

Rechtssicher im Internet

Freitag, 02. Oktober 2020

IHK Regensburg

Referent: Rechtsanwalt Markus von Hohenhau

Fachanwalt für IT-Recht - Kanzlei für IT-Recht

www.e-anwalt.de

Markus v. Hohenhau

Rechtsanwalt

Fachanwalt für IT-Recht

Zertifizierter EU-Datenschutzspezialist

www.e-anwalt.de

Lehrbeauftragter an den Dr. Robert Eckert Schulen

Lehrbeauftragter an der TH Ingolstadt

Geschäftsführer der e-Data Protection GmbH

externer Datenschutzbeauftragter für verschiedene
Firmen und Vereine

Mitglied in der Gesellschaft für Datenschutz und
Datensicherheit e.V.



e-anwalt.de
Kanzlei für IT-Recht

e-DATA
Protection GmbH

GDD
Gesellschaft für Datenschutz
und Datensicherheit e.V.

Themen

- Wahl der richtigen Domain
- Was ist eine Abmahnung / Reaktionsmöglichkeiten
- Anbieterkennzeichnung / Impressum (Social Media, Geschäftsbriefe)
- Disclaimer
- Urheberrecht
- AGB - Fernabsatzgeschäft
- Grundlagen DSGVO
- Datenschutzerklärung
- Home-Office und Videokonferenzen (DSGVO)
- Fragen

Domain

Domains bei eigenem Webauftritt

Keine Markennamen! (Vorsicht bei Fantasienamen – Prüfung DPMA)

Kein Verstoß gegen das Namensrecht von Dritten

- *Mein Tipp:*

Überprüfung von eingetragenen Marken unter www.dpma.de und www.oami.europa.eu vor Registrierung

Domain soll so kurz wie möglich sein

Domain soll aussprechbar sein

Bindestrichdomains und andere Endungen ebenfalls registrieren

Abmahnung

Eine Abmahnung ist ein Vorwurf (per Post, Fax oder e-Mail, auch telefonisch) eines Konkurrenten oder eines Wettbewerbsverbandes, dass eine Rechtsverletzung vorliegt (z.B. Urheberrechtsverletzung, Verletzung des Markenrechts, Namensrechts, Wettbewerbsrechts – UWG) mit der Aufforderung das gerügte Verhalten zukünftig bei Androhung einer Vertragsstrafe zu unterlassen (strafbewehrte Unterlassungserklärung).

Die Frist zur Reaktion ist in der Regel sehr kurz (z.B. eine Woche, oftmals auch nur Tage).

Jede Abmahnung sollte ernst genommen werden, da erhebliche (finanzielle) Folgen drohen können.

Wie sollte ich auf eine Abmahnung reagieren

- Keine Reaktion (*nicht empfohlen*).
- Negative Feststellungsklage, d.h. Klage des Abgemahnten bei dem zuständigen Zivilgericht, mit dem Antrag gerichtlich feststellen zu lassen, dass keine Rechtsverletzung vorliegt und die Abmahnung unberechtigt war (nur dann empfehlenswert, wenn mit hoher Wahrscheinlichkeit kein Rechtsverstoß besteht).
- Abgabe einer, die Wiederholungsgefahr ausräumenden strafbewehrten Unterlassungserklärung (UE) und Zahlung der geltend gemachten (Rechtsanwalts-) Kosten.

Dies sollte nur nach Prüfung der Rechtmäßigkeit der Abmahnung und des Vorwurfs der Rechtsverletzung erfolgen. Oft geht die geforderte Unterlassungserklärung über den konkreten Rechtsverstoß hinaus. In diesen Fällen sollte eine sog. modifizierte Unterlassungserklärung abgegeben werden.

Sollte keine, die Wiederholungsgefahr ausräumende strafbewehrte Unterlassungserklärung abgegeben werden, kann der Abmahnende gerichtliche Schritte einleiten (diese kann er jederzeit, auch ohne Abmahnung einreichen, jedoch besteht dann die Gefahr, dass er bei einem sofortigen Anerkenntnis des Rechtsverletzers auf seinen Kosten sitzen bleibt).

Impressum

§ 5 Telemediengesetz (TMG)

- (1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene **Telemedien** folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:
1. den **Namen** und die **Anschrift**, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich die **Rechtsform**, den **Vertretungsberechtigten** (..)
 2. Angaben, die eine schnelle elektronische **Kontaktaufnahme und unmittelbare Kommunikation** mit ihnen ermöglichen, einschließlich der Adresse der **elektronischen Post**,
 3. soweit der Dienst im Rahmen einer Tätigkeit angeboten oder erbracht wird, die der behördlichen Zulassung bedarf, **Angaben zur zuständigen Aufsichtsbehörde**,
 4. das **Handelsregister**, Vereinsregister, Partnerschaftsregister oder Genossenschaftsregister, in das sie eingetragen sind, und die entsprechende Registernummer,
 5. (..)
 - a) die **Kammer**, welcher die Diensteanbieter angehören,
 - b) die **gesetzliche Berufsbezeichnung** und den **Staat**, in dem die Berufsbezeichnung verliehen worden ist,
 - c) die **Bezeichnung der berufsrechtlichen Regelungen** und dazu, wie diese zugänglich sind,
 6. in Fällen, in denen sie eine Umsatzsteueridentifikationsnummer nach § 27a des Umsatzsteuergesetzes oder eine Wirtschafts-Identifikationsnummer nach § 139c der Abgabenordnung besitzen, die Angabe dieser Nummer,
 7. (..)
- (2) Weitergehende Informationspflichten nach anderen Rechtsvorschriften bleiben unberührt (**DL-InfoV**)

Musterimpresum GmbH & Co KG

Verantwortlich für den Inhalt und Anbieterkennzeichnung nach § 5 TMG

Max Mustermann GmbH & Co KG

Musterstraße 1a

12345 Musterstadt

Tel: 0941-123456

Fax: 0941-123457

e-Mail: kontakt@mustershop-gewerbe.de

eingetragen im Handelsregister Registergericht Musterstadt HRA-Nr. xxxx

Persönlich haftende Gesellschafterin: Mustershop Verwaltungs GmbH

Geschäftsführer Max Mustermann und Eva Mustermann

Musterstraße 1a

12345 Musterstadt

eingetragen im Handelsregister Registergericht Musterstadt HRB-Nr. xxxx

(sofern vorhanden) UStIdNr. DE-xxxxxxx

Hinweis auf OS-Plattform und VSBG

Online-Streitbeilegung gemäß Art. 14 Abs. 1 ODR-VO: Die Europäische Kommission stellt eine Plattform zur Online-Streitbeilegung (OS) bereit, die Sie unter <http://ec.europa.eu/consumers/odr/> finden. Unsere e-Mail für Verbraucherbeschwerden lautet: xxxxx@xxxx.de

Zu einer Teilnahme an einem Schlichtungsverfahren nach VSBG sind wir nicht verpflichtet und können die Teilnahme an einem solchen Verfahren leider auch nicht anbieten.

Disclaimer

1. Haftungsbeschränkung

Die Inhalte des Internetauftritts wurden mit größtmöglicher Sorgfalt und nach bestem Gewissen erstellt. Dennoch übernimmt der Anbieter dieser Webseite keine Gewähr für die Aktualität, Vollständigkeit und Richtigkeit der bereitgestellten Seiten und Inhalte.

Als Diensteanbieter ist der Anbieter dieser Webseite gemäß § 7 Abs. 1 TMG für eigene Inhalte und bereitgestellte Informationen auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich; nach den §§ 8 bis 10 TMG jedoch nicht verpflichtet, die übermittelten oder gespeicherten fremden Informationen zu überwachen. Eine Entfernung oder Sperrung dieser Inhalte erfolgt umgehend ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung. Eine Haftung ist erst ab dem Zeitpunkt der Kenntniserlangung möglich.

2. Externe Links

Die Webseite enthält sog. „externe Links“ (Verlinkungen) zu anderen Webseiten, auf deren Inhalt der Anbieter der Webseite keinen Einfluss hat. Aus diesem Grund kann der Anbieter für diese Inhalte auch keine Gewähr übernehmen.

Für die Inhalte und Richtigkeit der bereitgestellten Informationen ist der jeweilige Anbieter der verlinkten Webseite verantwortlich. Zum Zeitpunkt der Verlinkung waren keine Rechtsverstöße erkennbar. Bei Bekanntwerden einer solchen Rechtsverletzung wird der Link umgehend entfernt.

3. Urheberrecht/Leistungsschutzrecht

Die auf dieser Webseite veröffentlichten Inhalte, Werke und bereitgestellten Informationen unterliegen dem deutschen Urheberrecht und Leistungsschutzrecht. Jede Art der Vervielfältigung, Bearbeitung, Verbreitung, Einspeicherung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedarf der vorherigen schriftlichen Zustimmung des jeweiligen Rechteinhabers. Das unerlaubte Kopieren/Speichern der bereitgestellten Informationen auf diesen Webseiten ist nicht gestattet und strafbar.

Urheberrecht – Lizenzverträge - Quellenangabe

Beispiel Pixelio: *Der Nutzer hat in für die jeweilige Verwendung üblichen Weise und soweit technisch möglich am Bild selbst oder am Seitenende PIXELIO und den Urheber mit seinem beim Upload des Bildes genannten Fotografennamen bei PIXELIO in folgender Form zu nennen: ‚© Fotografenname / PIXELIO‘ Bei Nutzung im Internet oder digitalen Medien muß zudem der Hinweis auf PIXELIO in Form eines Links zu www.pixelio.de erfolgen. Bei der isolierten Darstellung des Bildes durch direkten Aufruf der Bild-URL ist eine Urheberbenennung nicht erforderlich.*

Beispiel Fotolia:

Bitte beachten Sie, dass die Verwendung unserer Dateien für die folgenden Zwecke untersagt ist: · Pornografie · Erwachsenenunterhaltung oder Escort Services · Politische Unterstützung · Logos, Markenzeichen oder Dienstleistungsmarken.

Bitte beachten Sie auch, dass die Verwendung unserer Bilder in sozialen Netzwerken nur gestattet ist, wenn die Größe weniger als 1000 x 1000 Pixel beträgt und die Copyright-Information direkt im Bild erscheint.

Aus dem Standard-Lizenzvertrag mit Fotolia - <http://de.fotolia.com/Info/Agreements/StandardLicense>

"Mit Ausnahme der ausdrücklichen Genehmigungen in obigem Abschnitt 2 ist Ihnen Folgendes untersagt:

(..)Die redaktionelle Verwendung des Werks ohne zugehörigen Urheberrechtsvermerk; dieser Urheberrechtsvermerk muss jedoch nicht angebracht werden, wenn er nach geltendem Recht für die Nutzung des Werks in einer bestimmten Situation nicht erforderlich ist UND wenn die Anbringung des Urheberrechtsvermerks in der speziellen Situation nicht üblich ist."

AGB – Allgemeine Geschäftsbedingungen

- rechtlich richtig (nicht von anderen Seiten kopieren)
- so wenig Klauseln wie möglich, aber
- alle Pflichtangaben zum Fernabsatz – Art 246a ff EGBGB
- im Shop vor Abgabe der Bestellung wirksam einbezogen

Auswahl unzulässiger AGB Klauseln (Abmahngefahr)

- **“Angaben über die Lieferfristen sind unverbindlich, soweit nicht schriftlich zugesagt wurde.”** z.B. OLG Frankfurt, Urteil v. 10.11.2005, 1 U 127/05)
- **“Lieferzeit auf Anfrage”** - OLG Hamm, Urteil v. 17. 03.2009, 4 U 167/08
- **“Lieferzeit in der Regel”** - KG Berlin, Beschluss v. 03. 04.2007, 5 W 73/07
- **„unversicherter Versand“**
- **“Versand auf Risiko des Käufers”**
- **“Versand erfolgt mit versichertem Paket” oder “versicherter Versand”** - irreführend, da der Händler im Versandhandel mit Verbrauchern ohnehin das Versandrisiko trägt.

- **“Sollten gelieferte Artikel offensichtliche Material- oder Herstellungsfehler aufweisen, wozu auch Transportschäden gehören, so reklamieren Sie bitte solche Fehler sofort gegenüber uns oder dem Mitarbeiter von ... der die Artikel anliefert.”** - LG Frankfurt a.M., Urteil v. 09.03.2005, 2-02 O 341/04
- **"Rücksendung nur in Originalverpackung"**
- **“Die Gewährleistungsrechte erlöschen sechs Monate nach Lieferung.”**
- **"Die Haftung des Verkäufers aus jedem Rechtsgrund ist ausgeschlossen. Dies gilt nicht für Haftung wegen grober Fahrlässigkeit und Verschulden."**
- **"Die Parteien verpflichten sich für den Fall der Unwirksamkeit einer Bestimmung, sie durch eine andere zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt."** (Salvatorische Klausel)
- **"Es gilt deutsches Recht."** - OLG Oldenburg, Beschluss vom 23.09.2014 – 6 U 113/14 - unwirksam, sofern auch Verträge mit Verbrauchern geschlossen werden, die nicht in Deutschland ansässig sind.
- **"Ich bin einverstanden, dass mich [der Anbieter] auch telefonisch zu seinen Produkten und Dienstleistungen sowie weiteren Angeboten, die im Zusammenhang mit xyz stehen, informieren und beraten kann."**
- **„24 Monate Garantie auf dieses Produkt!“** - Verstoß gegen § 477 BGB

Widerrufsbelehrung / Muster Widerrufsformular



Bundesamt für Justiz

Das gesetzliche Muster zur
Widerrufsbelehrung verwenden - Anlage 1
(zu Artikel 246a § 1 Absatz 2 Satz 2
EGBGB) - http://www.gesetze-im-internet.de/bgbeg/art_249anlage_1.html

Muster eines Widerrufsformulars im Shop bereit stellen und mit Ware an den Kunden senden

Widerrufsbelehrung und Muster der Widerrufserklärung sowie AGB mit Ware an Kunden senden – Textform (vorab per e-Mail bei Bestellbestätigung)

[Zurück](#) [weiter](#)

[Nichtamtliches Inhaltsverzeichnis](#)

Einführungsgesetz zum Bürgerlichen Gesetzbuche
Anlage 1 (zu Artikel 246a § 1 Absatz 2 Satz 2)
Muster für die Widerrufsbelehrung bei außerhalb von Geschäftsräumen geschlossenen Verträgen und bei Fernabsatzverträgen mit Ausnahme von Verträgen über Finanzdienstleistungen
(Fundstelle: BGBI I 2013, S. 3663 – 3664)

Widerrufsbelehrung

Widerrufsrecht
Sie haben das Recht, binnen vierzehn Tagen ohne Angabe von Gründen diesen Vertrag zu widerrufen.
Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag ^[1].
Um Ihr Widerrufsrecht auszuüben, müssen Sie uns (^[2]) mittels einer eindeutigen Erklärung (z. B. ein mit der Post versandter Brief, Telefax oder E-Mail) über Ihren Entschluss, diesen Vertrag zu widerrufen, informieren. Sie können dafür das beigefugte Muster-Widerrufsformular verwenden, das jedoch nicht vorgeschrieben ist.^[3]
Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechts vor Ablauf der Widerrufsfrist absenden.

Folgen des Widerrufs
Wenn Sie diesen Vertrag widerrufen, haben wir Ihnen alle Zahlungen, die wir von Ihnen erhalten haben, einschließlich der Lieferkosten (mit Ausnahme der zusätzlichen Kosten, die sich daraus ergeben, dass Sie eine andere Art der Lieferung als die von uns angebotene, günstigste Standardlieferung gewählt haben), unverzüglich und spätestens binnen vierzehn Tagen ab dem Tag zurückzuzahlen, an dem die Mitteilung über Ihren Widerruf dieses Vertrags bei uns eingegangen ist. Für diese Rückzahlung verwenden wir dasselbe Zahlungsmittel, das Sie bei der ursprünglichen Transaktion eingesetzt haben, es sei denn, mit Ihnen wurde ausdrücklich etwas anderes vereinbart; in keinem Fall werden Ihnen wegen dieser Rückzahlung Entgelte berechnet.^[4]

Gestaltungshinweise:

[1] Fügen Sie einen der folgenden in Anführungszeichen gesetzten Textbausteine ein:

- a) im Falle eines Dienstleistungsvertrags oder eines Vertrags über die Lieferung von Wasser, Gas oder Strom, wenn sie nicht in einem begrenzten Volumen oder in einer bestimmten Menge zum Verkauf angeboten werden, von Fernwärme oder von digitalen Inhalten, die nicht auf einem körperlichen Datenträger geliefert werden: „des Vertragsabschluss“;
- b) im Falle eines Kaufvertrags: „an dem Sie oder ein von Ihnen benannter Dritter, der nicht der Beförderer ist, die Waren in Besitz genommen haben bzw. hat“;
- c) im Falle eines Vertrags über mehrere Waren, die der Verbraucher im Rahmen einer einheitlichen Bestellung bestellt hat und die getrennt geliefert werden: „an dem Sie oder ein von Ihnen benannter Dritter, der nicht der Beförderer ist, die letzte Ware in Besitz genommen haben bzw. hat“;
- d) im Falle eines Vertrags über die Lieferung einer Ware in mehreren Teillieferungen oder Stücken: „an dem Sie oder ein von Ihnen benannter Dritter, der nicht der Beförderer ist, die letzte Teillieferung oder das letzte Stück in Besitz genommen haben bzw. hat“;
- e) im Falle eines Vertrags zur regelmäßigen Lieferung von Waren über einen festgelegten Zeitraum hinweg: „an dem Sie oder ein von Ihnen benannter Dritter, der nicht der Beförderer ist, die erste Ware in Besitz genommen haben bzw. hat“.

[2] Fügen Sie Ihren Namen, Ihre Anschrift und, soweit verfügbar, Ihre Telefonnummer, Telefonnummer und E-Mail-Adresse ein.

[3] Wenn Sie dem Verbraucher die Wahl einräumen, die Information über seinen Widerruf des Vertrags auf Ihrer Webseite elektronisch auszufüllen und zu übermitteln, fügen Sie Folgendes ein: „Sie können das Muster-Widerrufsformular oder eine andere eindeutige Erklärung auch auf unserer Webseite (Internet-Adresse) elektronisch ausfüllen und übermitteln. Machen Sie von dieser Möglichkeit Gebrauch, so werden wir Ihnen unverzüglich (z. B. per E-Mail) eine Bestätigung über den Eingang eines solchen Widerrufs übermitteln.“

[4] Im Falle von Kaufverträgen, in denen Sie nicht angeboten haben, im Falle des Widerrufs die Waren selbst abzuholen, fügen Sie Folgendes ein: „Wir können die Rückzahlung verweigern, bis wir die Waren wieder zurückerhalten haben oder bis Sie den Nachweis erbracht haben, dass Sie die Waren zurückgesandt haben, je nachdem, welches der frühere Zeitpunkt ist.“

[5] Wenn der Verbraucher Waren im Zusammenhang mit dem Vertrag erhalten hat:

- a) Fügen Sie ein:
 - „Wir holen die Waren ab.“ oder
 - „Sie haben die Waren unverzüglich und in jedem Fall spätestens binnen vierzehn Tagen ab dem Tag, an dem Sie uns über den Widerruf dieses Vertrags unterrichten, an ... uns oder an [hier sind gegebenenfalls der Name und die Anschrift der von Ihnen zur Entgegennahme der Waren ermächtigten Person einzufügen] zurückzusenden oder zu übergeben. Die Frist ist gewahrt, wenn Sie die Waren vor Ablauf der Frist von vierzehn Tagen absenden.“
- b) fügen Sie ein:
 - „Wir tragen die Kosten der Rücksendung der Waren.“;
 - „Sie tragen die unmittelbaren Kosten der Rücksendung der Waren.“;
 - Wenn Sie bei einem Fernabsatzvertrag nicht anbieten, die Kosten der Rücksendung der Waren zu tragen, und die Waren aufgrund Ihrer Beschaffenheit nicht normal mit der Post zurückgesandt werden können: „Sie tragen die unmittelbaren Kosten der Rücksendung der Waren in Höhe von ... EUR [Betrag einfügen]“, oder, wenn die Kosten verhältnismäßig nicht im Voraus berechnet werden können: „Sie tragen die unmittelbaren Kosten der Rücksendung der Waren. Die Kosten werden auf höchstens etwa ... EUR [Betrag einfügen] geschätzt“; oder
 - Wenn die Waren bei einem außerhalb von Geschäftsräumen geschlossenen Vertrag aufgrund Ihrer Beschaffenheit nicht normal mit der Post zurückgesandt werden können und zum Zeitpunkt des Vertragsschlusses zur Wohnung des Verbrauchers geliefert worden sind: „Wir holen die Waren auf unsere Kosten ab.“ und
- c) fügen Sie ein: „Sie müssen für einen etwaigen Wertverlust der Waren nur aufkommen, wenn dieser Wertverlust auf einen zur Prüfung der Beschaffenheit, Eigenschaften und Funktionsweise der Waren nicht notwendigen Umgang mit ihnen zurückzuführen ist.“

[6] Im Falle eines Vertrags zur Erbringung von Dienstleistungen oder der Lieferung von Wasser, Gas oder Strom, wenn sie nicht in einem begrenzten Volumen oder in einer bestimmten Menge zum Verkauf angeboten werden, oder von Fernwärme fügen Sie Folgendes ein: „Haben Sie verlangt, dass die Dienstleistungen oder Lieferung von Wasser/Gas/Strom/Fernwärme (Unzutreffendes streichen) während der Widerrufsfrist beginnen soll, so haben Sie uns einen angemessenen Betrag zu zahlen, der dem Anteil der bis zu dem Zeitpunkt, zu dem Sie uns von der Ausübung des Widerrufsrechts hinsichtlich dieses Vertrags unterrichten, bereits erbrachten Dienstleistungen im Vergleich zum Gesamtumfang der im Vertrag vorgesehenen Dienstleistungen entspricht.“

[zum Seitenanfang](#) [Datenschutz](#) [Seite ausdrucken](#)

Weitere rechtliche Pflichtangaben

- **PreisangabenVO** – Preis inkl. Umsatzsteuer
- Bei Verkauf von Waren nach Gewicht/Länge/Fläche Angabe des Grundpreises - PreisangabenVO
- TextilkennzeichnungsVO
- ElektrogeräteG
- HeilmittelwerbeG
- Lebensmittel-Informationsverordnung (LMIV)
- FSK18 oder USK-Artikel (Computerspiele, Filme)
- Bei Lieferung in andere Länder außerhalb der EU Angabe über Steuern, Zölle und andere Abgaben
- Zusatzkosten bei Lieferung bei Nachnahme (Übermittlungsentgeld)

Checkliste Webshop

- Domain – kein Verstoß gegen Marken/Namensrecht
- Anbieterkennzeichnung (Impressum - § 5 TMG) vollständig - von allen Seiten erreichbar
- Datenschutzerklärung (Bonitätsüberprüfung, Cookies, soziale Medien, Newsletter, etc)
- Produktbeschreibungen vollständig (z.B. TextilkennzeichnungsVO, BatterieVO, etc)
- Produktbilder rechtlich einwandfrei
- Preisangaben vollständig und richtig
- Versandkosten und ev. Zusatzkosten vollständig vor Bestellvorgang mitgeteilt
- Lieferzeiten genau angeben
- Korrekturmöglichkeiten bei Bestellvorgang einräumen
- Alle Zahlungsmöglichkeiten vor Bestellvorgang vollständig genannt
- Button-Lösung beim Kauf (§ 312 j BGB) – „zahlungspflichtig bestellen“
- Widerrufsbelehrung (Muster Anlage 1 zu Artikel 246a EGBGB)
- AGB rechtlich korrekt und wirksam einbezogen
- e-Mail Bestätigung nach Eingang der Bestellung – Angaben vollständig
- Lieferung mit rechtlichen Texten in Schriftform (AGB, Widerrufsbelehrung/ -formular)

Einführung DSGVO

Die Datenschutz-Grundverordnung (DSGVO), englisch General Data Protection Regulation (GDPR), ist eine Verordnung der EU, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Die Datenschutz-Grundverordnung gilt als EU-Verordnung unmittelbar in allen EU-Mitgliedstaaten **seit dem 25. Mai 2018** ohne dass es einer weiteren gesetzlichen Umsetzung bedarf.

Viele Bereiche des Datenschutzes werden durch die DSGVO nicht neu geregelt und waren auch schon im „alten„ Bundesdatenschutzgesetz enthalten. Insbesondere bleibt der Begriff der „personenbezogenen Daten“ im Artikel 4 DSGVO weiterhin weit gefasst

<https://www.youtube.com/watch?v=gbRuzVwBoLY>

Datenschutzerklärung

§ 13 TMG - Pflichten des Diensteanbieters

- (1) Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten (..) in allgemein verständlicher Form zu unterrichten, (..)
- (2) Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten.
- (3) Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Art 12 DSGVO

Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, **in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln**; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. ²Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.

Checkliste Datenschutz (Mindestanforderung)

- Aktuelle Software verwenden
- Virens Scanner und Firewall (immer aktuell)
- Passwörter (*sind wie Unterwäsche. Du willst sie nicht jedem sehen lassen, musst sie regelmäßig wechseln und solltest sie nicht mit Fremden tauschen – einfaches umdrehen empfiehlt sich nicht*)
- Verpflichtungserklärungen für Mitarbeiter und Hilfskräfte
- Arbeitsplatzanweisungen (Verbot privater e-Mails und Surfen)
- Daten verschlüsseln – insbesondere auch bei tragbaren Computer, Mobiltelefone, USB-Sticks
- Sichtbarkeit von Daten auf Computern einschränken (Bildschirmschoner, Passwörter, USB-Anschlüsse sperren)
- Ab 10 Beschäftigten Datenschutzbeauftragten bestellen
- Sichere Verwahrung des Servers
- Regelmäßige Sicherungen durchführen (und überprüfen)
- Notfallkonzept für Datenausfall erstellen
- Keine persönlichen Daten am Telefon mitteilen (auf Anrede verzichten)
- Sichere Verwahrung der Patientenkarteien
- Sicheres Löschen / Vernichten von Akten und Daten (PCs nicht einfach wegwerfen)
- ADV mit allen Auftragsdatenverarbeitern (IT-Dienstleistern, Fax, Drucker, Datenvernichter, etc)
- Sensibilisierung der Mitarbeiter

Corona-Pandemie

Die wirtschaftlichen Folgen sind schon jetzt massiv und erfordern umsichtiges und flexibles Handeln.

Prävention:

- Notfallpläne
- Auslagerung einzelner Bereiche

Ausweichmöglichkeiten

- Einsatz von Fremdpersonal
- **Home Office(umgangssprachlich) - § 2 VII ArbStättV (Telearbeitsplätze) -**
https://www.gesetze-im-internet.de/arbst_ttv_2004/_2.html

Der Begriff „Homeoffice“ ist nicht definiert und wird als Oberbegriff für Telearbeit sowie sonstige Formen des mobilen Arbeitens verwendet.

Kein Anspruch auf Home-Office (bislang).

Kein einseitiges Anordnen durch AG möglich – nur mit Zustimmung des AN oder durch Kollektivvereinbarung

Mobiles Arbeiten – AG bestimmt in der Regel den Arbeitsplatz

§ 106 GewO - Weisungsrecht des Arbeitgebers

Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind. Dies gilt auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb.

Probleme: Überprüfung – Zutrittsrecht

Wegen der nach Art. 13 Grundgesetz garantierten Unverletzlichkeit der Wohnung hat der Arbeitgeber kein generelles Zugangsrecht zu Wohnungen von Beschäftigten. Deshalb bedarf es für den Zugang zur Wohnung einer wirksamen Einwilligung des/der Beschäftigten.

Home-Office

Durchführbarkeit:

Ist praktische Umsetzung gewährleistet?

Ausstattung der Mitarbeiter mit IT, Software Internet, Mobiltelefon

Rechtliche Grundlagen

Gibt es Home-Office Vereinbarungen?

Geheimnisschutz und DSGVO eingehalten?

Datenschutz

AG ist für die Sicherstellung der technischen und organisatorischen Maßnahmen verantwortlich
(Art 32 DSGVO)

Klare Vorgaben für AG notwendig

Sensibilisierung der AG z.B. durch Schulungen notwendig.

Folge bei Nichteinhaltung -> Datenschutzverstoß!

Stellungnahmen der Datenschutzbehörden

- <https://lfd.niedersachsen.de/startseite/themen/wirtschaft/hilfestellung-zum-datenschutz-im-homeoffice-191192.html>

- Sonderinformationen zum mobilen Arbeiten mit Privatgeräten zur Bewältigung der Corona-Pandemie - Übergang zum Regelbetrieb **nach Aufhebung des Katastrophenfalls** – BayLfD

Die Nutzung von Privatgeräten sowie von "Outlook on the web" (OWA) sind auf das vor Corona übliche Maß unter Beachtung der datenschutzrechtlichen Regelungen zu reduzieren. Sollte sich zeigen, dass die im Katastrophenfall verwendeten zusätzlichen Anwendungen, Dienste, Apps etc. auch für einen Regelbetrieb sinnvoll und notwendig sind, so sollte dies zukünftig über Dienstgeräte erfolgen.

*Sollen zukünftig , Messenger, Cloud-Dienste etc. genutzt werden, so ist **spätestens jetzt insbesondere zu prüfen**, welchen Schutzbedarf die übermittelten Daten haben, welche Risiken bestehen und welche technisch-organisatorischen Maßnahmen wie beispielsweise Ende-zu-Ende-Verschlüsselung hierbei erforderlich sind. Zudem sind Verfahren und Dienstleister zu verwenden, die den gesetzlichen Anforderungen insbesondere der Datenschutz-Grundverordnung genügen.*

Datenschutz zu Hause

Vor Ort muss ein **geeigneter Arbeitsplatz** gefunden werden, an dem Dokumente mit personenbezogenen Daten sicher aufbewahrt werden können. Empfehlenswert ist ein **eigener abschließbarer Raum**, der nach Feierabend oder in Pausen für Dritte nicht zugänglich ist. Ist das räumlich nicht möglich, sollten sämtliche Unterlagen zumindest in einem abschließbaren Schrank oder Rollcontainer aufbewahrt werden.

In jedem Fall ist bei der Heimarbeit darauf zu achten, dass sich **berufliche und private Daten nicht mischen** und keine unberechtigte Person Zugriff auf die dienstlichen Daten hat.

Sämtliche genutzten Geräte müssen daher über **einen geeigneten sicheren Passwortschutz** (z. B. starkes Passwort) oder ein anderes geeignetes Authentifizierungsverfahren (z.B. Token, Chipkarte; weitere Informationen in der Handlungsempfehlung sichere Authentifizierung) sowie verschlüsselte Speicher verfügen.

Bildschirme müssen so stehen, dass Unbefugte keinen Einblick nehmen können, ggf. kann ein sog. Blickschutzfilter nützlich sein.

Beim (auch kurzfristigen) Verlassen des Arbeitsplatzes müssen eine Bildschirmsperre (z. B. mittels **Bildschirmschoner**) und ein Passwort-/Authentifikationsschutz aktiviert werden.

An einem dienstlichen Gerät sollten überdies **keine private Hardware angeschlossen** werden (z. B. Tastaturen, USB-Sticks oder Festplatten), um das Infektionsrisiko mit Schadsoftware zu verringern.

Home-Office

Dienstliche Papierdokumente sollten zwischen Arbeitsstätte und Homeoffice in **verschlossenen Behältern transportiert** werden. Zudem dürfen sie **nicht im privaten Papiermüll entsorgt**, sondern nach den jeweiligen Bestimmungen des Unternehmens vernichtet werden. Steht am heimischen Arbeitsplatz etwa kein Schredder zur Verfügung, sind die Dokumente mit ins Büro zu nehmen und dort zu vernichten.

Telefonate und Videokonferenzen mit vertraulichem Inhalt sind so zu führen, dass **andere Haushaltsmitglieder, Besucher, Nachbarn oder andere unbefugte Personen den Inhalt des Gesprächs nicht wahrnehmen können**. Hierbei sind auch geöffnete Fenster zu berücksichtigen. Balkon, Terrasse oder Garten eignen sich grundsätzlich nicht für solche Gespräche.

Auch evtl. vorhandene **digitale Assistenten**, welche über Sprache reagieren, sollten **ausgeschaltet** bzw. entfernt werden.

Nutzung von Geräten des Arbeitgebers

Was ist datenschutzrechtlich zu beachten - TOM

- Vom Arbeitgeber bereitgestellte Endgeräte sollten ebenso zentral administriert und einer einheitlichen Policy unterworfen werden wie Endgeräte in der Betriebsstätte. Damit muss ein regelmäßiges Update- und Patchmanagement sichergestellt werden sowie regelmäßige Updates von Signaturen für die Endgeräte, d.h. aktuelles Betriebssystem, Virens Scanner, aktuelle Patches,
- Verschlüsselung von tragbaren IT-Systemen und Datenträgern,
- Zugriffs/Zutrittsschutz (Kinder, Ehepartner, Freunde, Katzen, etc)
- Bildschirmschoner mit Passwort,
- Schutz gegen Sicht von Außen – Bildschirmfolien, nicht einsehbarer Bildschirm
- Schutz von sichtbaren Dokumenten
- Zugriff auf Firmen IT über VPN, verschlüsseltes WLAN, etc WiFi-Zugänge müssen mit einem sicheren Passwort abgesichert sein.
- Datenspeicherung und Datensicherung – besser nicht auf Arbeitsplatz
- Kein Anschluss privater Geräte – Drucker, USB-Sticks
- Entsorgung vertraulicher Dokumente und Daten nicht über den Hausmüll
- Bei dienstlichen Smartphones sollte eine PIN-Sperre erzwungen werden.
- Gehen mobile Endgeräte verloren, müssen Sofortmaßnahmen ergriffen werden: z. B. Remote Wipe (Löschung) bei Smartphones, Sperrung von Hardware-Token.
- Verlust, Datenpannen, sonstige Datenschutzverstöße sind sofort zu melden!

Nutzung von Geräten des Arbeitnehmer – bring your own device

In der Regel sollte auf die Nutzung privater Endgeräte verzichtet werden, da erhöhte Gefahr der Vermischung privater und beruflicher Daten.

Arbeitgeber können nicht die Nutzung privater Endgeräte für die Erbringung der Arbeitsleistung verlangen. Jedoch ist diese mit Einwilligung der Beschäftigten möglich. Allerdings muss der Arbeitgeber (IT-Abteilung) vor einer Nutzung von Privatgeräten prüfen, ob das Schutzniveau bei dieser Verarbeitung angemessen ist.

Falls es die in einer Risikoanalyse ermittelten Restrisiken tragbar erscheinen lassen, ausnahmsweise Daten an einem privaten Computer zu verarbeiten, sollte hierfür zumindest ein extra Konto eingerichtet und die Daten in einem verschlüsselten Bereich gesondert gespeichert werden.

Sobald die Daten auf dem dienstlichen Server abgelegt worden sind, sind sie auf dem Privat-PC unwiederbringlich zu löschen. Hierfür reicht es nicht aus, wenn sie lediglich in den Papierkorb verschoben werden.

Besonders sensible Daten Dritter (z. B. Gesundheitsdaten, Daten zu politischen oder weltanschaulichen Ansichten, vgl. Art. 9 DS-GVO) **dürfen nicht auf privaten Geräten verarbeitet werden.**

Nutzung von Geräten des Arbeitnehmer – bring your own device

Soweit möglich nicht gestatten

Falls nicht anders möglich:

- Nur Zugriff auf Unternehmensserver/Cloud – nur über sichere Verbindung (VPN)
- Trennung von privaten und beruflichen Daten (Container)
- Kein Weiterleiten von beruflichen e-Mails auf private e-Mail Adressen
- Sicheres Löschen nach Übertragung auf Firmen-Server

Problem: Lizenz von Software – private Lizenzen verbieten oftmals gewerbliche Nutzung

Weitere Infos – Datenschutzrechtliche Regelungen bei Homeoffice - Best-Practice-Prüfkriterien des BayLDA

- https://www.lda.bayern.de/media/best_practise_homeoffice_baylda.pdf
- <https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf>
- <https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html>
- https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/HomeOffice/homeoffice_node.html

Home-Office

Vorsicht vor **Phishing-Mails** und **Fake-Mails** welche die aktuelle Situation ausnutzen

Wie schützt man sich gegen Phishing?

https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/Schutzmassnamen/schutzmassnamen_node.html

Drei Sekunden für mehr E-Mail-Sicherheit

Video unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/E-Mail/E-Mail_node.html

weitere Beispiele unter

<https://www.kaspersky.de/blog/coronavirus-phishing/22112/>

Frage: Private Nutzung der IT?

Videokonferenzen

Videokonferenz nur wo notwendig einsetzen

- Wahl einer Telefonkonferenz anstatt einer Videokonferenz, wenn es keinen Mehrwert hat, dass sich die Teilnehmer zusätzlich sehen können
- Handschriftliche Protokolle oder das notieren von Rückfragen anstatt Videoaufzeichnungen

Sorgfältige Auswahl des Anbieters der Videokonferenz

Die Lösungen bei Videokonferenzen unterscheiden sich oft in Bezug auf ihre Anforderungen an die technische Infrastruktur bei Unternehmen und Beschäftigten. So existieren sogenannte Peer-to-peer-Lösungen (P2P) wie z.B. Jitsi und zentrale Lösungen wie bspw. Zoom.

Während **zentrale Lösungen** die eigene Infrastruktur belasten, belasten P2P-Lösungen die Infrastruktur bei den Beschäftigten im Home-Office (Internetanschluss).

Bei einer **P2P-Kommunikation** läuft nur der Verbindungsaufbau über die zentrale Infrastruktur, die eigentliche inhaltliche Kommunikation läuft direkt zwischen den Kommunikationsteilnehmern.

Eine P2P-Lösung entlastet den Internetzugang des Unternehmens, verlangt jedoch im Gegenzug mehr Bandbreite bei den Beschäftigten.

Videokonferenzen

Bei der Auswahl eines geeigneten und zuverlässigen Anbieters sollten Dienste mit möglichst **datensparsamen Voreinstellungen** bzw. Einstellungsmöglichkeiten („Privacy by Default“) und datenschutzfreundlicher Technikgestaltung („Privacy by Design“) gewählt werden, z.B. eine Deaktivierung der Erhebung von Statistikdaten, Senden von Absturzberichten oder automatischer Transkriptionen.

Nur verschlüsselte Übertragung - bestenfalls Ende-zu-Ende verschlüsselt.

Freigaben nur mit Zustimmung: Bildschirmübertragungen (Screen-Sharing/Desktop-Sharing) oder Aufzeichnungen sollten technisch nur möglich sein, wenn die Teilnehmer vorher aktiv zustimmen können.

Löschung von Protokollen und Aufzeichnungen: Aufzeichnungen, Chatverläufe, Transkripte oder ausgetauschte Dateien sollten nach Gesprächsende gelöscht werden können bzw. nur so lange gespeichert werden, wie erforderlich, ggf. sollten entsprechende Löschfristen gesetzt werden können.

Videokonferenzen

Zugangsbeschränkungen: Videokonferenzen dürfen nicht für jedermann zugänglich sein, es bedarf einer Login-Funktion bzw. der Zustimmung des Organisators, damit nur Berechtigte an der Videokonferenz teilnehmen können und ein Datenabfluss verhindert wird.

Blurr-Möglichkeiten: Videokonferenz-Tools sollten die Möglichkeit bieten, den Hintergrund auszugrauen bzw. unkenntlich zu machen.

Tipp

Entfernen Sie alle Objekte aus dem Hintergrund, die die Kommunikationspartner nicht sehen sollen. Achten Sie auch auf herumliegende Dokumente.

Eine Dia-Stativ-Leinwand oder ein Leintuch schafft als Sichtschutz einen neutralen Hintergrund.

Videokonferenzen

Auftragsverarbeitungsvertrag - immer wenn ein Verantwortlicher Videokonferenzlösungen nicht auf eigener IT-Infrastruktur erbringt, sondern sich eines Dritten bedient (SaaS-Anbieters oder anderen Dienstleister), muss geprüft werden, ob es eines Abschluss eines Vertrags zur Auftragsverarbeitung gem. Art. 28 DS-GVO oder eines Vertrags zur Regelung einer gemeinsamen Verantwortlichkeit gem. Art. 26 DS-GVO bedarf.

Der Verantwortliche ist bei der Auftragsverarbeitung als auch bei der gemeinsamen Verantwortlichkeit für die Einhaltung der in der DSGVO vorgesehenen technischen und organisatorischen Maßnahmen verantwortlich.

Erbringt ein Anbieter die Dienstleistung aus einem **Drittland** heraus und findet eine Datenübermittlung in eines statt (Länder außerhalb der EU/des EWR), dann muss der Verantwortliche sicherstellen, dass das Datenschutzniveau in diesen Ländern den Vorgaben der DS-GVO nach Art. 44 DS-GVO entspricht.

Angemessenheitsbeschluss gem. Art. 45 DS-GVO garantiert ein entsprechendes Datenschutzniveau.

Angemessenheitsbeschlüsse existieren z.B. für die Schweiz, Argentinien,

die Faröer Inseln, Japan und Kanada (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)

Problem: EU-US-Privacy Shield-Abkommen

Mit seinem Urteil vom 16. Juli 2020 (C-311/18 - "Schrems II"-) hat der Europäische Gerichtshof (EuGH) das EU-US Privacy Shield für unwirksam erklärt.

Für den Datenaustausch mit den USA müssen jetzt besondere Schutzmaßnahmen ergriffen werden. Unternehmen und Behörden können Daten nicht mehr auf der Grundlage des Privacy Shield übermitteln, das der EuGH für unwirksam erklärt hat.

Übersicht der Videokonferenztools unter (.xls)

https://www.gdd.de/downloads/praxishilfen/ph_video_konferenzsysteme_aktuelle-tabelle/at_download/file

Cloudflare
Facebook
Twitter
Instagram
Tumblr
LinkedIn
Pinterest
Google Analytics
WordPress
Stats
Google Ads
Google AdSense
Google Remarketing
Google Conversion Tracking
Google Doubleclick
Facebook Pixel
MailChimp
ActiveCampaign
YouTube
SoundCloud
Spotify
Zoom
Skype for Business
GoToMeeting
Microsoft Teams
Google Hangouts
Google Meet
Google Web Fonts
Adobe Fonts
Google Maps
Google reCAPTCHA
Amazon Partnerprogramm

EU-US-Privacy Shield-Abkommen

Der Europäische Datenschutzausschuss (EDSA) – das gemeinsame Gremium europäischer Datenschutzaufsichtsbehörden – hat eine Task Force ins Leben gerufen, die sich mit den zahlreichen Beschwerden, die nach dem „Schrems II“-Urteil (C-311/18) eingereicht wurden, befassen. Die Task Force will weiterhin Handlungsempfehlungen ausarbeiten, wie Datenexporteure zusätzliche Maßnahmen (z.B. rechtlicher, technischer und organisatorischer Natur) ergreifen können, um den rechtlichen Anforderungen der DSGVO bei Datenübermittlungen in Drittländer zu genügen.

Der EDSA betont jedoch zugleich, dass „die Auswirkungen des Urteils weitreichend, und die Umstände der Datenübermittlung in Drittländer sehr unterschiedlich sind. Es kann deshalb keine „Patentlösung“ geben, die allen Datenübermittlungen gleichermaßen gerecht wird. Jeder Datenexporteur muss vielmehr seine eigenen Datenverarbeitungsvorgänge und Datenübermittlungen bewerten und daraufhin geeignete Maßnahmen ergreifen“.

Es besteht deshalb kaum Hoffnung, dass in naher Zukunft eine einheitliche und praktikable Lösung geben wird um mit möglichst wenig administrativen Aufwand personenbezogene Daten in unsichere Drittländer, wie z.B. die USA, zu exportieren.

EU-US-Privacy Shield-Abkommen

1. Stellungnahme des LfDI Baden-Württemberg - Orientierungshilfe „Was jetzt in Sachen internationaler Datentransfer?“

Zusammenfassend empfiehlt der LfDI:

Internationale Datenübermittlungen auf Grundlage von Standardvertragsklauseln (sog. Standard Contractual Clauses = SCC) sind weiterhin denkbar, allerdings müssen bei Datenübermittlungen in die USA zusätzliche Maßnahmen ergriffen werden, wie z.B. die Verschlüsselung, die von US-Geheimdiensten nicht außer Kraft gesetzt werden kann, oder die Anonymisierung sämtlicher personenbezogener Daten. Der LfDI betont jedoch selbst, dass die vorgeschlagenen Maßnahmen wohl nur in wenigen Fallkonstellationen in Betracht kommen und daher wohl keine effektive Lösung darstellen können.

Als Alternative zu den SCC sollen verbindliche interne Datenschutzvorschriften gem. Art. 47 DSGVO (sog. Binding Corporate Rules) in Erwägung gezogen werden. Wobei – wie im Falle von SCC – zusätzliche Garantien erforderlich sein können.

Fehlt es an wirksamen Garantien – wie z.B. bei Datenübermittlungen in die USA – sollten Datenexporteure, um „wenigstens Ihren Willen zu rechtskonformem Handeln zu demonstrieren und zu dokumentieren“, Kontakt mit dem jeweiligen Datenimporteur aufnehmen und sich über effektive Ergänzungen zu den SCC verständigen, die in einer gesonderten Vereinbarung, z.B. einem Data Processing Addendum, festgehalten werden.

Videokonferenzen

Technisch-organisatorische Maßnahmen (TOM)

„**Härtung der eingesetzten IT-Systeme**“: z.B. Dateitrennung, aktueller Virens Scanner, Zugangssicherungen, aktuelle Softwareupdates des Betriebssystems und des Konferenztools.

Desktop-Sharing: Sofern überhaupt erforderlich, sollte auf dem Desktop **nur das angezeigt werden, was für die Besprechung erforderlich ist**. Es ist möglich bei Verwendung von mehreren Monitoren nicht den Hauptbildschirm auszuwählen oder unter Windows 10 Desktopsymbole auszublenden.

Schließen Sie Mail- und Messenger-Programme, damit nicht versehentlich Einblick in Kontaktdaten und/oder Nachrichten gegeben wird. So wird auch verhindert, dass immer wieder *“Neue Nachricht”*-Popups erscheinen.

keine **Geschäftsunterlagen erkennbar** liegen lassen.

Black- oder Whitelists: Wann und für welche Zwecke dürfen Anwendungsfunktionen durch den Benutzer verwendet werden. Welche Dateien dürfen empfangen/freigegeben werden.

Weitere Informationen:

Berliner BDI

[Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten \(mit Ampelschema\) \(03. Juli 2020\)](#)

[Durchführung von Video-konferenzen während der Kontaktbeschränkungen \(v. 1.1 v. 22. Mai 2020\)](#)

ULD Schleswig-Holstein

[Datenschutz: Plötzlich Videokonferenzen – und nun? \(29.04 2020\)](#)

[Nutzung von Messenger- und Videokonferenzdiensten in Zeiten der Corona-Pandemie \(April 2020\)](#)

BfDI

[Leitfragen zur Beurteilung von Angeboten \(April 2020\)](#)

[Telearbeit und Mobiles Arbeiten - Ein Datenschutz-Wegweiser \(Januar 2019\)](#)

LDI NRW

[Leitplanken für die Auswahl von Videokonferenzsystemen während der Kontaktbeschränkungen aufgrund der Corona-Pandemie \(18. Mai 2020\)](#)

[Leitplanken für die Auswahl von Messenger-Diensten während der Kontaktbeschränkungen aufgrund der Corona-Pandemie \(18. Mai 2020\)](#)

Vielen Dank für Ihre Aufmerksamkeit

Rechtsanwalt Markus v. Hohenhau
Fachanwalt für Informationstechnologierecht
Dachauplatz 8
93047 Regensburg
Tel: 0941-56712005
info@e-anwalt.de

e-anwalt.de
Kanzlei für IT-Recht