Checkliste

Ist – Zustand Analyse:

- Werden personenbezogene Daten (pseudonymisierte Daten) iSd DSGVO verarbeitet?
- Welche Prozesse der Datenverarbeitung finden statt?
- AGBs, Datenschutzerklärungen, Impressum, Vertrage, Website,…
- Einwilligungserklärungen vorhanden?
- Verarbeitung sensibler Daten?
- Informationspflichten werden erfüllt?
- Bestehen Dokumentationspflichten?
- Vorkehrungen bei Datenschutzverletzungen?
- Welche Auftragsverarbeiter werden eingesetzt?

Erkenntnisgewinn

- Welche Maßnahmen sind durchzuführen?
- Ist eine Datenschutz-Folgenabschätzung durchzuführen?
- Ist ein Datenschutzbeauftragter zu bestellen?
- Verträge mit Auftragsverarbeitern (Muster WKÖ)
- Sicherstellung der Rechtmäßigkeit der Datenübermittlung in Drittländer
- Nachweis der DSGVO-konformen Datenverarbeitung
- Erstellung eines Verarbeitungsverzeichnisses auf Basis teilweise vorbefülltes Muster WKÖ
- Sicherstellung der Einhaltung der Verpflichtungen zur fristgerechten Erfüllung der Betroffenenrechte
- Prozess für Data Breach Meldung einführen

FAQ zur DSGVO neu – Fachgruppe Buch- und Medienwirtschaft

Folgende Fragen betreffen die Rechtslage ab dem 25.05.2018

1.	Ein Unternehmen A hat in der Vergangenheit eigene Kunden (zB Buchkäufer), die beim Geschäftsabschluss ihre E-Mail-Adresse benutzt haben, automatisch in den Verteiler des regelmäßigen (kostenlosen) elektronischen Newsletter-Verteiler aufgenommen (informiert ca. alle 3 Wochen über neue Produkte des Unternehmen A). Dieser Newsletter hatte jedes Mal ein rechtskonformes Impressum und eine Abmeldemöglichkeit. Von dieser hat der Kunde nie Gebrauch gemacht.	Gemäß Art. 6 DSGVO ist die Verarbeitung von Daten nur dann zulässig, wenn der Betroffene (in diesem Fall der Kunde) seine Einwilligung ausdrücklich erklärt hat. Für künftige Aufnahmen in den Verteiler empfiehlt es sich daher eine Erklärung einzuholen, in der er sich einverstanden erklärt, regelmäßig bis auf Widerruf den Newsletter des Unternehmens zu erhalten. Bei eigenen Kunden kann jedoch alternativ ein Newsletterversand auch auf § 107 TKG gestützt werden, sofern die nachstehenden Voraussetzungen erfüllt sind (und im Beanstandungsfall auch nachgewiesen werden können): Gemäß § 107 TKG ist eine vorherige Zustimmung für die Zusendung elektronischer Post dann nicht notwendig, wenn 1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und 2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und 3. der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und 4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat. Diese Rechtsgrundlage gilt für eigene Kunden grundsätzlich weiter. Bei Nichtkunden ist eine vorherige Einwilligung erforderlich.
a.	Darf das Unternehmen diese Kunden ab dem 25.5.2018 weiter mit e-Newsletters beschicken, ohne eine ausdrückliche Einwilligung des Kunden dazu dokumentieren zu können?	Siehe Frage 1. Als Ausnahme ist eine Zusendung ohne Einwilligung dann zulässig, wenn: • Der Absender die Kontaktinformation von seinem Kunden erhalten hat • Die Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt • Dem Empfänger bei der Erhebung seiner E-Mail-Adresse und in jeder Werbe-E-Mail eine kostenlose Opt-Out-Möglichkeit geboten wird und • Der Empfänger die Zusendung nicht von Vornherein durch Eintragung in eine von der Behörde (RTR) geführten Liste abgelehnt hat
b.	Wenn Anfragen oder Beschwerden deswegen kommen, auf welche Rechtsgrundlage darf sich Unternehmen A beziehen?	§ 107 TKG, gilt für B2C und B2B genauso. Empfehlenswert ist aber, schon aus Beweisgründen nach und nach auf Newsletterversand mit vorheriger Einwilligung umzustellen (Einwilligungserklärung bei Datenerhebung).

c.	Wird es in absehbarer Zeit eine Novelle oder einen Ersatz zB des TKG geben, um Kollisionen mit dem Datenschutz zu vermeiden?	Eine Kollision besteht nicht, die Einwilligung ist nicht immer zwingend notwendig, nationale Rechtsvorschriften als Verarbeitungsgrundlage sind zulässig. Bei nicht-sensiblen Daten kommen als Rechtsgrundlage der Datenverarbeitung zudem auch berechtigte Interessen des Verantwortlichen in Betracht.
d.	Besseres Nutzen von Facebook	Siehe Antwort zu Frage 15
2.	Wer ist verantwortlich für die Einhaltung der DSGVO?	Grundsätzlich tragen mehrere Beteiligte die Verantwortung für die Einhaltung der DSGVO, wenn auch in unterschiedlichem Ausmaß. Man unterscheidet: • Verantwortlicher: jene natürliche oder juristische Person, die Zwecke und Mittel der Verarbeitung allein oder gemeinsam mit anderen Personen entscheidet. • Auftragsverarbeiter: jene Person, die im Auftrag des Verantwortlichen personenbezogene Daten bearbeitet. Der Verantwortliche ist grundsätzlich für den gesamten Datenverarbeitungsvorgang verantwortlich. Es besteht eine Nachweispflicht über die sich aus der DSGVO ergebenen Pflichten. Auch durch die Bestellung eines Auftragsverarbeiters kann die Verantwortung nicht abgegeben werden.
3.	Ab wann brauche ich einen Datenschutzbeauftragten?	Die Bestellung eines Datenschutzbeauftragten ist verpflichtend, wenn: • Die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht. Diese müssen aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von den betroffenen Personen erforderlich machen. (als Beispiele werden z.B. Banken, Versicherungen, Berufsdetektive… genannt) • Die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilung oder Straftaten besteht (z.B. Krankenhaus) All diese Fälle sind bei der bloßen Verarbeitung von nicht sensiblen Kundendaten im Buchhandel nicht gegeben. Vorsicht ist jedoch geboten, sobald die "Interessensgebiete" der KundInnen verarbeitet werden sollen, die ins Private hineinreichen.
4.	Müssen die Bildschirme jetzt vom Kunden weggedreht werden?	Der Verantwortliche hat für die Einhaltung der Datenschutzbestimmungen zu sorgen. Er hat in seinem Betrieb geeignete Maßnahmen zu ergreifen um diese Bestimmungen einhalten zu können. Intern ist deshalb dafür Sorge zu tragen, dass Daten nicht nach Außen gelangen. Somit dürfen Bildschirme, an denen personenbezogene Daten verarbeitet werden, nicht vom Kunden einsehbar sein. Insbesondere gilt dies, wenn Gefahr besteht, dass der/die KundIn Daten einer anderen natürlichen Person einsehen könnte. Statt wegdrehen können Sie aber auch (wie in Apotheken) einen "Sicherheitsabstand" einführen oder eine Schutzfolie am Display anbringen, die Einsicht verhindern kann.

5.	Wem muss ich Auskunft erteilen und wie überprüfe ich den Anfrager? Darf ich den Personalausweis verlangen?	Auskünfte müssen an jede betroffene Person erteilt werden. Betroffen ist eine Person, sobald sie Auskunft verlangt. Der Antrag kann formlos gestellt werden, allenfalls sogar mündlich. Bestehen berechtigte Zweifel über die Identität der Person (nicht zuordenbare E-Mail Anfrage, Telefonanruf, …) kann der Verantwortliche verlangen, dass die Identität nachgewiesen werden muss. Somit kann auch ein Ausweis als Beweis verlangt werden. Eine Beauskunftung ohne Identitätsfeststellung könnte ansonsten wiederum ein Datenschutzverstoß sein.
6.	Wo beginnt Datamining? Stichworte Google Analytics, Piwik und Kundenkategorisierung (Schlagworte)	Die DSGVO kennt den Begriff "Data Mining" nicht. Verfahren zur Analyse und Prognose werden unter dem Begriff Profiling verwendet. (Art. 4 Z. 4 DSGVO) Dies bezeichnet jede Art der automatisierten Verarbeitung und Bewertung personenbezogener Daten zur Analyse oder Vorhersagung von Arbeitsleistung, wirtschaftlicher Lage, persönlicher Vorlieben, Interessen, usw. Art 22 DSGVO beschränkt "ausschließlich automatisches" Profiling, durch das für Betroffene eine rechtliche Wirkung entstünde oder sie in „ähnlicher Weise erheblich beeinträchtigt" würden (zB wenn ihnen anhand ihrer Interessen beim Online-Shopping andere Preise angezeigt würden). Hier sind Einwilligung (Art. 22 Abs 2), erhöhte Informationsvoraussetzungen (Art. 13 und 14) und Anforderungen an den "nicht diskriminierenden Algorithmus" (Erwägungsgrund 71) zu beachten. Relevant hierbei ist vor allem, dass es sich um eine erlaubnisbedürftige Kategorie handelt. Das bedeutet, dass eine generelle und unkonkrete Einwilligung die Anwendung einer derartigen Verarbeitungsmethode nicht deckt.
7.	Muss ich die Einwilligungserklärungen in der WWS hinterlegen bzw. wie hat das zu erfolgen?	Einwilligungserklärungen müssen nachweisbar sein. Es kommt nicht darauf an, ob diese schriftlich oder mündlich erteilt werden. In welcher Form eine Dokumentation der Einwilligungserklärung erfolgen muss sieht das Gesetz nicht vor. Aus Beweisgründen ist aber Schriftlichkeit empfehlenswert und eine Ablage in einer Art und Weise, dass die zugehörige Einwilligung bzw. Rechtsgrundlage der Datenverarbeitung leicht aufgefunden werden kann.
8.	Dürfen meine Daten nur in der EU gespeichert werden?	Sollen Daten in ein außerhalb der EU befindliches Land übermittelt und in der Folge dort gespeichert werden, müssen folgende Voraussetzungen vorliegen: • Bereits die Datenverarbeitung im Inland muss den Voraussetzungen der DSGVO genügen. • Angemessenheitsbeschluss der Kommission. Solang ein derartiger Angemessenheitsbeschluss vorliegt, ist die Übermittlung in ein Drittland gestattet (Beachte zB die Privacy Shield-Vereinbarung mit den USA). • Vorliegen geeigneter Garantien. Dieser Fall kommt nur zur Anwendung, wenn keine Genehmigung der Aufsichtsbehörde vorliegt. • Von der Aufsichtsbehörde genehmigte verbindliche interne Datenschutzvorschriften (Binding Corporate Rules). • Standarddatenschutzklauseln, die von der Kommission erlassen wurden oder von einer Aufsichtsbehörde angenommen und von der Kommission genehmigt worden sind. • Genehmigte Verhaltensregeln oder einem genehmigten Zertifizierungsmechanismus.

		Die DSGVO kennt noch weitere Ausnahmen, welche ohne Genehmigung der Aufsichtsbehörde zur Zulässigkeit führen: • Bei Vorliegen einer ausdrücklichen Einwilligung des Betroffenen (Achtung! Hier gilt ein erhöhtes Maß für die erforderliche Aufklärung. Der Betroffene muss über die Risiken dieser Zustimmung informiert werden). • Die Übermittlung ist für die Erfüllung eines Vertrages zwischen dem Betroffenen und dem Verantwortlichen oder zur Durchführung vorvertraglicher Maßnahmen auf Antrag der betroffenen Person erforderlich. • Die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person vom Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich.
9.	Kann ich Microsoft Programme aus der Cloud verwenden?	Cloud Programme gelten als Auftragsverarbeiter. Deshalb sind die hierfür relevanten Regelungen anzuwenden. Es ist darauf zu achten, dass eine schriftliche Vereinbarung für die Auftragsverarbeitung vorliegen muss (Nutzungsvereinbarungen bzw Vorlagen der großen Anbieter (Google, Microsoft, Mailchimp, etc) wurden idR bereits aktualisiert oder ausgeschickt, ansonsten bietet sich Nachfragen beim Auftragsverarbeiter an). Außerdem muss der Verantwortliche sicherstellen, dass der Auftragsverarbeiter ausreichend zuverlässig ist. In der Regel erfolgt dies durch die Prüfung von Zertifikaten (ISO Zertifizierungen). Auch der Speicherort spielt bei der Cloudnutzung eine bedeutende Rolle. Werden die Daten an einen Drittstaat im Sinne der DSGVO übermittelt und in der Folge dort verarbeitet oder gespeichert, gelten die in der Frage 8 genannten Voraussetzungen.
10.	Was muss das Verfahrensverzeichnis enthalten und welche Datenfelder muss ich aufnehmen?	Die Dokumentationspflicht trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter. Der Umfang ist für den Auftragsverarbeiter jedoch geringer als für den Verantwortlichen. Der Verantwortliche hat ein Verzeichnis sämtlicher Verarbeitungstätigkeiten, die in seiner Zuständigkeit liegen, zu führen. Im Verzeichnis enthalten sein müssen: • Name und Kontaktdaten des Verantwortlichen, sowie eines bestellten Datenschutzbeauftragten • Zweck der Datenverarbeitung • Beschreibung der Kategorie betroffener Personen und der Kategorien personenbezogener Daten • Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden • Gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland • Die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien • Die allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen

		Da das Verzeichnis nur Kategorien von Daten, Betroffenen und Empfängern abbilden muss, ist daher nicht eine Darstellung auf Datenfeldbasis bzw. auf Einzelpersonen-Ebene notwendig (z.B. statt Datenfelder Straße, Hausnummer, PLZ, Faxnummer, E-Mail etc -> Datenkategorie "Anschrift und Kontaktdaten").
11.	Muss ich Daten löschen wenn die 7-jährige Aufbewahrungsfrist nicht abgelaufen ist?	Grundsätzlich dürfen personenbezogene Daten nur für die Dauer des Verarbeitungsvorgangs gespeichert werden. Die Löschungsbegehren Betroffener sind aber durch gesetzliche Speicher- und Aufbewahrungsfristen begrenzt. Betroffene haben ein sogenanntes "Recht auf Löschung". Ein Recht auf Löschung steht zu wenn: • die betroffene Person ihre Einwilligung widerrufen hat • die personenbezogenen Daten für die Zwecke, für die sie erhoben wurden nicht mehr notwendig sind • die betroffene Person einen Widerspruch gegen die Verarbeitung eingelegt hat Über die 7-jährige Aufbewahrungsfrist hinaus dürfen Daten daher aufbewahrt werden, wenn dafür eine Rechtsgrundlage besteht (z.B. bestehende Geschäftsbeziehung oä).
12.	Wie muss ich Daten an den Kunden übermitteln? Per Post eingeschrieben? Ist eine Mail nicht zu unsicher?	Eine Auskunft muss grundsätzlich schriftlich erteilt werden. Die Auskunft hat alle Kopien der Daten, die Verarbeitungszwecke, die Datenkategorien, die Empfänger oder Kategorien von Empfängern, die geplante Speicherfrist und alle verfügbaren Informationen über die Herkunft der Daten zu enthalten. Außerdem muss der Betroffene von der Möglichkeit der Einschränkung/Löschung/Berichtigung der Daten informiert werden. Ein E-Mail mit den oben genannten Daten ist grundsätzlich ausreichend (da dem anfragenden Kunden seine eigenen personenbezogenen Daten beauskunftet werden, kann grundsätzlich auch der Kommunikationsweg der Beantwortung mit ihm vereinbart werden). Auf ausdrücklichen Wunsch sind die Daten dennoch in Papierform an den Betroffenen zu übermitteln. Für den Nachweis der fristgerechten Erledigung der Auskunft an die richtige Person ist gegebenenfalls eine Auskunftserteilung in Papierform und per Einschreiben zu empfehlen. Grundsätzlich muss die Datenübertragung kostenlos erfolgen. Ein angemessenes Entgelt kann nur bei offenkundig unbegründeten oder insbesondere wegen ihrer Häufigkeit exzessiven Anträgen verlangt werden. Der Antrag ist unverzüglich, in jedem Fall aber binnen einem Monat ab Eingang, zu erledigen. Es genügt auch eine mündliche Auskunftserteilung, allerdings ist dies nur dann möglich, wenn der Betroffene dies ausdrücklich wünscht und keine Zweifel an dessen Identität bestehen.
13.	Wenn ich bis jetzt die Einwilligungserklärungen nicht systematisch abgelegt habe, was tu ich dann? Muss ich eine Aussendung an die Kunden machen?	Siehe Frage 1.a.) Grundsätzlich ist es empfehlenswert, wenn zukünftig Daten weiterhin verarbeitet werden sollen, eine Einwilligung der Betroffenen einzuholen und diese auch ausreichend zu dokumentieren. Für NeukundInnen muss dieses System adaptiert werden, für Daten bestehender eigener Kunden gelten die oben genannten Voraussetzungen.
14.	Muss ich verkaufte e-books auch übergeben/übertragen? Downloadlinks sind zum	Beauskunftet werden müssen personenbezogene Daten. Das ist uE nicht das gekaufte E-Book selbst. Sondern nur, welches Buch er gekauft hat.

	Teil nicht mehr verfügbar.	
15.	Wie ist der Social Media-Bereich (Facebook,…) betroffen? Ist da meinerseits was zu tun?	Wenn ein Unternehmen Kundendaten mit Facebook/Twitter oder anderen sozialen Netzwerken teilen will (zB E-Mail-Adressen oä hochladen für "Custom Audience" und zielgruppengesteuerte Posts), dann braucht man die DSGVO-konforme Einwilligung der Betroffenen. Insofern handelt es sich um einen eigenen Zweck, welcher vom Betroffenen eine eigene Einwilligung bedarf.
16.	Wie viele Daten darf ich bei Online Newsletter-Anmeldungen, Registrierungsprozessen zu Online-Produkten, Käufen im Webshop, Gratis-Downloads erheben und speichern (z.B. auch Branche und Funktion bei B2B)? Wie wirkt sich hier das Prinzip der Datenminimierung aus? Wie sind die Einwilligungserklärungen zu gestalten?	Es dürfen nur zweckbasierte Daten erhoben werden, kein Überschuss und keine Daten auf Vorrat (Prinzip der Datenminimierung bedeutet, dass die personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen). Die Einwilligungserklärungen sind genau im Umfang der zu erhebenden und zu speichernden Daten auszugestalten. In den hier genannten Fällen ist besonders das Koppelungsverbot zu beachten, welches verhindert, dass die Dienste nur denjenigen Nutzern angeboten werden, die im Gegenzug der Verarbeitung ihrer Daten (etwa für Werbezwecke) zustimmen. Als "Einwilligung" gilt jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung einverstanden ist. Eine "ausdrückliche" Einwilligung ist nur bei der Verarbeitung von sensiblen Daten erforderlich.
17.	Welche Änderungen sind in AGB und Datenschutzerklärung erforderlich, um DSGVO-konform zu sein?	• Weitergeltung bisher erteilter Einwilligungen, sofern sie entsprechend der DSGVO erteilt wurden (s. Art 7 und Art 8 DSGVO) • Schlüssige Einwilligung möglich (s. Art 4 Z 11 "in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung") • Ausdrückliche Zustimmung bei Verarbeitung sensibler Daten • Vor Verarbeitung persönlicher Daten von Kindern, die das 16. Lebensjahr noch nicht vollendet haben, muss die Zustimmung der Eltern eingeholt werden (Art 8 Abs 1 DSGVO) + Öffnungsklausel, dass MS das Mindestalter bis auf das 13. Lebensjahr senken können. Sofern AGB und Datenschutzerklärungen vorformulierte Zustimmungen oder Zustimmungsfiktionen enthalten, müssen diese angepasst werden. Darüberhinaus ist eine Adaptierung an die neue Rechtslage erforderlich.
18.	Gibt es Änderungen bezüglich der Cookie Meldung?	Die DSGVO per se enthält keine Änderungen bezüglich Cookie Meldungen. Es gibt eine Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies der Artikel 29-Datenschutzgruppe aus dem Jahr 2013. Seit Annahme der geänderten Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) im Jahr 2009, die in allen EU-Mitgliedstaaten umgesetzt wurde, haben die Website-Betreiber eine Reihe von praktischen Lösungen für die Einholung der Einwilligung zur Verwendung von Cookies oder ähnlicher Tracking-Technologien („Cookies“ genannt) entwickelt, die für verschiedene Zwecke genutzt werden (von verbesserten Funktionalitäten bis zu Webanalysen, gezielter Werbung und Produktoptimierung usw. durch die Website-Betreiber oder Dritte). Die Vielzahl der von Website-Betreibern

		genutzten Einwilligungsmechanismen ist Ausdruck der Vielfalt der Organisationen und ihrer Zielgruppen. Dem Website-Betreiber steht es frei, wie er die Einwilligung einholt, solange die Einwilligung im Rahmen der EU-Gesetzgebung als gültig anerkannt werden kann.
19.	Wie muss die Einwilligung in das personenbezogene Tracking formuliert und gestaltet sein?	Siehe Antwort zu Frage 18.
20.	Wie verhält es sich mit der Kommunikation im B2B-Bereich. Newsletter, Follow-button? Zeitungsabos etc.?	Die DSGVO betrifft alle Daten, anhand derer sich natürliche Personen identifizieren lassen, zB: • Adressen (etwa auf Rechnungen); • Kontodaten; • Fotos auf Homepage; Einordnung B2B/B2C irrelevant, sofern es sich um natürliche Personen handelt. Österreichisches DSG schützt derzeit auch noch Daten juristischer Personen.
21.	Wie schaut es aus mit der Veröffentlichung in Presseberichten von Personenfotos aus? Braucht man eine Einverständniserklärung der abgebildeten Personen?	Siehe Antwort zu Frage 20. Lassen Fotos die Identifikation natürlicher Personen zu, muss hierfür eine Einverständniserklärung eingeholt werden.
22.	Kurze Erklärung: kleine GmbH Jahresumsatz unter EUR 20.000. Benötigt unser Unternehmen einen Datenschutzbeauftragten, und wenn ja, kann ein Gesellschafter diese Funktion übernehmen?	Siehe Antwort zu Frage 3. Ob ein Datenschutzbeauftragter bestellt werden muss, hängt von der Datenverarbeitung ab. Grundsätzlich kann der Datenschutzbeauftragte sowohl Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein als auch seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen. Er kann auch andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter haben sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Beim Gesellschafter fraglich ist die Gewährleistung der Unabhängigkeit des Datenschutzbeauftragten (besonders dann, wenn es sich um einen Gesellschafter-Geschäftsführer handelt). Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können. Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt. Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der

		Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters. Der Verantwortliche hat die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Datenschutzbehörde mitzuteilen.
23.	Wie soll mit personenbezogenen Informationen in Online-Publikationen umgegangen werden, z.B. mit Autorenbiographien, email usw.? Wie mit Inhalten wie Biographien lebender Personen (z.B. in einem Komponistenlexikon oder Sportlerlexikon), wenn dies online erscheint?	Erfolgt die Veröffentlichung eines Werks rechtmäßig, so führt das Inkrafttreten der DSGVO nicht dazu, dass dieses keine personenbezogenen Daten mehr enthalten darf. Soweit dieses personenbezogene Daten natürlicher Personen umfasst, gilt der allgemeine Grundsatz, dass eine Rechtsgrundlage für die Datenverarbeitung vorliegen muss. Rechtsgrundlager der Veröffentlichung von Autorenbiographien wird in der Regel der Verlagsvertrag sein. Dies kann aber auch eine Einwilligungserklärung, sonstige Vertragserfüllung (z.B. Bewerbung einer Lesung des Autors in der Buchhandlung) oder auch berechtigte Interessen sein.
24.	Ein Verlag verschickt regelmäßig Newsletter und Veranstaltungsankündigungen. Die Newsletter gehen an die Kunden im Buchhandel. Die Veranstaltungseinladungen an Journalisten, Autoren, Veranstalter und interessierte Privatpersonen. Der Verteiler ist über Jahre gewachsen. Die Veranstaltungsankündigungen beinhalten teilweise auch eine Bitte um Anmeldung zur Veranstaltung per E-Mail. Was muss dabei beachtet werden? Wie ist mit solchen Verteilern (also Listen von Mail-Adressen, vlt. noch verbunden mit Namen) generell umzugehen? Muss da jetzt jede und jeder nachträglich seine Zustimmung abgeben?	Siehe Antwort zu Frage 1. Gemäß § 107 TKG (gilt gleichermaßen für B2C und B2B) ist eine vorherige Zustimmung für die Zusendung elektronischer Post dann nicht notwendig, wenn 1. der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und 2. diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und 3. der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und 4. der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die in § 7 Abs. 2 E-Commerce-Gesetz genannte Liste, abgelehnt hat.
25.	Ein Verlag vereinbart Lesungen mit Veranstaltern. Deren Daten (Name, Adresse, Kontaktdaten) werden in ein firmeninternes System eingespeichert. Muss dafür eine	Grundsätzlich ist eine gesonderte Zustimmungserklärung dann nicht notwendig, wenn die Verarbeitung der Daten zur Vertragserfüllung (Abhaltung der vertraglich vereinbarten Lesungen) erforderlich ist. Dies wird hier in der Regel der Fall sein. Sollen die Daten auch für andere Zwecke weiterverwendet werden, empfiehlt sich, eine Einwilligungserklärung

	Zustimmung eingeholt werden? Auf was ist zu achten?	vorzusehen. Wie eine solche Einwilligungserklärung zu erfolgen hat, ist in der Antwort zu Frage 7 beschrieben.
26.	Ein Verlag schickt Bücher an Journalisten und speichert die Daten (Name, Adresse, Kontaktdaten) in einem firmeninternen System. Nachverfolgt wird hier, welche Bücher an die- oder denjenigen geschickt wurden, ob angefordert oder unangefordert und zu welchen Büchern Rezensionen erschienen sind. Muss dafür eine Zustimmung eingeholt werden? Auf was ist zu achten?	Siehe Antwort zu Frage 23 und 25. Die DSGVO führt nicht dazu, dass die Ausübung der normalen Geschäftstätigkeit und dazugehörige Datenverarbeitung jedenfalls und unbedingt eine Zustimmungserklärung benötigt. Fordert der Journalist ein Buch an, dann dürfen die dafür notwendigen Daten auch verarbeitet werden, ohne dass dies einer gesonderten schriftlichen Zustimmungserklärung bedarf. Eine Verarbeitung von Daten ist neben der Vertragserfüllung oder einer Einwilligungserklärung insbesondere auch zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten zulässig, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Dies ist bei den beruflichen Kontaktdaten eine im Bereich Literaturkritik tätigen Journalisten, dessen Beruf es ist, Rezensionen zu verfassen, und zu diesem Zweck über neu erschienene Bücher informiert zu werden, wohl nicht der Fall. Auf sein Widerspruchsrecht bei Verarbeitung ohne Zustimmung und Zusendung ohne Anforderung ist der Journalist allerdings trotzdem hinzuweisen.
27.	Muss ich meine Festplatten (Server, Workstation, Laptop – Zugriff mittels VPN Verbindung) verschlüsseln?	Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen die DSGVO verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Personenbezogene Daten sollten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung.
28.	Wenn ich Kontaktdaten auf meinem Smartphone nutze, muss ich das Smartphone verschlüsseln?	Siehe Antwort zu Frage 27. Artikel 32 DSGVO besagt, dass "[u]*nter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*"