von Rechtsanwalt **Phil Salewski**

Gefragt, geantwortet: FAQ zur praktischen Umsetzung der DSGVO im Online-Handel (4. Update)

Auf verschiedensten Seiten im Internet werden bereits jetzt die Auswirkungen der Datenschutzgrundverordnung (DSGVO) auf den Online-Handel dargestellt – allerdings meist ausschließlich mit rechtlichem Schwerpunkt. Weil die praktische Umsetzung der Vorschriften Online-Händler aber noch immer vor erhebliche Schwierigkeiten stellt, die Rechtskennern im Zweifel wenig bewusst sind, hat die IT-Recht Kanzlei um Zusendung konkreter praxisrelevanter Fragen gebeten. Die folgenden FAQ sollen einfache, praktikable Antworten auf das geben, was Online-Händler im Zusammenhang mit der DSGVO umtreibt.

A. Allgemeine Fragen

Frage: Gilt die DSGVO auch für vor dem 25.05.2018 erhobene Daten?

Grundsätzlich ja, allerdings mit Erleichterungen.

Sofern Datenverarbeitungsvorgänge vor dem Inkrafttreten der DSGVO abgeschlossen sind, dürfen diese nach dem Inkrafttreten nur auf Basis einer Rechtfertigung nach der DSGVO erneut ablaufen. Die praktischen Auswirkungen dieses Grundsatzes sind allerdings gering, weil die Rechtfertigungsgründe des bisherigen Datenschutzrechts mit denjenigen der DSGVO weitgehend übereinstimmen und für neue Datenvorgänge nach dem 25.05.2018, die ursprünglich gerechtfertigt waren, auch eine Rechtfertigung nach der DSGVO bestehen wird.

Speziell für Datenverarbeitungen auf Grundlage von ausdrücklichen Einwilligungen gilt zudem das Privileg, dass vor dem 25.05.2018 eingeholte Einwilligungen auch unter der DSGVO unverändert ihre Gültigkeit behalten.

Datenverarbeitungsvorgänge, die vor der Geltung der DSGVO zum 25.05.2018 begonnen haben, mussten spätestens zu diesem Zeitpunkt mit ihr in Einklang gebracht werden. Dem Grunde nach sieht die DSGVO damit zumindest die Möglichkeit eines Überlebens der Rechtmäßigkeit alter Datenverarbeitungen unter der Einschränkung vor, dass diese Verarbeitungen ab dem 25.05.2018 auch die Vorschriften der DSGVO erfüllen.

Frage: Gilt die DSGVO auch außerhalb des Online-Handels, etwa bei Verkäufen auf Messen etc.?

Ja, sofern hierbei Daten von Käufern oder Interessenten manuell erfasst und in einem Dateisystem (etwa einer Kartei, einem Register, einer Liste) zusammengetragen werden.

Je danach, welche Daten von Kunden erhoben werden, muss auch bei direktem persönlichen Verkaufskontakt eine Rechtfertigung nach der DSGVO vorliegen.
Bestelldaten (Name und Anschrift, Zahlungsdaten, ggf. Mailadresse für eine elektronische Bestellbestätigung) können regelmäßig unter Berufung auf die vertragliche Erforderlichkeit erhoben werden, wohingegen Mailadressen zur Versendung von Werbung auch hier nur nach vorheriger Einwilligung im Wege des Double-Opt-Ins (Eintragung der Adresse in Liste und Bestätigung eines Aktivierungslinks per Mail) erfasst und verwendet werden dürfen.

Frage: Wer ist richtiger „Verantwortlicher" im Online-Handel?

Verantwortlicher ist grundsätzlich, wem die wesentliche Entscheidungsbefugnis für die Verarbeitung von personenbezogenen Daten zukommt. Ob dies eine natürliche Einzelperson oder eine Rechtsperson (Unternehmen) ist, ist egal.

Im Online-Handel besteht daher ein eingeschränktes Wahlrecht:

Datenverantwortlicher ist vorrangig der Online-Händler selbst als Einzelperson. Führt er ein Unternehmen (GmbH, GbR etc.), so kann er aber auch das Unternehmen als Verantwortlichen wählen. Alternativ kann er anstelle des Unternehmens den Geschäftsführer oder sich selbst in seiner Funktion als Inhaber des Unternehmens als Verantwortlichen einsetzen.

Detaillierte Informationen zur Bestimmung des Verantwortlichen finden Sie in diesem Beitrag.

Frage: Bezieht sich die DSGVO nur auf den Online-Handel?

Nein. Die DSGVO gilt für alle Stellen (sowohl Behörden als auch Unternehmen), die in irgendeiner Form personenbezogene Daten verarbeiten. Der Online-Handel ist ein Anwendungsfall, es existieren aber noch unzählige weitere.

Einige **Beispiele** sind: Unternehmen im Umgang mit Mitarbeitern; Tätigkeit von Auskunfteien; Forschungsinstitutionen im Umgang mit Studien; der Rundfunkbeitrag

Frage: Gilt die DSGVO auch im B2B-Geschäft?

Jein. Der Anwendungsbereich der DSGVO ist immer eröffnet, wenn personenbezogene Daten von natürlichen Einzelpersonen verarbeitet werden. Personenbezogene Daten von juristischen Personen (Unternehmen mit eigener Rechtspersönlichkeit) werden dahingegen nicht geschützt.

Insofern ist für das B2B-Geschäft zu differenzieren:

- Vertragsbeziehungen mit Einzelhändlern und Kaufleuten fallen unter die DSGVO.
- Vertragsbeziehungen mit Kapitalgesellschaften (AG, GmbH), eingetragenen Vereinen und Personengesellschaften (OHG, KG, GbR) fallen dann nicht unter die DSGVO, sofern allein die juristischen Personen unter ihrer Firmierung (und nicht auch die dahinterstehenden Funktionsträger als natürliche Personen) adressiert werden.

Beispiel für die Zusendung von Briefwerbung: Briefwerbung an die juristische Person selbst unter Verwendung ihrer Firma fällt nicht unter die DSGVO, Briefwerbung an einzelne Gesellschafter einer GmbH aber schon.

Frage: Gilt die DSGVO für einen B2B-only-Shop in Bezug auf (nicht akzeptierte) Vertragsanträge von Privatpersonen?

Ja. Auch wenn ein Shop ausschließlich mit Unternehmern handelt, muss die DSGVO eingehalten werden, wenn (nicht berechtigte) Privatpersonen eine Bestellung zu tätigen versuchen. Sie sind natürliche Personen und unterliegen dem DSGVO-Datenschutz.

Wie mit Daten von Privatpersonen umzugehen ist, hängt von der Art der Daten ab:

1.) Bestell-/Kundendaten

Im Wege des Vertragsangebots offengelegte personenbezogene Daten (Name, Anschrift, Mailadresse etc.) können für eine Nachricht über die Ablehnung von Vertragsbeziehungen verwendet werden, müssen dann aber unverzüglich aus allen Speicherorten gelöscht werden. Eine Weitergabe an Dritte ist stets unzulässig.

Über diese Konstellation ist in der Datenschutzerklärung, etwa im Punkt „Umgang mit Bestelldaten von Privatpersonen“, zu informieren.

2.) Nutzungsdaten (IP-Adresse etc.)

Werden bereits durch den Besuch der Website Daten wie die IP-Adresse etwa durch Cookies oder Plug-Ins erhoben und ausgelesen, kann sich der B2B-Shopbetreiber regelmäßig auf ein berechtigtes Interesse berufen, muss auf jeden solcher Datenvorgänge aber stets gesondert in seiner Datenschutzerklärung hinweisen. Dies gilt aber **unabhängig** davon, ob der Besucher eine Privatperson oder ein Mitarbeiter eines Unternehmenskunden ist, weil die Verarbeitung hier in beiden Fällen auf eine natürliche Person durchschlägt.

Frage: Gilt die DSGVO auch für den Handel auf Plattformen (eBay, Amazon und Co.?)

Ja. Auch wenn auf Plattformen der Kontakt zum Kunden über den Plattformbetreiber gemittelt wird, verarbeiten Händler hier personenbezogene Daten von Kunden, etwa im Rahmen von Bestellungen und deren Abwicklung (Buchhaltung, Bezahlung, Versand), aber teils auch im Zusammenhang mit Werbung.

Die notwendige Datenschutzerklärung für Plattform-Händler ist allerdings weniger umfangreich als die für einen klassischen Online-Shop, weil der Gestaltungs- und Entscheidungsspielraum für Datenprozesse auf der Plattform (etwa die Wahl von Zahlungsmitteln, der Einsatz von Plug-Ins und Cookies sowie die Verwendung von Tracking-Tools) deutlich eingeschränkt ist.

Die IT-Recht Kanzlei wird ihren Mandanten speziell für Handelsplattformen angepasste Datenschutzerklärungen zur Verfügung stellen.

Frage: Gilt die DSGVO auch für Kleinunternehmer?

Ja. Die DSGVO gilt für jeden, der personenbezogene Daten Dritter verarbeitet und hierbei nicht nur aus persönlichen oder familiären Gründen tätig wird.
Wer als Kleinunternehmer Produkte über das Internet verkauft und hierbei Kundendaten erhebt und verarbeitet, ist ebenso an die DSGVO gebunden wie ein Großhändler.

Privilegiert wird ein Kleinunternehmer nur insofern, als dass er keinen Datenschutzbeauftragten bestellen muss.

Frage: Wie erfüllen "kleinere" Händler die Vorgaben der künftigen Datenschutz-Grundverordnung (DSGVO)?

Hierauf sind wir hier im Einzelnen eingegangen.

Frage: Welche Bereiche im Online-Shop müssen vor Inkrafttreten der DSGVO überarbeitet werden?

Dies lässt sich nicht pauschal sagen. In jedem Fall muss die Datenschutzerklärung umfassend überarbeitet werden. Hieran anknüpfend müssen sämtliche Felder und Schaltflächen (vor allem Einwilligungsfelder wie z.B. dasjenige für einen Newsletter), die auf die Datenschutzerklärung verlinken, mit einem aktualisierten Link versehen werden.

Im Zusammenhang mit den durch die DSGVO verschärften Anforderungen an den Datenschutz werden auch Anpassungen bei bestimmten Plug-Ins und Social-Media-Buttons notwendig sein.

(Die AGB und Kundeninformationen der IT-Recht Kanzlei müssen nicht geändert werden.)

Auch Cookie-Banner, Produktdetailseiten, der Check-Out-Prozess, der Warenkorb, das Kunden-Login und der Kundenbereich nach Log-In brauchen keine Anpassungen.

Frage: Muss die Kenntnisnahme der Datenschutzerklärung im Bestellvorgang durch den Kunden ausdrücklich bestätigt werden?

Nein. Eine solche Ausgestaltung des Bestellvorgangs ist zwar weit verbreitet, aber nicht zwingend.

Gesetzlich vorgeschrieben ist es nämlich nicht, dass der Kunde die Kenntnisnahme der Datenschutzinformationen ausdrücklich bestätigt.

Daher genügt es, wenn Online-Händler ihre Kunden auf die Erklärungen deutlich hinweisen und ihnen durch Verlinkung der Bezeichnung die Möglichkeit verschaffen, von ihren Inhalten Kenntnis zu nehmen.

Weitere Informationen zur korrekten Ausgestaltung des Bestellvorgangs finden Sie in diesem Beitrag der IT-Recht Kanzlei.

B. Fragen zur datenschutzrechtlichen Einwilligung

Frage: Wie oft kommt die datenschutzrechtliche Einwilligung im Online-Handel zum Tragen?

Im alltäglichen Geschäft selten. Datenverarbeitungen im Bestell- und Kaufprozess (Verarbeitung von Kundendaten, Zahlungsdaten, Versandinformationen, aber auch das Nutzen von Kontaktformularen.) können weit überwiegend bereits durch die Erforderlichkeit zur Vertragsdurchführung oder -anbahnung gerechtfertigt werden. Datenverarbeitungen durch Cookies, Analysedienste oder Plug-Ins sowie Weitergaben von Daten zur Bonitätsprüfung im Zahlprozess rechtfertigen sich demgegenüber weitestgehend durch berechtigte Interessen. Einer Einwilligung von Betroffenen bedarf es insoweit nicht.

Über den Einsatz von Cookies ist im Webshop nach wie vor unter Verwendung eines Banners zu informieren. Dies gilt noch so lange, bis die von der EU zu verabschiedende sogenannte E-Privacy-Verordnung in Kraft tritt, welche den Gebrauch von Cookies unter das Erfordernis einer ausdrücklichen Nutzereinwilligung stellen soll. Ein Datum ist allerdings noch nicht bekannt.

Der bedeutsamste Fall für die Erforderlichkeit einer Einwilligung bleibt der Newsletter-Versand. Daneben kann die Einwilligung im Einzelfall je nach Geschäftsfeld, so z.B. für Online-Apotheken, die sensible Gesundheitsdaten verarbeiten, erforderlich werden. Schließlich lösen bestimmte Social-Media-Plugins durch den Umfang der durch sie erhobenen Daten eventuell die Pflicht zur Einholung einer Einwilligung aus.

Frage: An welcher Stelle des Kaufprozesses im Shop muss eine Einwilligung eingeholt werden?

Eine Einwilligung muss grundsätzlich immer dort eingeholt werden, wo im Anschluss unmittelbar einwilligungsbedürftige Datenverarbeitungsvorgänge ablaufen würden.

Für Datenverarbeitungen, die mit dem Prozess des Kaufs an sich zu tun haben (Erhebung von Name, Anschrift, Zahldaten, Mailadresse für die Bestellbestätigung etc.), bedarf es einer Einwilligung aber meist nicht, weil die Verarbeitung durch die Erforderlichkeit zur Vertragsdurchführung gerechtfertigt wird.

Hinweise:

1: Bedeutend wird die Einwilligung aber für Online-Apotheken und sonstigen Arzneimittel-Onlinehandel bei der Verarbeitung von Gesundheitsdaten (etwa Rezepten oder Informationen zu Krankheitsbildern oder -verläufen) im Kaufprozess. Diese Verarbeitung kann nur durch Einwilligung und gerade nicht durch die Erforderlichkeit zur Vertragsdurchführung gerechtfertigt werden. Die Einwilligung ist hier auf der Check-Out-Seite (Bestellseite, auf welcher der Kauf abgeschlossen wird) einzuholen.
2. Wird in den Kaufprozess die Möglichkeit einer Anmeldung zum Newsletter integriert, ist die

Einwilligung auf der Seite einzuholen, auf der die Anmeldung ermöglicht und vom System erfasst wird (meist auf der Check-Out-Seite).

Frage: Muss für die Anlegung eines Kundenkontos eine Einwilligung eingeholt werden? Wenn ja, im Double- oder im einfachen Opt-In-Verfahren?

Es muss eine Einwilligung im einfachen Opt-In-Verfahren vorzugsweise durch das Anklicken einer Checkbox mit der Bezeichnung „Ja, ich möchte ein Kundenkonto anlegen“ oder einem vergleichbaren Text eingeholt werden.

Die Zusammenführung von Kundendaten in einem Kundenkonto ist eine nach der DSGVO einschlägige Datenverarbeitung, für die eine Rechtfertigung vorliegen muss.

Auf die Erforderlichkeit zur Vertragsdurchführung kann sich ein Online-Händler hier aber nicht berufen, weil ein Kundenkonto für den Vertrag nicht zwingend vorhanden sein muss. Insofern sind auch Bestellungen als Gast möglich und ausreichend.

Aus diesem Grund ist eine ausdrückliche Einwilligung des Kunden notwendig. Eines Rückgriffs auf das Double-Opt-In-Verfahren bedarf es für ihre Einholung aber nicht, weil bei der Anlegung eines Kundenkontos keine Gefahr für ein Auseinanderfallen zwischen Kontoinhaber und Datensubjekt besteht, welche das Bedürfnis nach einer zweistufigen Verifikation wecken könnte.

Achtung: wird das Anlegen eines Kundenkontos mit einer Anmeldung zum Newsletter verbunden, ist für das Kundenkonto das einfache Opt-In, für den Newsletter hingegen dass Double-Opt-In vorauszusetzen.

Frage: Gelten vor Inkrafttreten der DSGVO erteilte Einwilligungen weiterhin fort?

Ja. Bereits erteilte Einwilligungen für Newsletter und sonstige einwilligungsbedürftige Vorgänge im Online-Shop bleiben für den jeweils Betroffenen auch unter der DSGVO bestehen und müssen nicht erneut eingeholt werden.

Frage: Müssen datenschutzrechtliche Einwilligungen protokolliert werden?

Ja. Der Verantwortliche muss nachweisen können, dass der jeweilige Betroffene in die Datenverarbeitung eingewilligt hat. Werden Einwilligungen – wie im Online-Handel üblich – elektronisch eingeholt, müssen diese mittels technischer Maßnahmen hinreichend protokolliert werden.

Frage: Wie kann eine elektronische Einwilligung in die Datenverarbeitung protokolliert werden?

Elektronische Einwilligungen werden standardmäßig durch das Setzen eines Häkchens neben einem entsprechenden Einwilligungstext eingeholt.

Die Protokollierung erfolgt durch Abspeicherung des Einwilligungstextes und der Aktion des Häkchensetzens (bzw. des Betätigens der Bestätigungs-Schaltfläche) mit Zeitstempel und IP-Adresse des verwendeten Endgeräts.

So lässt sich die erteilte Einwilligung einerseits einer konkreten Datenverarbeitung und andererseits einem individuellen Betroffenen zuordnen.

Ist der Betroffene bei Erteilung der Einwilligung in ein Kundenkonto eingeloggt, sollten zu Beweiszwecken auch der richtige Name sowie der Nutzernamen mit abgespeichert werden.

Frage: Wie kann die Einwilligung beim Double-Opt-In-Verfahren für den Newsletter-Versand protokolliert werden?

Die Protokollierung der Einwilligung in den Newsletter-Versand erfolgt in 2 Schritten:

1. Abspeicherung der Eintragung zum Newsletter und der verwendeten Mailadresse

2. Abspeicherung des Anklickens des Bestätigungslinks in der Verifizierungsmail mit Zeitstempel und IP-Adresse des verwendeten Endgeräts

Diese gespeicherten Informationen müssen sodann für die registrierte Mailadresse zusammengeführt werden.

Nur durch eine Verbindung der beiden Schritte kann hinreichend protokolliert werden, dass der tatsächliche Inhaber des Mailaccounts, für den die Anmeldung erfolgt ist, die Anmeldung höchstpersönlich vollzogen, also seine Einwilligung in den Erhalt von Werbemails selbst erteilt hat.

Frage: Muss die für die Protokollierung gespeicherte IP-Adresse maskiert werden?

Nein, davon ist sogar abzuraten. Zu Nachweiszwecken ist gerade die Protokollierung einer nicht anonymisierten IP-Adresse erforderlich, weil anderenfalls deren Zuweisung zum konkret Einwilligenden nicht gelingen kann.

Frage: Wie kann die Einwilligung bei Beauftragung eines Newsletter-Versanddienstleisters protokolliert werden?

Weil Newsletter-Versanddienstleister den Newsletter-Versand in fremdem Namen eigenständig abwickeln und regelmäßig auch selbstständig das für die Zulässigkeit des Mailversandes erforderliche Double-Opt-In-Verfahren vollziehen, ist eine Protokollierung von Einwilligungen für den beauftragenden Händler schwieriger. Insbesondere wird er keine IP-Adressen der Anmelder abspeichern können.

Allerdings gestatten die meisten Dienstleister den Werbenden eine Personalisierung der Anmelde- und Bestätigungsmail für den Double-Opt-In-Prozess und speichern die Anmeldung und Aktivierung des Bestätigungslinks mailadressenbezogen und für den Werbenden zugreifbar ab. Auch ohne Speicherung der IP-Adresse genügt dies für die Protokollierung einer individuellen Einwilligung, weil der Werbende infolge seines Zugriffs auf das System des Dienstleisters darlegen kann, dass für eine bestimmte Empfängeradresse zu einem jeweils eindeutigen Zeitpunkt sowohl eine Anmeldung zum Newsletter als auch eine Bestätigung des Aktivierungslinks erfolgt ist.

Wichtig: weil vor dem 25.05.2018 eingeholte Einwilligungen in den Newsletter-Versand auch unter der DSGVO weiterhin Bestand haben (Erwägungsgrund 171), muss bei Inanspruchnahme eines Newsletter-Versanddienstleisters kein neues Double-Opt-In-Verfahren ausgelöst werden. Es genügt hier die Nachweisbarkeit der originären Anmeldung, etwa in Form des Datenbankeintrags mit Empfänger-Adresse und Double-Opt-In-Zeitstempel.

Frage: Gilt das Double-Opt-In-Verfahren für Newsletter europaweit?

Ja, das Double-Opt-In-Verfahren für die Newsletteranmeldung sollte europaweit beachtet werden. Verbindlich vorgeschrieben ist es nicht, aber nur mit ihm kann sichergestellt werden, dass die Einwilligung tatsächlich vom Inhaber des anzumeldenden Accounts stammt.

Frage: Bleibt der für Newsletter verwendete Einwilligungstext weiterhin zulässig?

Ja, der Text (Hinweis auf Zusendung von Neuigkeiten zu Geschäft und Produkten und auf Widerrufsmöglichkeit) bleibt zulässig und muss nicht abgeändert werden.

Frage: Werden die besonderen Voraussetzungen für die Einwilligung Minderjähriger (Art. 8 DSGVO) im Online-Handel relevant?

Eher nicht. Dies zum einen, weil die meisten Datenverarbeitungen im Online-Shop über ihre Notwendigkeit zur Vertragsdurchführung oder über berechtigte Interessen und nicht über die Einwilligung gerechtfertigt werden. Zum anderen ist die Wahrscheinlichkeit, dass ein Online-Händler mit Minderjährigen in Kontakt gerät, ohnehin gering. Minderjährige sind nämlich bis zur Vollendung des 18. Lebensjahrs beschränkt geschäftsfähig und können online so grundsätzlich ohne die elterliche Einwilligung keine Verträge schließen.

C. Fragen zu bestimmten Verarbeitungsformen

Frage: Inwiefern ist der Einsatz von WhatsApp für Werbung unter der DSGVO zulässig?

Die Verwendung von WhatsApp für Werbung ist bei Einholung einer ausdrücklichen Einwilligung des Nutzers zulässig.
In der Mailwerbung hat sich als rechtsicherer Maßstab für die zuverlässige Einwilligungseinholung das sogenannte „Double-Opt-In"-Verfahren etabliert, in dessen Rahmen der Interessent nach Eintragung seiner Mailadresse zunächst eine Mail mit einem Bestätigungslink enthält, dessen Anklicken den Newsletter-Versand einleitet und eine Identität von Inhaber der verwendeten Mailadresse und bestimmungsgemäßem Empfänger sicherstellt.

Für die Zusendung von Werbenachrichten über WhatsApp dahingegen muss ein solches zweifaches Verifikationssystem nicht zwingend durchgeführt werden und ist aus organisatorischen Gründen auch nicht ratsam. Denkbar wäre zwar, den Interessenten zur Eintragung seiner mit WhatsApp verknüpften Telefonnummer aufzufordern und an diese zunächst eine Aktivierungsanfrage zu versenden, welche der Interessent für die Einleitung des Newsletter-Versandes sodann bestätigen muss. Dies würde aber erfordern, dass der Händler über die Website registrierte Telefonnummern stets manuell auf ein WhatsApp-fähiges mobiles Endgerät übertragen müsste, um sodann die individuelle Aktivierungsanfrage abzusenden.

Um den organisatorischen und zeitlichen Aufwand für Händler zu minimieren, empfiehlt es sich also, eine anfängliche Registrierung der Telefonnummer des Interessenten direkt über WhatsApp zu erreichen.

Etabliert hat sich hierfür ein Prozedere, bei dem der Interessent dazu aufgefordert wird, die WhatsApp-fähige Nummer des Händlers einzuspeichern und an diese eine Nachricht mit dem Text „Start" zu senden. Dadurch, dass der Interessent durch Einspeichern der Nummer zunächst selbst aktiv werden muss und durch die „Start"-Nachricht die Kommunikation über seine persönliche Nummernkennung überhaupt erst einleitet, wird automatisch sichergestellt, dass es sich bei diesem um den

empfangsbereiten Inhaber der Telefonnummer handelt. Diese Nachricht stellt die elektronische ausdrückliche Einwilligung dar, die zusammen mit der Telefonnummer hinreichend personenbezogen dokumentiert werden kann. Erhält der Händler die Nachricht, kann er die verwendete Telefonnummer direkt auf WhatsApp einer Newsletter-Broadcasting-Liste hinzufügen, ohne dass er vorher gehalten wäre, sie manuell abzuspeichern.

Freilich muss der Interessent - bestenfalls auf einer Unterseite der Händlerpräsenz – über dieses Prozedere sowie darüber informiert werden, dass es ihm möglich ist, dem Newsletter-Versand durch eine entsprechende Kurznachricht (etwa „Stop“) jederzeit mit Wirkung für die Zukunft zu widersprechen. Auch ist eine erläuternde Klausel, welche sämtliche Informationen über das Anmeldeverfahren und den Widerspruch enthält, in der Datenschutzerklärung notwendig.

Frage: Bleibt die Briefwerbung ohne Einwilligung unter der DSGVO erlaubt?

Ja. Werbebriefe können unter Nutzung bereits vorhandener Adressdaten auch weiterhin ohne Einwilligung verschickt werden. Der Händler stützt sich hierbei auf sein berechtigtes Interesse an persönlicher Direktwerbung.

Widerspricht der Empfänger dem Erhalt von Werbebriefen, so müssen die Werbebriefe aber unverzüglich abgestellt werden.

Achtung: von der Briefwerbung unter Nutzung von Kundendaten ist die sogenannte „Briefkastenwerbung“ zu unterscheiden, bei der wahllos in einem bestimmten Einzugsgebiet jeder Anwohner Werbepost an seinen Briefkasten erhält. Die Werbung wird insofern nicht an einzelne, vorausgewählte Adressen zugestellt. Die Briefkastenwerbung ist unzulässig, wenn der Empfänger etwa mittels Aufkleber „Keine Werbung und kostenlose Zeitschriften“ dem Erhalt solcher Wurfsendungen von vornherein widersprochen hat.

Frage: Ist der Versand von Newslettern ohne Einwilligung an vorhandene Geschäftskontakte zulässig?

Mit bestimmten Einschränkungen ja.

Newsletter können ohne Einwilligung an vorhandene Geschäftskontakte versendet werden, wenn

- der Händler im Zusammenhang mit dem Verkauf von Produkten von dem Kunden dessen Mailadresse erhalten hat,
- der Händler die Adresse **nur** zur Direktwerbung für **eigene ähnliche** Produkte verwendet,
- der Kunde der Verwendung nicht widersprochen hat **und**
- der Kunde bei Erhebung der Mailadresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann

Diese Voraussetzungen müssen alle zusammen (kumulativ) erfüllt sein.

Hinweis: der neue und allein für Mandanten einsehbare DSGVO-konforme Datenschutzgenerator der IT-Recht Kanzlei wird eine wählbare Klausel zu Newslettern ohne Einwilligung enthalten.

Frage: Können Newsletter weiterhin über den US-Dienst „Mailchimp“ versandt werden?

Ja. „Mailchimp“ ist für das us-europäische Datenschutzabkommen „Privacy Shield“ zertifiziert und hat sich so zur Einhaltung europäischer Datenschutzstandards verpflichtet. Das macht den Einsatz trotz internationaler Datentransfers unbedenklich.

Hinweis: die neue DSGVO-konforme Datenschutzerklärung der IT-Recht Kanzlei wird eine wählbare Klausel zum Einsatz von „Mailchimp“ enthalten.

Frage: Ist die Verwendung von Geburts- und Kontaktdaten für die Zusendung eines Geburtstagsrabatts zulässig?

Hier ist zu unterscheiden:

1.) Zusendung per Post

Die Zusendung eines Geburtstagsrabatts per Brief ist unter Nutzung bereits vorhandener Kundendaten ist ohne Einwilligung des Kunden zulässig, da sie durch das berechtigte Interesse des Händlers an personalisierter Direktwerbung gerechtfertigt wird.

2.) Zusendung per Mail oder über soziales Netzwerk

Dahingegen ist die Zusendung eines Geburtstagsrabatts per Mail oder über ein soziales Netzwerk ohne vorige ausdrückliche Einwilligung des Nutzers unzulässig.

Verfügt der Händler bereits über Mailadresse und Geburtsdatum, muss er vor der Rabattzusendung dennoch eine ausdrückliche Einwilligung hierin einholen. Der Versand eines Geburtstagsrabatts wird durch eine etwaige Newsletter-Einwilligung nicht gedeckt (weil zusätzlich das personenbezogene Geburtsdatum verarbeitet wird), es sei denn, dem Kunden wurde unter Aufforderung zur Eingabe seines Geburtsdatums schon bei der Newsletter-Anmeldung der Geburtstagsrabatt angekündigt.

Verfügt der Händler noch nicht über das Geburtsdatum und will dieses für den Geburtstagsrabatt einholen, so muss im Zuge der Einholung der Kunde/Nutzer darüber informiert werden, dass er mit der Bereitstellung seines Geburtsdatums in den Erhalt eines Geburtstagsrabatts auf einem zu nennenden elektronischen Kommunikationsweg einwilligt. Soll das Geburtsdatum darüber hinaus auch noch für

andere Zwecke genutzt werden dürfen, müssen diese im Einwilligungstext deutlich herausgestellt sein.

Frage: Bleibt der Einsatz von Facebook Pixel weiterhin zulässig?

Ja. Der Beginn von Datenverarbeitungen durch Facebook Pixel wird von der ausdrücklichen Einwilligung des Nutzers abhängig gemacht, welche Datenvorgänge auch unter der DSGVO rechtfertigt.

Hinweis: Die IT-Recht Kanzlei wird ihren Mandanten zeitig eine DSGVO-konforme Datenschutzerklärung (inkl. diverser Handlungsanleitungen) zur Verfügung stellen. Diese wird selbstverständlich auch eine wählbare Klausel zum Einsatz von "Facebook Pixel" enthalten.

Frage: Wie muss die DSGVO gehandhabt werden, wenn kundenspezifische Artikel angeboten werden, auf denen Adressendaten von Kunden angebracht werden (Stempel, Drucksachen etc.)?

Hier ist das Anbringen von Kundendaten auf dem Produkt selbst durch die vertragliche Erforderlichkeit gerechtfertigt. Das Anbringen der Kundendaten als Datenverarbeitung ist Teil der geschuldeten Leistung und mithin legitim. Eine gesonderte Einwilligung muss nicht eingeholt werden.

Hinweis: Obiges gilt sowohl gegenüber Privat- als auch gegenüber Firmenkunden.

D. Fragen zum Datenschutzbeauftragten

Frage: Brauchen Online-Händler künftig einen Datenschutzbeauftragten?

Es gilt Folgendes:

1. 20 oder mehr Personen verarbeiten ständig automatisiert personenbezogene Daten

Wenn 20 oder mehr Personen ständig mit der automatisierten Verarbeitung personenbezogene Daten beschäftigt sind, ist ein Datenschutzbeauftragten immer zu benennen (§ 38 BDSG-Neu).

2. Weniger als 20 Personen verarbeiten ständig automatisiert personenbezogene Daten

Wenn weniger als 20 Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind, muss kein Datenschutzbeauftragter benannt werden, es sei denn:

- es wird eine Datenverarbeitung vorgenommen wird, die einer sogenannten Datenschutz-Folgeabschätzung (DSFA) unterliegt. Die Regeltätigkeiten eines Online-Händlers lösen keine DSFA aus. Bei Online-Händlern könnte eine DSFA bei einer automatisierten Bonitätsprüfung in Frage kommen. Im Regelfall wird ein Online-Händler aber nur bei Vorleistung eine Bonitätsprüfung veranlassen. Eine solche Bonitätsprüfung löst aber keine Datenschutz-Folgeabschätzung aus. Die Versagung eines Vertrages wegen fehlender Bonität ist keine Beeinträchtigung des Kunden und ist von ihm hinzunehmen. Ebenfalls nicht erfasst von einer Datenschutz-Folgeabschätzung sind personalisierte Werbung und Tracking.
- es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet. Dies trifft jedoch auf den Online-Händler nicht zu, dessen Haupttätigkeit der Vertrieb von Produkten ist. Hier ist die Datenverarbeitung von Auskunfteien, Adresshändlern und Instituten zur Markt- und Meinungsforschung gemeint.

Weitere Informationen zum Thema finden Sie hier.

Frage: Wie bestellt man günstig einen Datenschutzbeauftragten?

Die IT-Recht Kanzlei zeigt hier eine Lösung für eine kostengerechte Bestellung eines Datenschutzbeauftragten auf.

Frage: Ist die Maßzahl an Mitarbeitern überschritten, wenn 20 oder mehr Mitarbeiter im Rahmen ihrer Tätigkeit mit personenbezogenen Daten in Berührung kommen?

Grundsätzlich nicht. Ein Datenschutzbeauftragter muss nur bestellt werden, wenn mindestens 20 Mitarbeiter ständig personenbezogene Daten **automatisiert** verarbeiten. Die Kerntätigkeit dieser Mitarbeiter müsste also gerade in der systematischen und technisch-automatisierten Datenverarbeitung bestehen. Ein bloßes „In-Berührung-Kommen“ mit personenbezogenen Daten reicht nicht aus.

Frage: Müssen bei den Mitarbeitergrenzen externe Kooperationspartner (Zahlungsdienstleister, Bonitätsprüfer) und deren Angestellte mitgezählt werden?

Nein. Für die Mitarbeitergrenzen sind ausschließlich eigene Beschäftigte des Online-Händlers zu berücksichtigen.

Frage: Wann verarbeiten Mitarbeiter Daten „automatisiert“?

Wenn sie die Verarbeitung unter Einsatz von IT-Technik (z.B. am PC) durchführen. Nicht automatisierte Verarbeitungsvorgänge sind nur solche, bei denen keinerlei Technik genutzt wird, wie z.B. bei Auswertungen von Karteien oder Aktensammlungen.

Frage: Müssen Mitarbeiter, die mit der Auftragsbearbeitung, Produktion, Buchhaltung, dem Marketing und dem Versandmanagement betraut sind, berücksichtigt werden?

Grundsätzlich ja. Derartige Mitarbeiter sind mit der kontinuierlichen Verarbeitung personenbezogener Daten betraut und tun dies im Regelfall automatisiert unter Einsatz von IT-Technik.

Frage: Zählen auch Auszubildende und Praktikanten zu den Mitarbeitern?

Ja. Die Art der Anstellung ist egal. Entscheidend ist die tatsächliche Eingliederung in den Betrieb. Verarbeiten Auszubildende oder Praktikanten ständig personenbezogene Daten automatisiert, zählen sie zu den maßgeblichen Mitarbeitern.

Frage: Hängt die Pflicht zur Bestellung eines Datenschutzbeauftragten von der Art der Geschäftstätigkeit ab?

Nein. Die Voraussetzungen für die verpflichtende Bestellung eines Datenschutzbeauftragten gelten unabhängig von der Branchenzugehörigkeit. Ein Online-Händler könnte eine Verpflichtung nicht mit der Begründung abwenden, seine Haupttätigkeit sei der Verkauf von Waren.

Frage: Muss ein Datenschutzbeauftragter schriftlich bestellt werden?

Das ist aus Beweisgründen zu empfehlen, obwohl die DSGVO nichts über die Art der Bestellung sagt.

Frage: Können auch externe Datenschutzbeauftragte benannt werden?

Ja. Datenschutzbeauftragte müssen nicht Mitarbeiter des Unternehmens sein.

Frage: Kann auch eine juristische Person (ein Unternehmen) Datenschutzbeauftragter sein?

Nein. Datenschutzbeauftragter kann nur eine natürliche (Einzel-)Person sein.

Frage: Welche fachlichen Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?

Die DSGVO fordert, dass der Datenschutzbeauftragte

- eine gewisse berufliche Qualifikation aufweist,
- Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis hat und
- in der Lage ist, die gesetzlich definierten Aufgaben zu erfüllen

Diese Anforderungen sind allgemein formuliert, damit sie auf sämtliche Wirtschaftszweige und Unternehmensformen passen. Je nach Betriebsgröße und Art der Datenverarbeitungen müssen sie aber konkretisiert werden.

Jedenfalls ist von Nöten, dass der Datenschutzbeauftragte über rechtliche, technische und organisatorische Kenntnisse auf dem Gebiet des Datenschutzes verfügt.

Daneben muss der Datenschutzbeauftragte mit den branchenspezifischen Besonderheiten vertraut sein. Dies umfasst das Wissen über spezialgesetzliche Datenschutzvorschriften, Kenntnisse der Informations- und Telekommunikationstechnologie sowie der Datensicherheit.

Zudem muss er wegen in seiner Funktion zuverlässig und neutral sein.

Ein Zertifikat oder eine bestimmte Ausbildung ist aber nie zwingend.

Auch unter Geltung der DSGVO können die Leitlinien des sog. Düsseldorfer Kreises für die beruflichen Anforderungen an den Datenschutzbeauftragten herangezogen werden.

Weitere Informationen zum Thema finden Sie auch hier.

Frage: Kann unter den obigen Voraussetzungen also „jedermann“ Datenschutzbeauftragter werden?

Grundsätzlich ja. Allerdings darf kein Interessenkonflikt entstehen. Dies ist vor allem bei internen Datenschutzbeauftragten denkbar. Interessenkonflikte entstehen insbesondere dann, wenn der eingesetzte Datenschutzbeauftragte zusätzlich einer anderen Tätigkeit im Unternehmen nachgeht. Das ist ihm zwar gestattet, er muss sich dann aber unter Umständen selbst kontrollieren. Eine Pflicht zur Selbstkontrolle kann insbesondere bei Mitarbeitern der IT-Abteilung, Personalabteilung und der Geschäftsführung angenommen werden.

E. Fragen zur Speicherung bestimmter Daten und zur Speicherdauer

Frage: Gelten Speicherfristen auch für Daten juristischer Personen (GmbHs, GbRs etc.)?

Speicherfristen nach der DSGVO gelten für generelle Daten juristischer Personen nicht. Nach Erwägungsgrund 14 findet die DSGVO auf personenbezogene Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person, keine Anwendung. Derartige Daten können somit grundsätzlich beliebig lang gespeichert werden.
Besondere gesetzliche Aufbewahrungsfristen, etwa der 10-Jahres-Zeitraum für Rechnungen und Buchungsbelege, gelten aber auch für juristische Personen.

Achtung: sofern personenbezogene Daten betroffen sind, die auf die hinter einer juristischen Person stehenden natürlichen Personen durchgreifen (etwa Daten des Geschäftsführers einer GmbH), finden die DSGVO-Speicherfristen (sowie die sonstigen Vorschriften) aber wieder Anwendung. Insofern sind dem Verordnungsschutz nur solche Daten bezogen, die gerade die Rechtspersönlichkeit einer Personen- oder Kapitalgesellschaft bzw. eines Vereins betreffen.

Frage: Ist die Speicherung von IP-Adressen in Access- und Errorlogs des Webservers unbedenklich?

Jein. IP-Adressen sind personenbezogene Daten, das heißt die Speicherung in Log-Dateien bedarf grundsätzlich einer Rechtfertigung nach DSGVO. Logfiles können statistisch ausgewertet werden und dienen daher der Verbesserung der Stabilität und Funktionalität der Website. Dies begründet ein überwiegendes berechtigtes Interesse des Online-Händlers an deren Speicherung und macht sie insoweit unbedenklich.

Auf die Speicherung von Accers- und Errorlogs ist allerdings unter Angabe der Rechtsgrundlage (Art. 6 Abs. 1 lit. f DSGVO) und Nennung des berechtigten Interesses zwingend in der Datenschutzerklärung zu informieren.

Hinweis: die neue DSGVO-konforme Datenschutzerklärung der IT-Recht Kanzlei wird eine wählbare Klausel zur Log-Files enthalten.

Frage: Was müssen die in der Datenschutzerklärung erforderlichen Informationen über die Dauer der Speicherung enthalten?

In der Information genügt folgender Hinweis:

> *"Die Dauer der Speicherung von personenbezogenen Daten bemisst sich anhand der jeweiligen gesetzlichen Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind und/oder unsererseits kein berechtigtes Interesse an der Weiterspeicherung fortbesteht. Gebietet die Ausübung von Interventionsrechten die Löschung, werden die entsprechenden Daten unverzüglich gelöscht."*

Eine Angabe von Zeitspannen (10 Jahre o.ä.) ist nicht erforderlich, weil für verschiedene Datensätze je nach Gesetz auch verschiedene Aufbewahrungsfristen bestehen. Es genügt also, als Kriterium für die Dauer der Speicherung pauschal auf die gesetzlichen Aufbewahrungsfristen zu verweisen.

Hinweis: die DSGVO-Datenschutzerklärung der IT-Recht Kanzlei wird diese Pflichtinformation selbstverständlich standardmäßig enthalten.

Frage: Was droht, wenn personenbezogene Daten über die maximale Speicherdauer hinaus gespeichert werden?

Werden personenbezogene Daten auch nach Ablauf der gesetzlichen Aufbewahrungsfristen oder nach berechtigter Ausübung des Löschungsrechts durch Betroffene weiter gespeichert, drohen einerseits Interventionen der Aufsichtsbehörden. Grundsätzlich ergeht hier zunächst eine Verfügung, mit der die Löschung angeordnet wird. Kommt der Händler der Verfügung nicht nach, werden Bußgelder verhängt.

Andererseits muss der Händler bei Überschreitung der zulässigen Speicherdauer auch Unterlassungsansprüche von Mitbewerben fürchten.

Aber: starre gesetzliche Aufbewahrungsfristen gibt es nur vereinzelt für bestimmte Daten (etwa nach der Abgabeordnung für steuerrechtlich relevante Daten oder dem Handelsgesetzbuch für Geschäftsunterlagen). Im Regelfall ist die Speicherung nach der DSGVO solange zulässig, wie die jeweilige Rechtsgrundlage für die Verarbeitung (Vertragliche Erforderlichkeit; berechtigte Interessen; Einwilligung) beim Händler fortbesteht. Dass dem nicht mehr so ist, muss nicht der Händler, sondern die Aufsichtsbehörde oder der Mitbewerber nachweisen.

Frage: Inwiefern und wann müssen Händler Daten von nicht registrierten Kunden nach einer Bestellung löschen?

Hier ist je nach Speicherort und -zweck zu unterscheiden:

1.) Shop-IT-System: 6 Monate

Tätigen Kunden, die kein Kundenkonto angelegt haben, eine Bestellung, so sollte der Händler die online erhobenen Kundendaten grundsätzlich nach ca. 6 Monaten **aus dem Shop** löschen.

Dies deshalb, weil die Löschung zu erfolgen hat, wenn der Zweck der Verarbeitung entfällt. Kundendaten nicht registrierter Kunden werden für die Vertragsdurchführung verarbeitet. Der 6-Monats-Zeitraum stellt hinreichend sicher, dass etwaige nachvertragliche Mängelanzeigen und damit verbundene Rechtsausübungen meist noch auf Basis der erhobenen Daten bearbeitet werden können. Dies fällt noch unter den Zweck der Vertragsdurchführung. Das Begrenzen der Speicherdauer auf die Widerrufsfrist wäre zu kurz. Benötigt der Händler die Daten länger als 6 Monate, etwa für einen Jahresabschluss oder Jahresabrechnungen, kann die Frist verlängert werden.

2.) Rechnungen und Buchungsbelege: 10 Jahre

Rechnungen (ob digital oder gedruckt) und Buchungsbelege, die die Daten enthalten, müssen dahingegen aus steuerrechtlichen Gründen 10 Jahre aufbewahrt werden.

3.) Kundendaten in der Warenwirtschaft: 2 Jahre nach Lieferung

Kundendaten, die in Unterlagen oder Dateien der Warenwirtschaft gespeichert sind und die die Rückverfolgbarkeit von Warenbewegung sowieso die Zuordnung von Käuferidentitäten im Gewährleistungs- und Garantiefall sicherstellen, sollten dahingegen so lange aufbewahrt werden, wie die regelmäßige Gewährleistungszeit läuft. Das sind 2 Jahre nach Lieferung der bestellten Ware.

Daten von Kunden mit Kundenkonto können demgegenüber so lange gespeichert werden, wie das Kundenkonto bestehen bleibt.

Frage: Wie verhält es sich mit Kundendaten der Warenwirtschaft, wenn diese durch einen zusätzlichen Dienst zur Rechnungserstellung genutzt werden (müssen)?

Wird ein Dienst verwendet, der für die Rechnungserstellung unmittelbar auf Kundendaten der Warenwirtschaft zurückgreift (z.B. AfterBuy) und könnten Rechnungen bei Löschung der Daten nach 2 Jahren anderenfalls nicht mehr generiert oder digital eingesehen werden, dürfen die Daten für die für Rechnungen vorgesehene Dauer von 10 Jahren gespeichert werden.

Frage: Welche Daten sind nach Ablauf der Speicherdauer zu löschen?

Nach Ablauf der jeweiligen Speicherdauer sind alle personenbezogenen Daten zu löschen, die für den jeweiligen Betroffenen vorliegen.

Frage: Müssen Rechnungen auf Wunsch des Kunden vernichtet werden?

Innerhalb der gesetzlichen Speicherfrist auf keinen Fall. Rechnungen müssen sogar zwingend 10 Jahre aufbewahrt werden. Eine Kundenaufforderung ist aber berechtigt und muss befolgt werden, wenn die Rechnung über die benannte Speicherdauer hinaus aufbewahrt und nicht eigeninitiativ vernichtet wird.

F. Fragen zu Betroffenenrechten

Frage: Muss bei Auskunftsanfragen innerhalb eines Monats Auskunft erteilt werden oder innerhalb eines Monats die Bearbeitung bestätigt werden?

Es muss grundsätzlich innerhalb eines Monats die verlangte Auskunft erteilt werden.

Diese Frist kann unter Angabe von Gründen **durch Mitteilung innerhalb des ersten Monats** um 2 weitere Monate verlängert werden, wenn dies wegen der Vielschichtigkeit oder der Vielzahl eingegangener Anfragen erforderlich ist.

Frage: Gibt es Dokumentations-/Aufbewahrungs-/Bestätigungspflichten im Fall eines Kundenwunschs auf Löschung seiner Daten?

Dokumentations- und Aufbewahrungspflichten gibt es nicht. Eine Bestätigungspflicht existiert insofern, als dass der Antrag grundsätzlich binnen eines Monats bearbeitet und beantwortet werden muss. Steht dem Betroffenen das Recht auf Löschung zu, besteht die Beantwortung in der Bestätigung der Löschung. Kommt der Händler zu dem Entschluss, dass keine Löschpflicht besteht, besteht die Beantwortung in der Ablehnung des Antrags unter Angabe von Gründen.

Frage: Welchen Drittparteien gegenüber muss die Löschung mitgeteilt werden?

Macht ein Betroffener erfolgreich sein Recht auf Löschung geltend, ist die Löschung allen Empfängern mitzuteilen, welchen die Daten offengelegt wurden.
Wer zu informieren ist, hängt aber davon ab, welche konkreten Daten gelöscht wurden, inwieweit die Löschung ferngewirkt hat und in welcher Form die Daten übermittelt wurden.

Daher ist die Informationspflicht auf 3 Arten beschränkt:

1.) Empfängerkreis

Zunächst muss bestimmt werden, an wen die zu löschenden Daten übermittelt wurden. Für jede Art der zu löschenden Daten kommt hier ein abgrenzbarer Kreis an Drittempfängern in Betracht (z.B. für Adressdaten: Versanddienstleister + ggf. abhängig von der Zahlungsmethode Zahlungsdienstleister und Bonitätsprüfer).

2.) Nicht von Löschung durch den Händler betroffen

Sodann ist zu beachten, dass eine Löschung durch den Händler bereits gegenüber Dritten den Zugriff auf die Daten sperren kann. So gilt die Informationspflicht nur gegenüber denjenigen Dritten, bei denen die offengelegten Daten trotz Löschung fortbestehen. Website-Hoster und Cloud-Anbieter sind also nicht zu informieren, weil eine Löschung durch den Händler die Datenbestände automatisch auch mit Wirkung für diese beseitigt

3.) Zugriffsmöglichkeit

Schließlich ist wichtig, dass die ermittelten Dritten auf die Daten ihrem Inhalt nach müssen zugreifen können. Empfänger von verschlüsselten Datensätzen müssen nicht informiert werden, weil sie die Daten nicht entgegen des Betroffeneninteresses über die Löschung hinaus personenbezogen nutzen könnten.

Um den Informationspflichten nachkommen zu können, sollten sämtliche Datenübertragungen in jedem Fall sorgsam dokumentiert werden.

Frage: Wie ist die Information gegenüber Drittempfängern vorzunehmen?

Bestimmte Erfordernisse an die Form oder Art des Kommunikationsmittels gibt es nicht. Möglich ist die Information also in jedem denkbaren Wege (Mail, Brief, Telefon etc.).

Empfehlenswert ist die Vorbereitung einer Muster-Benachrichtigung, in welche nur noch der Name des Betroffenen und die von der Löschung betroffenen Daten eingesetzt werden müssen.

Fristen für die Information gibt es ebenfalls nicht. Es ist aber davon auszugehen, dass diese unverzüglich (= ohne schuldhaftes Zögern) erfolgen sollte.

Frage: Müssen Online-Händler Kontaktformulare schaffen, welche zur Geltendmachung von Rechten des Betroffenen genutzt werden können?

Nicht zwingend. Kontaktformulare für die Rechtsausübung durch Betroffene (etwa für den Antrag auf Auskunft oder Löschung) stellen zwar ein geeignetes Mittel dar, um dem Betroffenen die Durchsetzung seiner Rechte zu erleichtern. Auch können solche Kontaktformulare für den Händler nützlich sein, um Anfragen schnell und automatisch nach Anliegen zu sortieren und dann zu bearbeiten.

Notwendig ist die Bereitstellung von Kontaktformularen aber nicht. Es genügt insofern, dass der Betroffene aus der Datenschutzerklärung die Kontaktdaten des Verantwortlichen einsehen kann.

Nähre Informationen zur Bereitstellung von Kontaktformularen für die Ausübung von Betroffenenrechten finden Sie hier.

Frage: Können Händler Muster für die Mitteilungen/Reaktionen verwenden, die innerhalb eines Monats nach Antrag des Betroffenen erforderlich sind?

Ja, dies ist sogar zu empfehlen.

Online-Händler werden für den Fall der Rechtsausübung durch Betroffene gehalten, die eingehenden Anträge innerhalb von einem Monat zu bearbeiten und entsprechend zu reagieren.

Um die Bearbeitung schnell und lückenlos zu vollziehen, ist es sinnvoll, Muster für verschiedene Antragsszenarien zu verwenden. In diesen müssen dann nur noch die auf den jeweiligen Betroffenen zugeschnittenen Informationen zusammengetragen werden, bevor sie an diesen übermittelt werden. Die Muster sollten also „Grundgerüste“ für die in Betracht kommenden Reaktionen auf Betroffenenanträge sein.

Muster-Mitteilungen empfehlen sich für

1.) Fristverlängerung und Verweigerung der Antragsbearbeitung

- Information über eine Fristverlängerung für die Bearbeitung mit Gründen
- Verweigerung der Bearbeitung wegen offenkundiger Unbegründetheit oder unzumutbarer Antragshäufung

2.) Anträge auf Auskunft

- Bestätigung der Verarbeitung von personenbezogenen Daten des anfragenden Betroffenen und Auskunft über die konkreten Daten (Art. 15 Abs. 1 Satz 1 DSGVO)
- Information, dass keine personenbezogenen Daten des Betroffenen verarbeitet werden

3.) Anträge auf Löschung

- Bestätigung der Löschung der Betroffenendaten
- Ablehnung der Löschung wegen Fortbestand des Verarbeitungszwecks (etwa berechtigtes Interesse oder Vertragsdurchführung)
- Unterrichtung über Drittempfänger von personenbezogenen Daten gegenüber dem Betroffenen (Art. 19 S. 2 DSGVO)

4.) Anträge auf Datenübertragung

- Auflistung der bereitgestellten personenbezogenen Daten zwecks der Übertragung an einen Dritten durch den Betroffenen (Art. 20 Abs.1 DSGVO)

Hinweis: die IT-Recht Kanzlei wird Muster-Mitteilungen zeitnah ausarbeiten und ihren Mandaten im Mandatenportal zur Verfügung stellen.

G. Fragen zu internationalen Datenvorgängen

Frage: Bleiben Plug-Ins und Analysedienste, die Daten in die USA übermitteln, weiterhin zulässig?

Im Regelfall ja. Die meisten großen Plug-In- und Analysedienstanbieter (Google, Facebook, Twitter) mit Sitz in den USA sind für ein us-europäisches Datenschutzübereinkommen (sogenanntes „Privacy Shield“) zertifiziert. Dieses stellt die Einhaltung europäischer Datenschutzstandards auch in den USA sicher und macht den Einsatz solcher Dienste durch deutsche Händler unbedenklich. Freilich ist über jedes Plug-In/jeden Analysedienst in der Datenschutzerklärung einzeln zu informieren.
Sofern einzelne Anbieter nicht zertifiziert sind (derzeit z.B. „Pinterest“), werden Sie auf die damit verbundenen Risiken innerhalb des neuen DSGVO-konformen Datenschutzgenerators der IT-Recht Kanzlei hingewiesen werden.

Frage: Müssen Händler bei EU-weitem Versand die Einhaltung der DSGVO gegenüber ausländischen Datenschutzbehörden nachweisen?

Nein. Auch bei EU-weitem Versand bleiben deutsche Aufsichtsbehörden zuständig, sofern die Verarbeitung der Daten im Inland erfolgt. Maßgeblich ist insofern die Niederlassung des Händlers. Sitzt der Händler in Deutschland und bereitet von hier den Versand vor, haben Aufsichtsbehörden des EU-Mitgliedsstaats, in den versendet werden soll, keine Zuständigkeit.

Frage: Muss bei Übermittlungen von Daten an Drittparteien stets eine schriftliche Bestätigung eingeholt werden, dass die DSGVO eingehalten wird?

Nein. Sofern diese Drittparteien in der EU niedergelassen sind, sind sie ohnehin direkt an die DSGVO gebunden.

Bei Datenübermittlungen an Parteien außerhalb der EU würde eine einzeln eingeholte Bestätigung der DSGVO-Einhaltung demgegenüber nicht ausreichen, weil die Anforderungen an den Datenschutz hier besonders streng sind.

So ist die Zulässigkeit von Übermittlungen ins EU-Ausland vordergründig dann gegeben, wenn die Kommission für das jeweilige Land einen sogenannten „Angemessenheitsbeschluss“ verabschiedet hat oder ein spezifisches Datenschutzübereinkommen besteht.

Ein Angemessenheitsbeschluss existiert derzeit für diese Länder:

- Schweiz
- Kanada
- Argentinien
- Guernsey
- Uruguay
- Insel Man
- Jersey
- Faröer Inseln
- Andorra
- Israel
- Neuseeland

Ein Datenschutzübereinkommen existiert dahingegen in Form des sog. „Privacy Shield“ mit den USA, erfordert aber eine eigenständige Zertifizierung von US-Unternehmen.

Existiert weder ein Angemessenheitsbeschluss für das noch ein Abkommen mit dem Drittland, müssen andere Garantien für den Datenschutz geschaffen werden. Dies sind vor allem Standard-Datenschutzverträge (von der EU vorbereitet) mit und von der EU genehmigte Verhaltensregeln gegenüber dem jeweiligen Empfänger im Drittland.

Eine bloße schriftliche Bestätigung der DSGVO-Einhaltung genügt aber in keinem Fall.

H. Fragen zu technischen und organisatorischen Maßnahmen

Frage: Werden unter der DSGVO Absicherungen der Räumlichkeiten zum Zweck der Datensicherheit erforderlich?

Nein. Zwar müssen Händler auch unter der DSGVO „geeignete technische und organisatorische Maßnahmen“ zur Gewährleistung der Datensicherheit treffen. Die DSGVO verfolgt aber den Ansatz, dass die Schutzmaßnahmen vom Risiko für die Betroffenen bei etwaigen Datenlecks oder einem Datenklau abhängen sollen. Je wahrscheinlicher Rechte und Freiheiten der Betroffenen tangiert werden können, desto höher muss das Schutzniveau sein.

Händler verarbeiten in der Regel keine mit einem gesteigerten Risiko behafteten Daten, sodass die bisher verwendeten IT-Lösungen (Verschlüsselung, Server- und PC-Zuverlässigkeit, Passwörter) auch unter der DSGVO ausreichen.

Frage: Müssen IT-Richtlinien zum Umgang mit Daten für Mitarbeiter aufgestellt werden?

Das hängt von der Größe des Unternehmens ab. IT-Sicherheitsrichtlinien geben Mitarbeitern einen bestimmten, möglichst datensicheren Umgang mit IT-Systemen vor und können so eine geeignete „technische und organisatorische Maßnahme“ für die Datensicherheit im Sinne der DSGVO sein. Allerdings sind derartige Richtlinien nur dann sinnvoll, wenn ein Unternehmen über so viele Mitarbeiter mit eigenständigen Arbeitsaufgaben verfügt, dass eine durchgängige Kontrolle des Datenverkehrs und der Verwendung von IT-Systemen nicht anders gelingen kann. Für einen Online-Händler mit 3 Mitarbeitern ist die Aufstellung von Richtlinien weniger sinnvoll, für einen mit 10 oder mehr Mitarbeitern dahingegen schon.

Richtwert für die Zweckmäßigkeit von IT-Richtlinien kann das Erreichen der Voraussetzung für die verpflichtende Bestellung eines Datenschutzbeauftragten sein (= wenn mindestens 10 Personen ständig automatisiert personenbezogene Daten verarbeiten).

Frage: Was kann in IT-Richtlinien geregelt werden?

In IT-Richtlinien können Mitarbeitern verpflichtende IT-Sicherheitsstandards vorgegeben werden, deren Einhaltung einen hinreichenden Datenschutz gewährleistet.

Dazu gehört beispielsweise die Verpflichtung, dass

- Passwörter nicht nur eine bestimmte Sicherheitsstufe erreichen müssen, sondern auch ausschließlich über bestimmte Passwort-Manager gespeichert werden dürfen
- Passwörter regelmäßig zu ändern sind
- ein Arbeitsgerät bei Verlassen des Arbeitsplatzes zu sperren ist

Auch kann geregelt werden, dass

- private oder sonstige Geräte von außerhalb nur unter bestimmten Voraussetzungen ans Firmennetzwerk angeschlossen werden dürfen
- private Social-Media-Accounts nicht oder nur über eine Verschlüsselung über den Browser des Firmen-PCs abgerufen werden dürfen

Frage: In welcher Form sind IT-Richtlinien zu fassen?

Zwingend schriftlich. Zudem sollte von jedem Mitarbeiter die schriftliche Bestätigung (mit Datum und Unterschrift) eingeholt werden, dass er die Richtlinie akzeptiert.

Nur so kann die IT-Richtlinie als hinreichender Nachweis für eine „technische und organisatorische Maßnahme“ im Sinne der DSGVO dienen.

Frage: Reicht der Einsatz von Passwörtern zur Verschlüsselung von Dateien, Programmen und sonstigen Speicherorten von Daten?

Grundsätzlich ja. Die Passwort-Verschlüsselung von Datensätzen (etwa Ordner) sowie von Dateien (Excel-Tabellen, Dokumente) und Programmen, in denen personenbezogene Daten gespeichert werden (etwa Outlook) , ist eine hinreichende Sicherheitsmaßnahme gegen Fremdzugriffe. Das Passwort sollte allerdings so gewählt werden, dass es nicht leicht entschlüsselt werden kann.

I. Fragen zur Datenverarbeitung im Auftrag

Frage: Muss mit jedem Auftragsverarbeiter ein separater Vertrag geschlossen werden?

Ja. Jede Auslagerung von Verarbeitungsprozessen an einen Dritten setzt einen individuellen Vertrag mit diesem voraus, Art. 28 Abs. 3 DSGVO

Frage: Muss der Verarbeitungsvertrag zwingend handschriftlich unterzeichnet werden?

Nicht mehr. Unter der DSGVO ist der Abschluss eines Verarbeitungsvertrags (anders als nach derzeitigem Recht) aus elektronisch, also per Mausklick, möglich, Art. 28 Abs. 9 DSGVO.

Frage: Reicht die Zusendung der Vertragsdokumente an den Auftragsverarbeiter per Mail für den Abschluss?

Nein. Der Vertrag wird freilich nur wirksam, wenn beide Parteien ihren Rechtsbindungswillen ausdrücklich (etwa per Unterschrift oder elektronisch per Klick) bestätigen.

Eine Zusendung per Mail für den eigentlichen Vertragsschluss genügt für sich alleine nie.

Je nach gewählter Form für den Vertragsschluss (handschriftliche Signatur oder elektronisch) kann die E-Mail aber wie folgt zum Einsatz kommen:

1.) Handschriftliche Unterzeichnung

Der Vertrag mit Unterschrift des Auftraggebers kann per Mail an den Auftragsverarbeiter versendet werden, muss für seine Wirksamkeit aber mit Unterschrift des Auftragsverarbeiters wieder an ersteren zurückgelangen.

Aus Beweisgründen empfiehlt sich eine doppelte Ausführung, sodass sowohl der Auftraggeber als auch der Auftragsverarbeiter jeweils ein Vertragsexemplar erhalten.

Hinweis: als Alternative zum Versand via Mail kann das Vertragsdokument auch auf der Website des Auftraggebers zum Download bereitgestellt, vom Auftragsverarbeiter unterzeichnet an den Auftraggeber zurückgesendet und sodann vom Auftraggeber unterschrieben werden.
Eine Kopie mit beiden Unterschriften sollte dann auch dem Auftragsverarbeiter zugehen.

2.) Elektronischer Abschluss

Wird der Vertrag per Mausklick elektronisch geschlossen, sollte die Bestätigung des Vertrages sowie dessen Abschrift dem Auftragsverarbeiter im Anschluss per Mail zugehen.

Frage: Entsteht beim Anbieten über eBay, Amazon und Co. ein Verhältnis der Auftragsverarbeitung und müssen hierfür gesonderte Verarbeitungsverträge geschlossen werden?

Nein. Der Händler ist zu keinem Zeitpunkt Auftragsverarbeiter einer Handelsplattform, noch ist diese jemals Auftragsverarbeiter des Händlers. Verträge über die Auftragsdatenverarbeitung müssen also nicht geschlossen werden.

Die Plattform, auf der Nutzer registriert sind, übermittelt Kundendaten erst nach Vertragsschluss an den Händler. Er ist somit nie Auftragnehmer, weil er die Daten selbst für die Vertragsdurchführung nutzt und nicht nur unselbstständig als Gehilfe der Plattform tätig wird. Er ist aber auch nie Auftraggeber, weil er keine Herrschaft über die Daten hat und erst nach Vertragsschluss auf diese zugreifen kann.

Bis zum Vertragsschluss ist die Plattform Verantwortliche für die von Nutzern bereitgestellten Daten. Bei Verarbeitung der Daten durch den Händler nach Vertragsschluss wird dieser im Rahmen der Vertragsdurchführung Datenverantwortlicher

Frage: Ist die Inanspruchnahme eines Webhosters (Strato, Estugo) für den Online-Shop eine Auftragsverarbeitung?

Ja. Über den Webhoster werden alle Datenverarbeitungsprozesse für die Shop-Plattform abgewickelt, sodass hier zwingend ein Datenverarbeitungsauftrag zu schließen ist.

Viele Hoster bieten einen solchen bereits in vorgefertigter Version auf Anfrage an, s. z.B. für „estugo“ https://www.estugo.de/support/adv-vertrag/

Frage: Ist der Einsatz einer Shop-Software (z.B. Gambio) eine Auftragsverarbeitung?

Regelmäßig nein. Die bloße Nutzung der Shop-Software von Gambio auf Installationsbasis stellt keine Auftragsverarbeitung dar, weil diese vom Händler selbst zu installieren ist und grundsätzlich keine Daten an Gambio übertragen werden. Hier werden alle datenschutzrelevanten Prozesse allein in der Verantwortlichkeit des Händlers abgewickelt, ohne dass Gambio als Software-Provider an diesen Prozessen teilhätte.

Etwas anderes gilt aber für die Nutzung der "Gambio-Cloud" und des "Gambio Payment Hub". Hier erfolgt jeweils eine Übermittlung von Kundendaten an Gambio zum Zwecke der Funktionsgewährleistung. Im Falle der Gambio-Cloud werden alle Datenbestände des Händler-Shopsystems fremdgehostet und fremdverarbeitet. Jegliche Datenprozesse im Shop werden mithin über Gambio abgewickelt. Im Falle des "Gambio Payment Hub" werden Kontakt-, Personen- und Zahlungsdaten von Kunden zur Abwicklung einer Bezahlung über Gambio übertragen. Somit liegt sowohl bei Inanspruchnahme der "Gambio Cloud" als auch bei Nutzung des "Gambio Hub" eine jeweils eigenständige Auftragsverarbeitung vor.

Frage: Ist das Betreiben einer Wordpress-Plattform mit einem eigenen Hosting-Dienst für Dritte eine Auftragsverarbeitung?

Wer eine Wordpress-Plattform auf seinem eigenen Server betreibt und Kunden anbietet, über diese Plattform Webseiten und/oder Shops zu hosten, ist als eigenständiger Webhoster Auftragsverarbeiter der Kunden. Insofern muss mit jedem Kunden ein Vertrag über die Auftragsverarbeitung geschlossen werden.

Frage: Ist die Beauftragung von Versanddienstleistern eine Auftragsverarbeitung?

Nein. Zwar sind Versanddienstleister für die ordnungsgemäße Zustellung auf die Bereitstellung von Kundendaten angewiesen. Eine Auftragsverarbeitung liegt aber nicht bei in Anspruch genommenen Tätigkeiten vor, die im eigentlichen Kern nicht den Umgang (Erhebung, Verarbeitung, Nutzung) mit personenbezogenen Daten betreffen, sondern in denen andere Dienstleistungsschwerpunkte im Vordergrund stehen und der dabei notwendigerweise mit verbundene Kontakt mit personenbezogenen Daten nur ein unvermeidliches "Beiwerk" darstellt.

Frage: Liegt eine Auftragsdatenverarbeitung durch IT-Dienstleister vor?

Regelmäßig ja. Ist Gegenstand des Vertrages zwischen Verantwortlichem und dem Dienstleister die die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten in Systemen des Auftraggebers) und besteht in diesem Rahmen für den Dienstleister die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich um eine Auftragsverarbeitung und die Anforderungen des Art. 28 DSGVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen.

Ist ein Datenzugriff durch den IT-Dienstleister hingegen ausgeschlossen, ist nicht von einer Auftragsverarbeitung auszugehen.

Frage: Ist der Einsatz von Newsletter-Versanddiensten (etwa „Mailchimp“) eine Auftragsverarbeitung?

Regelmäßig ja. Dienstleistern, die Newsletter für einen Verantwortlichen versenden, werden zum Zwecke der werblichen Ansprache, die sie anstelle und im Namen des Verantwortlichen übernehmen, bestimmte personenbezogene Daten zur weisungsgebundenen Verwendung übertragen. Dies ist grundsätzlich eine Auftragsverarbeitung, die den Abschluss eines Verarbeitungsvertrags voraussetzt.

Frage: Ist die Zusammenarbeit mit Zahlungsdienstleistern (Billbee etc.) im Rahmen der Zahlungsabwicklung eine Datenverarbeitung im Auftrag?

Wahrscheinlich nicht. Problematisch ist, dass die DSGVO nicht mehr zwischen der bloßen Funktionsübertragung und der Auftragsverarbeitung differenziert. Die Grenzen sind nun fließend.

Nach bisher geltendem Datenschutzrecht war für eine Auftragsdatenverarbeitung erforderlich, dass sich die Tätigkeit des Auftragnehmers in einer reinen Hilfsfunktion für die Erfüllung der Zwecke und Aufgaben des Auftraggebers erschöpfte. Eine Hilfsfunktion schied aber dann aus, wenn ihm die Aufgabe, zu deren Erfüllung die Verarbeitung der Daten notwendig war, übertragen wurde. Dies galt als bloße Funktionsübertragung, die noch keinen Vertrag über eine Auftragsdatenverarbeitung erforderlich

machte.

Nach bisherigem Recht war die Einschaltung von Zahlungsdienstleistern eine solche Funktionsübertragung. Den Dienstleistern wird die Aufgabe der Zahlungsabwicklung zur eigenständigen Wahrnehmung selbst übertragen, ohne dass sie bloß Gehilfen des Händlers sind.

Ob hieran auch unter der DSGVO festgehalten werden kann, kann derzeit nicht abschließend beurteilt werden. Vieles spricht aber dafür, dass Zahlungsdienstleister auch fortan nicht als Auftragsverarbeiter anzusehen sein werden, weil sie über zu viel Eigenständigkeit verfügen.

Möglicherweise gelten sie und der Händler aber als „gemeinsame Verantwortliche“ (Art. 26 DSGVO), was ebenfalls eine Vereinbarung erforderlich machen würde.

Es bleibt zu hoffen, dass die Aufsichtsbehörden bzw. die Artikel-29-Gruppe sich hierzu künftig klarer positionieren werden

Frage: Ist die Weitergabe von Rechnungsunterlagen an einen Steuerberater eine Auftragsverarbeitung?

Nein. Hier herrscht Einigkeit. Rechnungsunterlagen enthalten zwar personenbezogene Kundendaten. Bei der Tätigkeit des Steuerberaters handelt es sich aber nicht um eine Unterstützungshandlung bei der Datenverarbeitung, sondern um eine eigenständige Dienstleistung mit steuerrechtlichem Ziel, die allenfalls punktuell mit Daten in Berührung kommt.

Autor:
RA Phil Salewski
Rechtsanwalt