitsrecht insbesondere die Frage, von welchem Ort der Arbeitnehmer aus seine arbeitsrechtlichen Pflichten erfüllen darf. Die Möglichkeiten reichen hier von der zusätzlichen Möglichkeit im Homeoffice als auch von einem durch den Arbeitnehmer frei wählbaren (mobilen oder flexiblen) Arbeitsplatz.

Gibt es Gesichtspunkte der DSGVO, die im Homeoffice beachtet werden müssen?
Es gelten grundsätzlich die gleichen datenschutzrechtlichen Pflichten, die auch ohne Homeoffice relevant sind. Zu berücksichtigen ist, dass für die Datenverarbeitung aus dem Homeoffice weiterhin der Arbeitgeber verantwortlich bleibt. Dieses bedeutet natürlich nicht, dass dem Arbeitnehmer nicht besondere Pflichten hinsichtlich der Art und Weise der Datenverarbeitung auferlegt werden können.

Dieses findet üblicherweise über eine Homeoffice-Richtlinie statt, die über einen Verweis im Arbeitsvertrag die Bedeutung einer arbeitsrechtlichen Weisung erlangt.
Die Arbeitnehmer sollten insbesondere dahingehend unterrichtet werden, wie sie vertrauliche Daten vor dem Zugriff Dritter schützen können – und dazu gehören auch Familienmitglieder oder Mitbewohnern.
Der Computer sollte sich nach einer gewissen Zeit automatisch sperren, das Arbeitszimmer sollte verschlossen sein und vertrauliche Telefonate nicht mitgehört werden können. Soweit Akten oder sonstige papierbasierte Unterlagen existieren, sollten diese nach Gebrauch in Schränken verschlossen werden.
Grundsätzlich ist allerdings zu empfehlen, dass hauptsächlich elektronisch zu arbeiten, da digitale Dokumente einfacher durch technische Maßnahmen geschützt werden können. Ferner sollte die Richtlinie auch Regelungen zu der Frage enthalten, ob die betrieblich zur Verfügung gestellten Arbeitsgeräte für private Zwecke genutzt werden dürfen. Das Verbot einer Privatnutzung ist aus rechtlicher Sicht sinnvoll, da die Privatnutzung eine Vielzahl zu regelnder Folgefragen und teilweise auch Pflichten aufwirft.

Kann der Arbeitnehmer das Homeoffice von der Steuer absetzen?
Das Arbeiten im Homeoffice ist grundsätzlich steuerlich absetzbar. Arbeitnehmer müssen dafür allerdings nachweisen, dass ihr Arbeitgeber das Arbeiten von Zuhause aus angeordnet hat. Die Kosten für die Einrichtung des Homeoffice lassen sich nur absetzen, wenn der Arbeitnehmer ein eigenes Arbeitszimmer unterhält. Unabhängig hiervon können aber die Kosten für zusätzlich benötigte Arbeitsmittel wie etwa zusätzliches Büromaterial abgesetzt werden. Welche genauen Positionen steuerlich absetzbar sind ist jedoch eine Frage des Einzelfalles.

Wo finde ich ein Muster zu einer Datenschutz-Vereinbarung fürs Homeoffice?
Wir stellen Ihnen gern eine Datenschutz-Vereinbarung fürs Homeoffice bereit. Sprechen Sie uns einfach an.

Gibt es Ausnahmen hinsichtlich der Arbeitszeit für „systemrelevante Tätigkeiten“?
Ja, zur Gewährleistung der Produktion und des Erhalts existentieller Güter und Dienstleistungen der Daseinsvorsorge im Zusammenhang mit der Covid-19-Pandemie, sind Ausnahmeregelungen im Arbeitszeitrecht möglich. Zu den systemrelevanten Tätigkeiten zählen beispielsweise das Kommissionieren von Waren und Befüllen von Regalen im Lebensmittel- und Drogeriewareneinzelhandel, die medizinische Versorgung von Patientinnen und Patienten durch Arztpraxen, labordiagnostische Tätigkeiten und mobile Testcenter, die Produktion von Desinfektionsmitteln und Mundschutz. Auch Tätigkeiten in Krankenhäusern, Pflegeeinrichtungen, Behörden, bei Energie- und Wasserversorgern und in Abfall- und Entsorgungsbetrieben gehören hierzu.
Arbeitnehmer, die in systemrelevanten Bereichen arbeiten, dürfen dem Grunde nach

- täglich bis zu 12 Stunden arbeiten,
- an Sonn- und Feiertagen arbeiten sowie
- durchschnittlich bis zu 48 Std. in der Woche arbeiten.

Zu beachten ist allerdings, dass diese Regelungen nur dann greifen, wenn die jeweils zuständigen Landesbehörden eine entsprechende Verordnung erlassen (§ 15 Abs. 2 ArbZG).

Darf der Arbeitgeber bei einem Verdacht eine ärztliche Untersuchung anordnen?
Nein. Auch hier hat das Weisungsrecht des Arbeitgebers Grenzen. Entsprechende Anordnungen dürfen grundsätzlich nicht in das Recht auf körperliche Unversehrtheit des Arbeitnehmers eingreifen. Dieser muss einer entsprechenden Anordnung nicht nachkommen. Im Übrigen gilt das auch für eine perspektivisch mögliche Impfung. Verweigert der Arbeitnehmer sich jedoch trotz Infektionsverdachts einer Untersuchung, darf der Arbeitgeber ein Betreten der betrieblichen Einrichtungen verweigern und gegebenenfalls Homeoffice anordnen. Letzteres setzt jedoch wiederum voraus, dass geeignete Arbeitsmittel zur Verfügung gestellt werden.

Das sollten Ihre Angestellten im Homeoffice beachten
Ihre Angestellten sollten einige Vorkehrungen treffen, die den Datenschutz und die Datensicherheit auch bei der Heimarbeit sicherstellen. Diese Zusammenstellung gibt Ihnen einen Überblick über die wichtigsten Maßnahmen. Jedes Unternehmen sollten aber individuell prüfen lassen, welche Anforderungen erfüllt werden müssen.
Ist das WLAN rechtssicher verschlüsselt?

Wird der Zugang in das Internet zu Hause über ein WLAN hergestellt, muss dieses WLAN ausreichend verschlüsselt sein. Das betrifft sowohl die Art der Verschlüsselung als auch die Komplexität des Schlüssels.

Nutzen Sie sichere VPN-Verbindungen
Die Online-Verbindung zu den Servern des Unternehmers darf nur über eine sichere VPN Verbindung hergestellt werden.

Videokonferenz im Homeoffice: Diese Anbieter sind sicher
Videokonferenzen sind häufig ein wichtiger Bestandteil der Arbeit von zuhause. Auch hier gilt es, den Datenschutz sicherzustellen. Welche Programme sich besonders für Ihr Unternehmen eignen finden Sie hier in einem ausführlichen Artikel zum Thema.

Vorsicht mit privaten E-Mail-Adressen
Es ist nicht verboten, private E-Mail-Adressen zu verwenden, gleichwohl kann aus IT-technischer und datenschutzrechtlicher Sicht hiervon nur angeraten werden. Der Zugriff auf unter Umständen vertrauenswürdige Inhalte innerhalb einer ungesicherten Verbindung ist kritisch zu bewerten. Auch bleibt der Arbeitgeber datenschutzrechtlich verantwortlich für die Verarbeitung personenbezogener Daten. Berufsbereiche, in denen besondere Pflichten zur Geheimhaltung existieren, wie im Gesundheitswesen oder der Rechtspflege, kann allein die Weiterleitung ein Verstoß gegen entsprechende Geheimhaltungspflichten begründen.

Vorsicht bei Kommunikation über Messenger
Werden Messenger-Anwendungen verwendet, sollten sie eine ausreichende Ende-zu-Ende Verschlüsselung haben.

Schützen Sie Ihr Zimmer
Wenn man das Zimmer verlässt, sollten die (personenbezogenen) Daten vor unberechtigtem Zugriff geschützt werden. Auf dem Computer sollte deshalb ein Bildschirmschoner mit Kennwort-Schutz aktiviert werden.
Idealerweise ist der Raum, in dem man arbeitet, abschließbar. Schriftliche Dokumente sollten ohnehin in einem verschlossenen Behältnis aufbewahrt werden.
Es ist darauf zu achten, dass die anderen Personen, die sich im Haushalt aufhalten, keinen Zugriff auf personenbezogene Daten erhalten. Deshalb sollte der Bildschirm so aufgestellt werden, dass andere ihn nicht ablesen können. Telefonate sollten in Räumen geführt werden, in denen andere nicht mithören können. Ausdrucke sollte möglichst rasch aus dem privaten Drucker entfernt werden. Druckaufträge sollten natürlich auch nicht auf Druckern im Unternehmen landen, wo sie der Auftraggeber nicht abholen kann.

Ein Papierkorb ist keine sichere Ablage.
Beim Papiermüll ist ebenfalls Vorsicht geboten. Geschäftsunterlagen und insbesondere Dokumente mit personenbezogenen Daten sollten immer in das Unternehmen gebracht und dort fachgerecht entsorgt werden. Auf gar keinen Fall sollten solche Unterlagen in den Hausmüll geworfen werden.

Was tun bei Datenverlust?
Kommt es doch einmal zu einem Datenverlust, sollten die Mitarbeiter auch wissen, dass sie den Vorfall schnellstmöglich melden müssen und an wen sie ihn im Unternehmen melden müssen. Sorgen Sie für regelmäßige Back-Ups Ihrer relevanten Daten.

Wir unterstützen Sie bei der Implementierung von Datenschutz, Datensicherheit und Arbeitsrecht im Homeoffice
Gerne unterstützen wir Sie schnell und kosteneffizient bei allen Fragen rund um Datenschutz, Datensicherheit und Arbeitsrecht im Homeoffice und erstellen für Sie entsprechende Unternehmens-Richtlinien.

Basisbausteine:

- Nutzen Sie unsere Checklisten zu allen rechtlichen Fragen, die im Rahmen der Einführung von Heimarbeitsplätzen (Homeoffice) in Abgrenzung zu mobilen Arbeitsplätzen geprüft werden müssen.
- Durchführung praxisnaher Online- und Präsenz-Schulungen
- Bereitstellung von Schulungsunterlagen und Service-Cards

Datenschutz und Datensicherheit

- Beurteilung der Datenschutz- und IT-Sicherheitsmaßnahmen beim Arbeiten im Homeoffice
- Individuell abgestimmte Datenschutzrichtlinien für Ihr Unternehmen
- FAQ-Dokumente und Arbeitsanweisungen zum Datenschutz für Ihre Anwender

Arbeitsrecht

- Rechtliche Beratung, wann der Betriebsrat in das Thema Homeoffice eingebunden werden muss
- Individuell abgestimmte Betriebsvereinbarungen und Ergänzungsvereinbarungen zu Arbeitsverträgen
- Homeoffice in der arbeitsrechtlichen Praxis

Sonstige rechtliche Themen

- Homeoffice und Sicherstellung des Geschäftsgeheimnis-Schutzes
- Homeoffice und Versicherungsschutz
- Homeoffice und steuerrechtliche Fragen
- Homeoffice und Beachtung der Persönlichkeitsrechte von Mitarbeitern und Geschäftspartnern

Die einzelnen Bausteine bieten wir wahlweise planbar zu vorab vereinbarten Festpreisen oder individuell nach Aufwand an.

Kostentransparenz ist für uns in jedem Fall selbstverständlich.

Weiterführende Hinweise zum Homeoffice der Datenschutzaufsichtsbehörden

Datenschutz im Homeoffice. Informationen des Datenschutzzentrums:

https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Datenschutz in Zeiten von Covid-19. Informationen des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit:

https://datenschutz-hamburg.de/assets/pdf/Corona-FAQ.pdf

Corona-Pandemie: Datenschutz und Heimarbeit. Informationen der Landesbeauftragten für Datenschutz und Akteneinsicht Brandenburg:

https://www.lda.brandenburg.de/sixcms/detail.php/947857

Telearbeit und Mobiles Arbeiten. Ein Datenschutz-Wegweiser des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit:

https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

Dr. Oliver M. Bühr, Frankfurt/Main, o.buehr@skwschwarz.de
Dr. Oliver Hornung, Frankfurt/Main, o.hornung@skwschwarz.de
Bettina-Axenia Bugus, Hamburg, b.bugus@skwschwarz.de
Tabea Frühinsfeld, Berlin, t.fruehinsfeld@skwschwarz.de
Dr. Alexander Schmid-Lossberg, Berlin, a.schmid-lossberg@skwschwarz.de
Arndt Tetzlaff, Berlin, a.tetzlaff@skwschwarz.de
Heiko Wunderlich, München, h.wunderlich@skwschwarz.de

Datenschutz und Datensicherheit im Home-Office

Viele berufstätige Menschen, Arbeitnehmer ebenso wie Selbstständige, hat es im Angesicht der Corona-Pandemie unversehens ins Home-Office verschlagen. Dabei darf natürlich der Datenschutz und die Datensicherheit nicht auf der Strecke bleiben. Wer schon bisher das Arbeiten im Home-Office zuließ, konnte seinen Beschäftigten eher Leitlinien geben als Unternehmen, bei denen das bislang nicht der Fall war. Auch der Arbeit im Home-Office steht das Datenschutzrecht nicht entgegen.

Wichtig ist allerdings, dass Vorkehrungen für die Sicherheit der Daten getroffen werden, die dem mit der Verarbeitung zusammenhängende Risiko angemessen sind.

Im Home-Office werden die Daten zwar zumindest teilweise an einem anderen Ort und mit anderen Mitteln verarbeitet. Verantwortlicher im Sinne des Datenschutzrechts bleibt auch im Home-Office der Arbeitgeber. Deshalb ist es wichtig, dass private und dienstliche Daten nicht vermischt werden. Der Arbeitgeber legt die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten auch im Home-Office fest.

Werden Daten für einen Dritten im Auftrag verarbeitet, ist der zugrunde liegende Vertrag über Auftragsverarbeitung zu prüfen. Nicht jeder Vertrag lässt die Tätigkeit im Home-Office zu. Manche Verträge enthalten zumindest Einschränkungen oder fordern bestimmte Sicherheitsvorkehrungen. Das betrifft natürlich nur die Fälle, in denen der Arbeitnehmer für den Auftragnehmer tätig ist.
Die datenschutzrechtlichen Pflichten sind nicht einschlägig, wenn nur Daten ohne Personenbezug verarbeitet werden. In den meisten Fällen lässt es sich jedoch gar nicht vermeiden, dass zumindest einige personenbezogene Daten genutzt oder verarbeitet werden. Auch vertrauliche Daten ohne Personenbezug, wie z.B. Geschäftsgeheimnisse, müssen im Unternehmen durch ausreichende technische Vorkehrungen geschützt werden.

Empfehlenswert für ein Unternehmen ist es, alle Vorgaben im Zusammenhang mit der Arbeit zu Hause in einer Home-Office Richtlinie festzulegen. Dort können dann auch alle Vorkehrungen zur Sicherheit beschrieben werden. Folgende Punkte sollten insbesondere aufgenommen werden:

- Vorrangig sollten die IT Geräte des Unternehmens genutzt werden und nicht private Geräte. So wird gewährleistet, dass die Sicherheitsvorkehrungen wie z.B. Betriebssystem, Virenschutz und Firewall auf dem aktuellsten Stand sind. Eine Privatnutzung dieser Geräte sollte untersagt werden, weil ansonsten der Zugriff auf gespeicherte Daten durch das Unternehmen erschwert werden kann.
- Die Speichermedien auf den IT-Geräten und externe Speichermedien sollten verschlüsselt sein. Gehen die Speichermedien verloren oder werden gestohlen, sind die Daten so trotzdem vor unberechtigtem Zugriff gesichert. Am besten ist jedoch, wenn Dateien mit personenbezogenen Daten auf den Servern des Unternehmens gespeichert werden und nicht auf dem Endgerät im Home-Office.
- Wird der Zugang in das Internet zu Hause über ein WLAN hergestellt, muss dieses WLAN ausreichend verschlüsselt sein. Das betrifft sowohl die Art der Verschlüsselung als auch die Komplexität des Schlüssels.
- Die Online-Verbindung zu den Servern des Unternehmers darf nur über eine sichere VPN Verbindung hergestellt werden.
- Die Weiterleitung von geschäftlichen E-Mails auf private E-Mail-Adressen sollte unterbleiben.
- Werden Messenger-Anwendungen verwendet, sollten sie eine ausreichende Ende-zu-Ende Verschlüsselung haben.
- Wenn man das Zimmer verlässt, sollten die (personenbezogenen) Daten vor unberechtigtem Zugriff geschützt werden. Auf dem Computer sollte deshalb ein Bildschirmschoner mit Kennwort-Schutz aktiviert werden.
- Idealerweise ist der Raum in dem man arbeitet, abschließbar. Schriftliche Dokumente sollten ohnehin in einem verschlossenen Behältnis aufbewahrt werden.
- Es ist darauf zu achten, dass die anderen Personen, die sich im Haushalt aufhalten, keinen Zugriff auf personenbezogene Daten erhalten. Deshalb sollte der Bildschirm so aufgestellt werden, dass andere ihn nicht ablesen können. Telefonate sollten in Räumen geführt werden, in denen andere nicht mithören können. Ausdrucke sollte möglichst rasch aus dem privaten Drucker entfernt werden. Druckaufträge sollten natürlich auch nicht auf Druckern im Unternehmen landen, wo sie der Auftraggeber nicht abholen kann.
- Beim Papiermüll ist ebenfalls Vorsicht geboten. Geschäftsunterlagen und insbesondere Dokumente mit personenbezogenen Daten sollten immer in das Unternehmen gebracht und dort fachgerecht entsorgt werden. Auf gar keinen Fall sollten solche Unterlagen in den Hausmüll geworfen werden.

Kommt es doch einmal zu einem Datenverlust, sollten die Mitarbeiter auch wissen, dass sie den Vorfall schnellstmöglich melden müssen und an wen sie ihn im Unternehmen melden müssen. Weiterführende Hinweise zum Home-Office geben auch die Datenschutzaufsichtsbehörden z.B.:

- https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf
- https://datenschutz-hamburg.de/assets/pdf/Corona-FAQ.pdf
- https://www.lda.brandenburg.de/sixcms/detail.php/947857
- https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

Gerne unterstützen wir Sie bei allen datenschutzrechtlichen Fragen rund um das Homeoffice und insbesondere bei der Erstellung entsprechender Unternehmens-Richtlinien.

Dr. Oliver Hornung, Frankfurt/Main, o.hornung@skwschwarz.de
Dr. Hendrik Skistims, Frankfurt/Main, h.skistims@skwschwarz.de

Digitale Signaturen in Ihrem Unternehmen

Immer mehr Unternehmen haben die Notwendigkeit erkannt, ihre Entscheidungsprozesse und Unterschriftenvorgaben zu digitalisieren. Und das nicht nur in Zeiten eingeschränkter Bewegungsfreiheit und vermehrter Homeoffice-Aufenthalte.

In globalisierten Unternehmen ist es schlicht nicht möglich, immer auf die nächste persönliche Geschäftsführungsbesprechung oder Vorstandssitzung zu warten, um per Unterschriften eine Entscheidung zu treffen.

Und auch im Personalbereich werden die Vorteile eines virtuellen „Onboardings“ von Mitarbeitern deutlich. Vermehrt treten Personalabteilungen an uns heran, um die Möglichkeiten zu prüfen, mit Mitarbeitern auch über die Distanz rechtssicher Vereinbarungen schließen zu können.
Eine einfache Lösung für diesen Bedarf ist die Verwendung elektronischer Signaturen.
Unternehmen sollten allerdings die rechtlichen Rahmenbedingungen kennen, zu denen digitale Signaturen genutzt werden können und wissen, wann dies eben auch mal nicht möglich ist.
Denn in einigen Fällen schreibt das Gesetz die Schriftform vor, die nur zum Teil mit einer relativ aufwendigen sogenannten qualifizierten elektronischen Signatur ersetzt werden kann. Und zum Teil ist die elektronische Form sogar gänzlich ausgeschlossen.

Welche Arten der elektronischen Signatur gibt es? Und wann sind sie zulässig?
Grundsätzlich wird zwischen drei Arten der digitalen Signatur unterschieden:
- (Einfache) elektronische Signatur
- Fortgeschrittene elektronische Signatur
- Qualifizierte elektronische Signatur.

Jede dieser drei Signaturen ist an konkrete Voraussetzungen geknüpft, die verschiedenen Sicherheitsstufen entsprechen. Die Anforderungen, die an die jeweilige Signatur gestellt werden, ergeben sich aus der europäischen eIDAS Verordnung [Link einfügen].

Was ist die eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste?
Die eIDAS-Verordnung ist eine EU-Verordnung, die sich mit der Regelung von sogenannten elektronischen Identifizierungsmitteln und Vertrauensdiensten befasst. Als EU-Verordnung gilt sie in allen EU-Mitgliedsstaaten unmittelbar und vorrangig vor den jeweiligen nationalen Gesetzen (anders als dies etwa EU-Richtlinien normalerweise tun). Inhaltlich befasst sich die eIDAS-Verordnung insbesondere mit Anforderungen an elektronische Signaturen, stärkt diese unter gewissen Bedingungen aber auch, indem sie etwa ihren Beweiswert vor Gericht festschreibt. Neben der elektronischen Signatur sind auch verschiedene andere Elemente Gegenstand der Verordnung, so etwa elektronische Siegel und Dienste für die Zustellung elektronischer Einschreiben.
www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html

Wann genügt eine einfache elektronische Signatur als verbindliche Unterschrift?
Nach der gesetzlichen Definition sind (einfache) elektronische Signaturen Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft werden und die der Unterzeichner zum Unterzeichnen verwendet (Art. 3 Nr. 10 eIDAS-VO). Dies kann z.B. bereits bei einer einfachen E-Mail Signatur oder einer eingescannten Unterschrift als eingebettetes Bild im PDF Dokument der Fall sein. Dieses Mittel sollte für Erklärungen verwendet werden, die keine übermäßigen Risiken für das Unternehmen bedeuten und daher auch nur einen vergleichsweise geringen Beweiswert benötigen. Dies können etwa Erklärungen im Rahmen laufender

Vertragsbeziehungen sein, die lediglich weniger bedeutende Aspekte dieser Beziehung bestimmen (z.B. Abstimmung von Protokollen, Terminbestätigungen in laufenden Projekten etc.).
Je nach Risikobereitschaft und individueller Situation können auch Verträge, die in großer Menge aber jeweils nur mit kleinen Volumina abgeschlossen werden sollen, ein sinnvolles Anwendungsfeld für die einfache elektronische Signatur sein. Auf keinen Fall darf die einfache Signatur dort verwendet werden, wo die Schriftform als eigenhändige Unterschrift gesetzlich vorgeschrieben ist.

Wo wird eine fortgeschrittene elektronische Signatur im Unternehmen benötigt?
Für die fortgeschrittene elektronische Signatur sind bereits deutlich höhere Anforderungen zu erfüllen. Die zu erfüllenden Kernmerkmale sind, dass diese Signatur eindeutig dem Unterzeichner zugeordnet werden kann und die Identifizierung des Unterzeichners ermöglicht wird (Art. 3 Nr. 11, 26 eIDAS-VO). In vielen Fällen werden dafür zum Beispiel biometrische Erkennungsmerkmale wie der Fingerabdruck genutzt.

Eine Zwei-Faktor-Authentifizierung ist aus rechtlichen Gründen nicht zwingend notwendig, wird aber oft als zusätzliches Element zur eindeutigen Identifizierung des Signierenden eingesetzt. Außerdem muss gewährleistet sein, dass nachträgliche Veränderungen erkannt werden können.
In Abgrenzung zur einfachen elektronischen Signatur sollte die fortgeschrittene elektronische Signatur verwendet werden, wenn die hohe Bedeutung eines Dokuments auch eine stärkere Verlässlichkeit der Unterschrift erforderlich macht. Auch der Beweiswert ist damit erhöht. Die meisten Vertragsschlüsse werden hierfür ein geeignetes Anwendungsfeld darstellen. Daher ist die fortgeschrittene elektronische Signatur oft die Standardunterschrift für übliche Verträge im normalen Geschäftslauf.
Nicht ausreichend ist die fortgeschrittene elektronische Signatur nur dann, wenn entweder die Schriftform gesetzlich vorgeschrieben oder die Bedeutung des Vertrages so groß ist, dass selbst kleinste Unsicherheiten vermieden werden müssen. Hierunter werden etwa Asset-Deals fallen, aber auch wichtige Erklärungen im Arbeitsverhältnis, bei Bürgschaften oder im Familien- und Erbrecht.

Was unterscheidet die qualifizierte von der fortgeschrittenen elektronischen Signatur?
Bleibt letztlich noch die qualifizierte elektronische Signatur nach Art. 3 Nr. 12, 15, 23 eIDAS-VO als technisch und operativ aufwendigste Form der digitalen Unterschrift. Um den Anforderungen an eine qualifizierte elektronische Signatur zu genügen, muss eine Signatur mindestens alle Merkmale der fortgeschrittenen Signatur aufweisen. Zusätzlich muss sie auch noch von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt worden sein und auf einem qualifizierten Zertifikat für elektronische Signaturen beruhen.

Qualifizierte Zertifikate können wiederum nur von sog. **Vertrauensdiensteanbietern** ausgestellt werden, die den Antragsteller anhand geeigneter Mittel identifizieren. Sie können außerdem nur an natürliche Personen ausgestellt werden, nicht etwa an juristische Personen wie eine GmbH oder Aktiengesellschaft. Das bedeutet, dass für jeden Unterschriftsberechtigten (z.B. jeden Geschäftsführer, Prokurist oder Vorstand) eine eigene digitale Signatur individuell erstellt werden muss.

Eine Liste der deutschen Vertrauensdiensteanbieter findet sich auf der Homepage der Bundesnetzagentur.

Immer dann, wenn das Gesetz (nicht nur die Parteien eines Vertrages oder eine AGB Schriftformregelung) die Schriftform – also die eigenhändige Unterschrift – vorschreibt, kann diese durch die qualifizierte elektronische Signatur, aber auch nur durch diese ersetzt werden. Denn nur die qualifizierte elektronische Signatur erfüllt die Anforderungen an die sog. elektronische Form nach § 126a BGB.

Die elektronische Form ist wiederum als einzige Alternative zur Schriftform gesetzlich zulässig, wenn sich nicht aus den gesetzlichen Vorschriften etwas anderes ergibt. Beispiele, in denen nur die qualifizierte digitale Signatur den hohen Anforderungen des Gesetzes genügt, sind die Stiftung unter Lebenden, die zeitliche Befristung eines Mietvertrages, die Kündigung und der Aufhebungsvertrag zum Arbeitsvertrag, die Kündigung von Bau- oder Architektenvertrag, Bürgschaften und Schuldanerkenntnisse, bestimmte Vereinbarungen mit Handelsvertretern und öffentlich rechtliche Verträge zwischen Bürgern und der Verwaltung (damit sind nicht die normalen Beschaffungsvorgänge der Behörden gemeint).

Worin unterscheiden sich elektronische Signatur und digitale Signatur?
Elektronische und digitale Signatur sind im Kern völlig verschiedene Gattungsbegriffe. Die elektronische Signatur ist ein rechtlicher Begriff und beschreibt vereinfacht gesagt die (in verschiedenen Graden abgesicherte) Unterschrift einer Person durch elektronische Mittel.
Die digitale Signatur als technischer Begriff umfasst hingegen eine Vielzahl von speziellen Verfahren, die etwa nachträgliche Manipulation an einem Dokument verhindern sollen. Die Begriffe können sich auch überlagern, müssen das aber nicht. Eine einfache elektronische Signatur wird etwa kaum jemals eine digitale Signatur umfassen.

Im Falle einer fortgeschrittenen elektronischen Signatur ist die Verwendung einer digitalen Signatur aber durchaus wahrscheinlich.

Wie bekommen Sie eine elektronische Signatur?
Es gibt verschiedene Anbieter, die eine digitale Signatur zur Verfügung stellen. Die wohl bekanntesten dürften dabei DocuSign und Adobe sein. Aber auch europäische Anbieter wie Certeurope sind auf dem Markt für elektronische Signaturen tätig. Die aufwendigeren Zertifikate, die für eine qualifizierte digitale Signatur notwendig sind, können allerdings nur die hierfür benannten Vertrauensdiensteanbieter zur Verfügung stellen.

Ist eine elektronische Unterschrift genauso rechtswirksam wie eine handschriftliche?
Die elektronische Signatur ist fast immer so rechtswirksam wie die eigenhändige Unterschrift. Gegebenenfalls muss aber die richtige Art der elektronischen Signatur gewählt werden. Erfordert eine Erklärung die Schriftform, so vermag nur die qualifizierte elektronische Signatur diesem Erfordernis gerecht zu werden.

Ist sogar die notarielle Beglaubigung angeordnet (etwa bei Grundstücksgeschäften), so wird keine elektronische Signatur für sich ausreichen. Notare haben hier aber auch besonders geregelte Instrumente, mit denen einige Ihrer Tätigkeiten elektronisch durchgeführt werden können. Die tatsächlich eigenhändige und handschriftliche Form („Tinte auf Papier“ bzw. „wet ink“) ist allerdings nur in ganz seltenen Ausnahmen und bei höchstpersönlichen Erklärungen wie z.B. beim eigenhändig errichteten Testament notwendig.

Wie ist die internationale Rechtslage (z.B. in den USA) zu digitalen Unterschriften?
International sind die jeweils anwendbaren nationalen rechtlichen Rahmenbedingungen zu beachten. Innerhalb der EU gilt aufgrund der eIDAS-VO ein einheitlicher Rechtsrahmen mit identischen Unterschriftsregeln für alle Mitgliedstaaten.

In den USA werden digitale Unterschriften mit elektronischen Signaturen z.B. gleichrangig mit handschriftlichen Unterschriften behandelt. Festgelegt ist das im Gesetz zu elektronischen Signaturen im globalen und nationalen Handel (ESIGN) und im Gesetz zur Vereinheitlichung elektronischer Transaktionen (UETA).

Können digitale Unterschriften auch im Behördenverkehr genutzt werden?
Über ihre jeweiligen E-Goverment-Gesetze haben Bund und Länder umfassende Regelungen zum elektronischen Behördenzugang getroffen. Insbesondere haben sie ihre Behörden dabei etwa verpflichtet, Zugang für die Übermittlung elektronischer Dokumente zu ermöglichen und elektronische Bezahlmöglichkeiten einzurichten.

Ob sich der konkrete Behördengang im Einzelnen elektronisch durchführen lässt, muss immer im Einzelfall und teilweise auch in Abhängigkeit von der jeweiligen Behörde beurteilt werden.

Können Verträge auch auf dem Smartphone oder Tablet unterschrieben werden?
Jede Erklärung, die mittels eines PCs abgegeben werden kann, ist auch über mobile Endgeräte möglich. Sowohl die einfache als auch die fortgeschrittene elektronische Signatur sind am Smartphone oder Tablett ohne Weiteres technisch nutzbar. Das geschieht z.B. durch Einbindung eines Feldes zur Unterschrift mit dem Finger oder einem digitalen Stift.

Selbst qualifizierte elektronische Signaturen, die notwendig sind, um gesetzliche Schriftformanforderungen zu erfüllen, sind am mobilen Endgerät einsetzbar. Meist ist dafür dann gegebenenfalls ein Gerät mit Webcam notwendig (was heute aber ohnehin Standard ist).

Kann man Verträge, die eine Klausel zur Schriftform enthalten, digital unterschreiben?
Wenn in Verträgen die Einhaltung der Schriftform vereinbart wird, hat das eine andere Wirkung, als wenn das Gesetz dies zwingend vorschreibt. Gesetzliche Schriftformvorgaben können nur durch eine qualifizierte elektronische Signatur erfüllt werden. Daher sind Verträge mit nicht ausreichend signierter digitaler Unterschriften unwirksam.

Bei vertraglichen Schriftformklauseln ist hingegen zu beachten, dass grundsätzlich diese „vertragliche Schriftform" auch durch elektronische Signaturen erfüllbar ist. Die Parteien eines Vertrages können das aber auch in ihrem jeweiligen Interesse individuell miteinander regeln.

Im Unternehmensverkehr (z.B. zwischen Lieferanten und Kunden oder im Unterauftragsverhältnis) einigt man sich oft darauf, welcher Level an Beweiskraft und damit auch welche elektronische Signaturform für bestimmte Verträge von beiden Seiten anerkannt wird (sog. Beweisvereinbarungen). Im Arbeitsverhältnis lässt sich dies im Arbeitsvertrag oder in entsprechenden Betriebsvereinbarungen regeln.

Wann ist eine digitale Signatur unwirksam?
Dort, wo die Schriftform gesetzlich vorgeschrieben ist, können andere digitale Unterschriftsformen als die qualifizierte elektronische Signatur keine wirksame Vereinbarung möglich machen. Verträge ohne individuelles qualifiziertes Zertifikat des Unterschriftsberechtigten im Unternehmen sind daher unwirksam. Keine Vertragspartei kann sich auf sie berufen.

Das gleiche gilt für Erklärungen wie Kündigungen oder Befristungen von Arbeits- und Mietverträgen, soweit das Gesetz hierfür die Schriftform – also die qualifizierte elektronische Signatur – vorschreibt. Wenn das Gesetz die Beteiligung eines Notars vorschreibt (z.B. beim Grundstückseigentum oder der Gründung einer GmbH), sind Dokumente, die „nur" digital unterschrieben wurden, unabhängig von der Art der elektronischen Signatur komplett nichtig und werden so behandelt, als hätte es sie nie gegeben.

Wenn die Parteien hingegen in der Wahl der Form frei sind oder lediglich vertragliche Schriftformvereinbarungen (auch in akzeptierten AGB) getroffen haben, können Verträge aus rechtlicher Sicht auf viele Arten wirksam geschlossen werden.

Sobald zwei Willenserklärungen vorliegen, die inhaltlich übereinstimmen, kommt eine Vereinbarung u.U. auch mündlich oder per Telefon rechtsverbindlich zustande. Für die effektive Wirksamkeit der digitalen Unterschrift im Unternehmensalltag kommt es dann aber auch darauf an, dass sich der tatsächlich erfolgte rechtlich wirksame Einigungsprozess mit ausreichender Überzeugungskraft beweisen lässt.

Wer sich auf eine wirksame Vereinbarung berufen und daraus Ansprüche oder Rechte ableiten will, muss im Ernstfall zur Überzeugung eines Richters belegen können, dass alle Beteiligten bewusst eine verbindliche Vereinbarung treffen wollten. Und der Richter wird dabei allein objektiv und als Nichtbeteiligter die bewiesenen Umstände des Vertragsschlusses betrachten. Je stärker die elektronische Signatur abgesichert ist oder der Unterzeichnungsprozess dokumentiert ist, umso eher wird dies auch in der Praxis gelingen.

Können geheime und vertrauliche oder persönliche Dokumente digital unterzeichnet werden?
Beim Einsatz der Produkte von Anbietern elektronischer Signaturen ist es oft technisch unvermeidbar, dass die zu unterzeichnenden Dokumente zum Austausch zwischen den Unterschriftspartnern über die Systeme des Anbieters weitergeleitet werden oder der Anbieter zumindest einen technisch notwendigen Zugriff auf die Dokumente hat. Dabei sind dann wie im analogen Unterschriftenprozess auch die besonderen Vorgaben zur technisch-organisatorischen Einhaltung von Vertraulichkeit gerade bei Geschäftsgeheimnissen und zur Einhaltung des Datenschutzes zu beachten. Wenn nötig, sind entsprechende Auftragsverarbeitungsverträge und Vertraulichkeitsverpflichtungen mit dem Anbieter zu schließen.

Können Arbeitsverträge per digitaler Unterschrift geschlossen werden?
Grundsätzlich können Arbeitsverträge und Änderungsvereinbarungen formfrei geschlossen werden, d.h. den Parteien steht es auch frei, auf welche Art sie (elektronisch) signieren. Denkbar ist damit z.B, der Arbeitsvertragsschluss mittels fortgeschrittener elektronischer Signatur.

Im Arbeitsrecht gibt es allerdings eine Vielzahl an Erklärungen und Vereinbarungen, für die der Gesetzgeber die Schriftform zwingend vorgesehen hat. Mehr Details dazu erfahren Sie hier.

Wie finden Sie den richtigen Anbieter von elektronischen Signaturen für Ihr Unternehmen?
Fragen, die Ihnen helfen können, den richtigen Anbieter für elektronische Signaturen in Ihrem Unternehmen zu finden:

- Welche Art(en) elektronischer Signatur benötigt Ihr Unternehmen (einfach, fortgeschritten oder qualifiziert), d.h. für welche Vertragssituationen soll das Tool zum Einsatz kommen und welche gesetzlichen Formvorgaben bestehen hierfür bzw. wie hoch muss der Beweiswert der digitalen Unterschrift sein?
- Benötigen Sie einen Anbieter, der auch die qualifizierte elektronische Signatur erstellt?
- Ist es für Sie wichtig, verschiedene Arten von Signaturen gleichzeitig anzubieten?
- Wie einfach lässt sich das Tool technisch in Ihre IT-Umgebung im Unternehmen integrieren und welche Lizenzvorgaben macht der Anbieter dafür?
- Stellt der Anbieter detaillierte und nachvollziehbare Protokolle des Signaturvorgangs als Nachweis der digitalen Unterzeichnung zur Verfügung?
- Kann der Anbieter auf Anfrage überzeugende Antworten und Mustervereinbarungen zum Datenschutz, der IT-Sicherheit und zum Schutz von Geheimnissen liefern?

Fazit
Elektronische Signaturen sind aus dem Geschäftsalltag nicht mehr wegzudenken und können Unternehmensprozesse enorm effizient machen. Insbesondere bei gänzlich formfreien Vereinbarungen stellen elektronische Signaturen eine attraktive Alternative zur papierbasierten Unterschrift dar. Oftmals lässt sich die Identität des Unterzeichnenden bei der elektronischen Signatur sogar besser nachvollziehen als beim unleserlichen Kürzel mit Tinte auf dem Vertragspapier.
Bei Vereinbarungen, die einer Formvorschrift unterliegen, ist jedoch penibel auf die Einhaltung der korrekten Art der Unterschrift bzw. der elektronischen Signatur zu achten.
Auch bei allen anderen digitalen Unterschriftsformen ist auf die Einhaltung der rechtlichen Rahmenbedingungen für die jeweils verwendete elektronische Signatur zu achten.

Nutzen Sie unsere Expertise bei der Digitalisierung Ihrer Unternehmensentscheidungen.
Wir unterstützen Sie mit rechtlichem Know-how, technischem Verständnis und pragmatischen Lösungsansätzen:

Basisbausteine

- Nutzen Sie unsere Checklisten zu allen rechtlichen Fragen, die im Rahmen der Digitalisierung Ihrer Unternehmensentscheidungen geprüft werden müssen.
- Sie erhalten von uns konkrete Empfehlungen geeigneter E-Signaturen auf Basis eines umfassenden Produktvergleichs der wichtigsten marktüblichen Tools und Anbieter
- Beratung bei der Integration in Ihre internen Prozesse
- Erstellung von Unterschriftsvereinbarungen mit Geschäftspartnern, Lieferanten und Kunden
- Rechtliche Begleitung Ihrer Angebotsanfrage bei den Anbietern zur Gestaltung Ihrer Prozesse
- Durchführung praxisnaher Online- und Präsenz-Schulungen zu digitalen Unterschriftsformen, individuell zugeschnitten auf die relevanten Ansprechpartner in Ihrem Unternehmen
- Bereitstellung von Schulungsunterlagen und Service-Cards für Ihre interne Verwendung im Unternehmen

Datenschutz und Datensicherheit

- Konkrete Bewertung der marktüblichen Tools und deren Anbieter bezüglich allgemein gültiger Datenschutz- und Datensicherheitsanforderungen. Hierbei berücksichtigen wir alle aktuellen Auslegungen von Gerichten und Datenschutzaufsichtsbehörden sowie die relevanten Hinweise aus der juristischen Literatur.
- Beurteilung der Datenschutz- und Verschlüsselungseinstellungen nach DSGVO-Konformität
- Vollständige Prüfung der Auftragsverarbeitungsverträge (AVV) der wichtigsten Anbieter für E-Signaturen, inklusive vollständiger Prüfberichte
- Erstellung von konkret einsetzbaren Datenschutzhinweisen/Datenschutzerklärungen für Anwender in deutscher und englischer Sprache.

Arbeitsrecht

- Individuell abgestimmte Betriebsvereinbarungen, Richtlinien und Arbeitsanweisungen

Lizenzrecht

- Unterstützung bei der Einbindung der Tools in die Lizenz- und IT-Landschaft Ihres Unternehmens
- Rechtliche Absicherung von Geschäftsgeheimnissen und Know-how gegenüber den Tool-Anbietern, wenn diese Zugriff auf die zu signierenden Dokumente benötigen
- Antworten auf Ihre weiteren IT-rechtlichen Fragen und zu lizenzvertraglichen Stolpersteinen bei der Einbindung der Tools in den Unternehmensalltag

Die einzelnen Bausteine bieten wir wahlweise planbar zu vorab vereinbarten Festpreisen oder individuell nach Aufwand an.

Kostentransparenz ist für uns in jedem Fall selbstverständlich.
Gerne unterstützen wir Sie effizient bei allen Fragen rund um das Thema digitale Signaturen in Ihrem Unternehmen. Sprechen Sie uns einfach an.
Weitere Informationen finden Sie in unserem Flyer.

Weiterführende Links
Grundlagen der elektronischen Signatur. Eine Broschüre vom Bundesamt für Sicherheit in der Informationstechnik.

Die Bundesnetzagentur stellt eine **Anbieterliste** elektronischer Vertrauensdienste zur Verfügung (Trusted List Browser)

Link zum **Trusted List Browser** der Europäischen Kommission mit allen **deutschen Anbietern**.

Ein Leitfaden zur Gesetzgebung und Durchsetzbarkeit von elektronischen Signaturen weltweit.

Links zu den beiden YouTube Videos von Stefan Schicker zu Digitalen Signaturen und Adobe: Video zu „Das Gesetz und die elektronische Signatur“ und „Die Risikobetrachtung der elektronischen Signatur“

Dr. Matthias Orthwein, München, m.orthwein@skwschwarz.de
Stefan C. Schicker, München, s.schicker@skwschwarz.de
Nikolai Schmidt, München, n.schmidt@skwschwarz.de
Yvonne Schäfer, Frankfurt/Main, y.schaefer@skwschwarz.de
Julian Westpfahl, Frankfurt/Main, j.westpfahl@skwschwarz.de

Vorsicht bei IT-Audits und eDiscovery: Dateinamen und Dateiendungen als Geschäftsgeheimnis

Das Bundesverwaltungsgericht (BVerwG) hat in einem kürzlich veröffentlichten Beschluss (BVerwG, Beschl. v. 5.3.2020, Az. 20 F 3/19) den Schutz von Geschäftsgeheimnissen auf die äußeren Merkmale von Dateien, in denen Geschäftsgeheimnisse gespeichert sind, ausgeweitet. Vor dem Zugriff unberechtigter Dritter geschützt sind nunmehr auch Merkmale wie Dateinamen, Dateiendungen, Dateitypen und Dateigrößen. Was auf den ersten Blick wie eine willkommene Stärkung des Geschäftsgeheimnisschutzes wirkt, stellt die Unternehmenspraxis aber vor neue Herausforderungen.

Nachdem der Schutz von Geschäftsgeheimnissen im deutschen Recht lange Zeit ein Schattendasein als Anhängsel des Gesetzes gegen den unlauteren Wettbewerb (UWG) gefristet hatte, wurde er in Umsetzung europäischer Vorgaben vom deutschen Gesetzgeber in 2019 mit dem Geschäftsgeheimnisgesetz (GeschGehG) auf eigene Füße gestellt.

Definition des Begriffs Geschäftsgeheimnis nach dem GeschGehG:

- Eine nicht allgemein bekannte Information, die nicht ohne weiteres zugänglich ist und daher einen wirtschaftlichen Wert hat,
- Berechtigtes Interesse des inhabenden Unternehmen an der Nichtverbreitung der Information, und
- Ergreifen angemessener Geheimhaltungsmaßnahmen.

Ausweitung des Schutzes von Geschäftsgeheimnissen auf die äußeren Merkmale von Dateien
Geschäftsgeheimnisse sind vor dem Zugriff unberechtigter Dritter geschützt, im digitalen Bereich also etwa der Zugriff auf den Inhalt einer vertraulichen Datei. Der Schutz gilt aber auch für solche Umstände, aus denen sich Geschäftsgeheimnisse nur indirekt ableiten lassen können. Hier setzt das BVerwG an und erklärte in einem softwarerechtlichen Kontext die äußeren Merkmale von Dateien, in denen Geschäftsgeheimnisse gespeichert sind, zu eben solchen Umständen. Danach können auch Dateinamen, Dateiendungen, Dateitypen und Dateigrößen als Geschäftsgeheimnisse vor dem Zugriff Dritter geschützt sein.

Bereits die Kenntnis von Dateinamen (und der dahinterstehenden Programmbibliotheken) erlaube einem Fachmann weitreichende Schlüsse auf das verwendete Know-how. Dies werde noch verstärkt, wenn sich anhand von Dateiendungen zum Beispiel die verwendete Programmiersprache erschließen lasse. Das könne bis zur vollständigen Offenlegung des Geschäftsgeheimnisses führen, je mehr Dateien offengelegt seien und sich die jeweiligen Informationen miteinander verknüpfen ließen. Insoweit seien auch Dateigrößen relevant, da sie in Kombination mit Dateinamen Hinweise auf den Aufwand der hinter einem Dateinamen stehenden Funktionalität liefern könnten.

Praxistipp: Welche Maßnahmen sollten Unternehmen ergreifen?
Was zunächst wie eine willkommene Stärkung des Geschäftsgeheimnisschutzes im Softwarebereich wirken mag, kann in der Unternehmenspraxis zu erheblichen Konsequenzen im Umgang mit Geschäftsgeheimnissen führen. Wer Geschäftsgeheimnisse verletzt, zum Beispiel indem er trotz bestehender Vertraulichkeitsvereinbarung Daten eines Vertragspartners im Rahmen gesetzlicher Auskunftsansprüche, vertraglicher Lizenzaudits oder mittels eDiscovery offenlegt, sieht sich Beseitigungs-, Unterlassungs- und Schadensersatzansprüchen gegenüber und macht sich eventuell sogar strafbar. In Zukunft werden Unternehmen daher nicht nur darauf achten müssen Dateiinhalte, sondern bereits die äußeren Umstände der Existenz einer Datei geheim zu halten. Wichtig ist ein umfassendes und effektives Management von Geschäftsgeheimnissen, von der Identifizierung der schützenswerten Informationen über sichere Verknüpfung mit ausreichenden Sicherungsmaßnahmen und aktuellen Vertraulichkeitsvereinbarungen bis zur regelmäßigen Schulung aller beteiligten Mitarbeiter im Unternehmen, die mit den Informationen in Berührung kommen.
SKW Schwarz unterstützt Sie gerne bei der Identifizierung schützenswerter Informationen nach den gesetzlichen Definitionen mit Hilfe unseres automatisierten LegalTech Tools (in Zusammenarbeit mit der SKW@Tech GmbH), beim Entwurf und der Überarbeitung von Vertraulichkeitsvereinbarungen nach den aktuellen gesetzlichen Anforderungen aber auch beim Umgang mit Auskunfts- und Auditverlangen Dritter, um Ihr Unternehmen vor der Falle der unbeabsichtigten Preisgabe fremder Geheimnisse zu schätzen. Für die Durchführung von Schulungen und Bereitstellung von Schulungsmaterial sind wir der richtige Partner für Sie.

Dr. Matthias Orthwein, München, m.orthwein@skwschwarz.de
Philipp Thomé, München, p.thome@skwschwarz.de

Schonzeit für Verantwortliche nach Einführung der DSGVO ist vorbei

Auch wenn derzeit sicherlich andere Themen für Unternehmen im Vordergrund stehen, dürfen datenschutzrechtliche Aspekte nicht außer Acht gelassen werden. Anfang Mai 2020 veröffentlichte der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (nachfolgend Landesbeauftragte) Informationen zu seiner Rolle, seinen Strategien und seinem Aktionsplan im Jahr 2020. Aus diesem ergibt sich, dass das Corona-Virus für die Aufsichtsbehörden keine „Ausrede“ für Fehler im Datenschutzmanagement ist.

Zunächst wird im "Konzept zur effektiven Durchsetzung des Datenschutzrechts" festgestellt, dass sich die Beschwerdebereitschaft der betroffenen Personen auf einem hohen Niveau stabilisiert hat. Insofern werden Datenschutzverstöße nicht nur durch anlasslose Kontrollen der Aufsichtsbehörden festgestellt, sondern vor allem durch Beschwerden. Beschwerden erreichten den Landesbeauftragten vor allem zu den Themen: (i) Weiterleitung von Daten an Dritte, (ii) Problemen bei der Auskunft nach Art. 15 DSGVO, (iii) Tracking-Maßnahmen auf Webseiten. (iv) Videoüberwachung und (v) Bewerbungsverfahren.

Der Landesbeauftragte kündigt an, dass das Jahr 2020 im „***Zeichen der konsequenten Beseitigung und Ahndung festgestellter Datenschutzverstöße***“ stehen wird. Die Behörde befindet sich

nunmehr in der Phase der konsequenten Anwendung der Abhilfebefugnisse und Sanktionsmaßnahmen. Defiziten wird je nach Schwere des Verstoßes, mit angemessenen Abhilfebefugnissen und Sanktionen zu begegnen sein, wobei die Instrumentarien des DSGVO vollständig ausgeschöpft werden können. Zurückhaltung sei aufgrund der bereits weit zurückliegenden Einführung der Verordnung nicht mehr geboten.

Neben der Prüfung von Beschwerden werden jedoch auch Kontrollen des Landesbeauftragen und seiner Behörde stattfinden. Diese sind im Aktionsplan 2020 festgehalten. Danach soll zum einen der Bereich ***Biometrie und automatisierte Kennzeichenlesesysteme*** im Fokus stehen. Einen weiteren Schwerpunkt bildet zusammen mit anderen Aufsichtsbehörden die Durchsetzung der Position der Datenschutzkonferenz im ***Bereich Tracking auf Webseiten***. Die Datenschutzkonferenz fordert hier eine Einwilligung der Webseitennutzer. Zudem werden zumindest in Rheinlandpfalz Versicherungsunternehmen und Banken sowie die Immobilienverwaltung und das Maklerwesen genauer geprüft.

Fazit:
Unternehmen sollten sich auf vermehrte Kontrollen der Aufsichtsbehörden einstellen. Die Schonzeit der letzten Jahre ist vorbei und Datenschutzverstöße werden rigoros verfolgt werden. Dazu trägt sicherlich auch das neue Bußgeldmodell bei, auf welches sich die Aufsichtsbehörden in Deutschland geeinigt haben. Mit Kontrollen durch die Aufsichtsbehörden ist insofern deutschlandweit zu rechnen. Aus dem Aktionsplan ergibt sich insofern, dass zumindest im Bereich des Tracking deutschlandweit zusammen gearbeitet werden wird. Andere Behörden setzen unter Umständen aber andere Schwerpunkte in ihren Kontrollen.

Franziska Ladiges, Frankfurt/Main, f.ladiges@skwschwarz.de

Neue Leitlinien des EDSA zur Cookie-Einwilligung auf Webseiten

Der Europäische Datenschutzausschuss (EDSA) hat am 5. Mai 2020 Leitlinien zum Umgang mit Einwilligungen unter der DS-GVO veröffentlicht. Ganz überwiegend orientiert sich der EDSA dabei an einem früheren Workingpaper der Art-29-Datenschutzgruppe. Dr. Oliver Hornung und Dr. Elisabeth von Finckenstein informieren.

Im Vorwort der Leitlinie wird festgehalten, dass mit dieser Aktualisierung insbesondere zu 2 Themen rechtliche Klarstellungen vorgenommen werden sollen:

- Die Gültigkeit der Einwilligung, die von der betroffenen Person bei der Interaktion mit sog. „Cookie-Walls“ gegeben wird;
- Die vermeintliche Einwilligung durch Scrollen auf einer Website.

Die Änderungen zum früheren Workingpaper der Art-29-Datenschutzgruppe betreffen im Wesentlichen die Änderungen der Leitlinie unter den Randnummern 38 bis 41 zum Oberbegriff der „Freiwilligkeit“ und Randnummer 86 zum Themenkomplex „eindeutige Angabe von Wünschen“.

Freiwilligkeit der Einwilligung
Ein besonderes Augenmerk legt der EDSA auf die Frage, wann eine Einwilligung als „freiwillig“ angesehen werden kann. Dabei verfolgt der EDSA ein sehr restriktives Verständnis. Jeder unangemessene Einfluss auf betroffene Personen bei der Abgabe der Einwilligung sei unzulässig. Beispielsweise dürfe eine App die Nutzung nicht von einer Einwilligung in die Erhebung und Nutzung von personenbezogenen Daten abhängig machen, die nicht für die App erforderlich sind.

Cookie-Walls
Auch zu sog. Cookie-Walls nimmt der EDSA Stellung. Als „Cookie-Wall“ wird ein Verfahren bezeichnet, das von Nutzenden eines Online-Angebots einfordert Cookies zu akzeptieren, um das Angebot nutzen zu können. Bei der Verwendung von Cookies werden personenbezogene Daten, wie etwa die IP-Adresse, verarbeitet. Zwar bedarf nicht jedes Setzen von Cookies einer Einwilligung (bspw. technisch notwendige Cookies), ist aber Tracking/Retargeting Zweck der zugrundeliegenden Verarbeitung, muss diese nach schon früher geäußerter Ansicht von Datenschutzbehörden vorher eingeholt werden. Diese Auffassung vertritt das BayLDA etwa auch hinsichtlich des Einsatzes von Google Analytics.

Der EDSA stellt fest, dass der Zugang zu einem Web-Service nicht von der Erlaubnis in das Setzen von Cookies abhängig gemacht werden darf. Hier fehle es an der Freiwilligkeit einer solchen Einwilligung, was auch bereits in Erwägungsgrund 43 der DS-GVO festgehalten wird.

Keine konkludenten Einwilligungen durch Scrollen
Die vermeintliche Einwilligung durch das bloße Nutzen einer Website oder das Scrollen, erfüllen nach der Auffassung des EDSA unter keinen Umständen das Erfordernis einer eindeutigen bestätigenden Handlung. Das ergibt sich bereits aus Erwägungsgrund 32 der DS-GVO, wonach die Einwilligung durch eine eindeutig bestätigende Handlung erfolgen sollte.

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit begrüßt die Leitlinie des EDSA
Als Mitglied des EDSA befürwortet der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Prof. Ulrich Kelber die aktuellen Leitlinien:
„Es gibt immer noch Internetseiten, die durch ihren Aufbau den Nutzenden Tracking aufdrängen. Die aktualisierten Leitlinien machen erneut deutlich, dass Einwilligungen nicht erzwungen werden können. Die meisten Cookie-Walls und die Annahme, dass das Weitersurfen eine Einwilligung bedeutet, widersprechen dem Aspekt der Freiwilligkeit und verstoßen gegen die Datenschutz-Grundverordnung. Ich wünsche mir, dass Verantwortliche daraus die richtigen Schlüsse ziehen und endlich datenschutzfreundliche Alternativen anbieten“.

Praxistipp
Die aktuelle Leitlinie des EDSA ist eine Zusammenfassung und Klarstellung zur Auslegung der DS-GVO durch die Aufsichtsbehörden und stellt keinen Paradigmenwechsel dar. Vielmehr werden Selbstverständlichkeiten festgehalten an die sich Betreiber von Webseiten zu halten haben.
Die aktuelle Leitlinie des EDSA bringt nochmals Klarheit in die Gestaltung von Cookie-Bannern und zeigt mit deutlichen Worten auf, dass Umgehungen der DS-GVO-Vorgaben datenschutzrechtlich unzulässig sind. Die in der aktuellen Leitlinie adressierten Themen „Cookie-Walls“ und „vermeintliche Einwilligung“ durch Nutzung/Scrollen auf einer Website stellen zwei häufig anzutreffende Ausgestaltungen dar bei denen Betreiber einer Website eine konkludente Einwilligung des Nutzers einholen, um das Tracking von Website-Nutzern datenschutzrechtlich zu legitimieren.
Es wird sich in naher Zukunft die Frage stellen, ob die aktuelle Leitlinie des EDSA zu deutlich mehr rechtskonformen Einwilligungen bei Aufruf einer Website führt. Nach wie vor sind viele Cookie-Banner mit Einwilligungslösungen datenschutzrechtlich unzulässig und beachten nicht die Vorgaben der europäischen und deutschen Datenschutzaufsichtsbehörden. Der Grund liegt möglicherweise auch darin, dass sich die Aufsichts- und Kontrolltätigkeit der Datenschutzaufsichtsbehörden bis 2019 auf die Beratung und Unterstützung von Unternehmen fokussiert haben. Damit wird aber 2020 Schluss sein. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hat am 5. Mai 2020 sein Konzept zur effektiven Durchsetzung des Datenschutzes und seinen Aktionsplan für das Jahr 2020 vorgestellt. Verstärkte stichprobenweise Prüfungen und Untersuchungen von Webseiten stehen auf dem Programm des LfDI Rheinland-Pfalz.
Es steht zu erwarten, dass auch andere Landesdatenschutzaufsichtsbehörden in Kürze einen Aktionsplan für das Jahr 2020 vorstellen. In einem gesonderten Beitrag werden wir das Konzept zur effektiven Durchsetzung des Datenschutzes in Rheinland-Pfalz und den Aktionsplan für 2020 vorstellen.

Dr. Oliver Hornung, Frankfurt/Main, o.hornung@skwschwarz.de
Dr. Elisabeth von Finckenstein, München, e.vonfinckenstein@skwschwarz.de

Plattformregulierung: EU gibt grünes Licht für Medienstaatsvertrag, der neben klassischen Medien viele Online-Geschäftsmodelle und Plattformen reguliert

Rundfunk und andere klassische Medien sind in Deutschland schon lange stark reguliert. Ein neuer Medienstaatsvertrag stellt jetzt umfassende Regel für viele weitere E-Commerce und Online-Plattformen auf, z.B. für App Stores, Suchmaschinen und sogar Sprachassistenten oder „Social Bots“. Maximilian König und Christoph Krück informieren.

Um was geht es beim neuen Medienstaatsvertrag?
Seit fünf Jahren arbeiten die Bundesländer an einer umfassenden Reform der deutschen Plattform- und Medienlandschaft: Dieses Jahr noch soll der neue „Medienstaatsvertrag“ in Kraft treten. Der alte

Rundfunkstaatsvertrag soll unter anderen an die technischen Entwicklungen angeglichen werden – und dabei wird sein Anwendungsbereich gleich erheblich erweitert.

Mehr Regulierung wird es für viele **Online-Geschäftsmodelle** und **Plattformen** geben, dateilweise weitreichende und komplizierte Transparenz- und Diskriminierungsverbote eingeführt werden. Die Algorithmen der Plattformen sollen gleichfalls transparenter werden. Und die Anforderungen an **Werbung im Internet** wurden teilweise auch neu justiert. Die Novelle dehnt aber z.B. auch den lizenzfreien Rundfunk aus. Dies könnte zu regulatorischen Erleichterungen bei **Live-Streams im Esport** führen.

EU-Kommission gibt grünes Licht - sieht aber Konflikte mit E-Commerce Richtlinie
Bis zuletzt wurde die Vereinbarkeit mit EU-Recht heftig diskutiert und dies wird wahrscheinlich auch noch so bleiben: Das Regelwerk sieht eine Anwendung auf Dienste vor, die „zur Nutzung in Deutschland bestimmt" sind. Da das Regelwerk somit auch für Dienste aus dem europäischen Ausland gelten soll, könnte dies im Konflikt mit dem **Herkunftslandprinzip** der E-Commerce Richtlinie stehen. Auch potenzielle Widersprüche mit den **Haftungsregeln** für Online-Plattformen wurden diskutiert.

Schlussendlich hatte die EU-Kommission im EU-Notifizierungsverfahren zwar Anmerkungen zu diesen Aspekten – über die Details berichten wir gerne, sobald diese verfügbar sind. Sie gab das Vorhaben aber Ende April frei, also steht dem Inkrafttreten in Deutschland zunächst nichts mehr im Weg.
Die Unterschriften der Ministerpräsidenten aller Bundesländer liegen laut einiger Medienberichte bereits vor. Jetzt müssen noch die Länderparlamente zuzustimmen. Das **Inkrafttreten** ist für **Herbst 2020** geplant.

EU plant weitere Regulierung von Online-Plattformen – „Digital Services Act"
In ihren Anmerkungen kritisiert die EU-Kommission das Vorhaben grenzüberschreitende Dienste durch nationale Regeln zu regulieren. Sie betont in diesem Zusammenhang erneut, dass auch sie eine Überarbeitung der Regeln für den E-Commerce und für Online-Plattformen plane: Bis Ende des Jahres solle ein entsprechendes Gesetzgebungspaket geschnürt werden – es handelt sich um den schon öfters angekündigten „**Digital Services Act**".

Maximilian König, München, m.koenig@skwschwarz.de
Christoph Krück, München, c.krueck@skwschwarz.de

Corona-Pandemie: Umgang mit Fristen beim Datenschutz

Für Maßnahmen zur Eindämmung der Corona-Pandemie gilt selbstverständlich, dass der Schutz der Bevölkerung Vorrang hat und andere Grundrechte – auch im Hinblick auf den Datenschutz – zum Teil eingeschränkt werden können. Auch wenn der Datenschutz aktuell nicht die Hauptsorge aller Beteiligten sein dürfte, sollten sowohl Unternehmen als auch deren Beschäftigte im Blick behalten, dass eine Einschränkung des Datenschutzes und der Datensicherheit nur möglich ist, wenn die Maßnahmen unbedingt erforderlich sind und auf die Dauer der Ausnahmesituation beschränkt bleiben.

Gesetzliche Fristen der DS-GVO gelten nach dem Meinungsbild der deutschen Datenschutzaufsichtsbehörden unverändert weiter (https://datenschutz-hamburg.de/assets/pdf/Corona-FAQ.pdf). Selbstverständlich haben betroffene Personen zum Beispiel auch in Zeiten von Covid-19 das Recht, vom Verantwortlichen binnen eines Monats Auskunft über zu ihrer Person gespeicherten personenbezogenen Daten zu erhalten. Eine Verlängerung nach Art. 12 Abs. 3 Satz 2 DS-GVO ist auch in Krisenzeiten nur dann möglich, wenn diese aufgrund der Komplexität und Anzahl von Anträgen erforderlich ist. Erfreulicherweise steht zum Beispiel der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit auf dem Standpunkt, dass Verstöße bei Überschreitung der gesetzlichen Fristen nicht verfolgt werden, wenn die Arbeitsfähigkeit des Verantwortlichen wegen der Corona-Krise nachweislich stark eingeschränkt ist. Im Zuge der Ermessensentscheidung der zuständigen Datenschutzaufsichtsbehörde wird es im Einzelfall entscheidend auf die Länge der Überschreitung sowie die Unternehmensgröße des verantwortlichen Unternehmens ankommen.

Selbstverständlich müssen auch in Krisenzeiten die Meldungen von Datenschutzverletzungen an die zuständige Datenschutzaufsichtsbehörde nach Art. 33 Abs. 1 DS-GVO unverzüglich und möglichst binnen 72 Stunden erfolgen. Pandemiebedingte Einschränkungen der Arbeitsfähigkeit bei Unternehmen können aber auch hier ggf. Berücksichtigung finden. Wichtig ist jedoch, dass auch bei Arbeiten im Home Office die Beschäftigten unverzüglich etwaige Datenschutzverletzungen an das Datenschutzteam des Unternehmens melden. Denn Kriminelle nutzen die aktuelle Ausnahmesituation für ihre Zwecke aus und Cyberattacken nehmen nahezu täglich weiter zu (https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html).

Praxistipp:
Für Arbeiten im Home Office sind Vorkehrungen zu treffen, die den Datenschutzrechten sowohl der Beschäftigten als auch anderer betroffener Personen – soweit wie möglich – Rechnung tragen. Dazu zählen Festlegungen zur Gewährleistung der Betroffenenrechte (z. B. auf Auskunft und Löschung) sowie die Meldung etwaiger Datenschutzverletzungen. Dazu dient die Sensibilisierung und möglichst schriftliche Verpflichtung der Beschäftigten zur Einhaltung der datenschutzrechtlichen Maßnahmen.

Dr. Oliver Hornung, Frankfurt/Main, o.hornung@skwschwarz.de

Verhandlung auf Distanz in Zeiten von #Corona? – Die Videokonferenz im Nachprüfungsverfahren

Die mündliche Verhandlung ist in allen Prozessordnungen im Grundsatz vorgesehen. Die Präsenz der Beteiligten, die Möglichkeit mündlicher Diskussion, der direkte Kontakt mit Zeugen und die über reinen Text und Sprache hinausgehende Kommunikation ermöglichen eine Interaktion, die oft den Ausgang eines Rechtsstreits beeinflusst. Es stellt sich die Frage, ob und wie in Nachprüfungsverfahren ggf. auf Distanz per Videokonferenz mündlich verhandelt werden kann.
weiterlesen auf vergabeblog.de

René M. Kieselmann, Berlin, r.kieselmann@skwschwarz.de