Auftragsverarbeiter nach EU-Datenschutz-Grundverordnung - FAQ

Antworten auf die wichtigsten Fragen

1. Wer zählt zu den Auftragsverarbeitern?
2. Was ist der Unterschied zu Empfängern?
3. Worauf muss man achten falls man sich entscheidet dieses Thema out zu sourcen? Ist das überhaupt erlaubt oder möglich?
4. Unser Unternehmen wird evtl. die Stammkundendaten an einen externen Anbieter auslagern. Was ist hier zu beachten, wenn wir die bestehenden Daten "mitnehmen" möchten?
5. Als IT Unternehmen verarbeiten wir Daten für andere. Inwieweit müssen wir für unsere Kunden Prozesse protokollieren, Folgeabschätzungen machen? Können wir als Dienstleister davon ausgehen, dass Kunden auf uns aktiv zugehen und uns informieren was diese von uns benötigen?
6. Sind Online-Cloud Services (zB Dropbox, Google Drive) geeignet für die neue DSGVO? Ist ein Backup der Daten online auf Microsoft Onedrive oder Dropbox zum Beispiel erlaubt?
7. Darf eine Firma die Kontaktdatenbank zB im Office 365, also bei Microsoft speichern? Ist MS damit Auftragsverarbeiter oder "nur" Provider, brauchen wir eine spezielle DSGVO Vereinbarung bzw Bestätigung von Microsoft?
8. Es wurde immer wieder gesagt, man muss mit dem Dienstanbieter (dem Auftragsverarbeiter) einen Vertrag machen. Heißt das also, ich muss mit WhatsApp (Facebook), Google, Apple uvm einen Vertrag schließen, aus dem hervorgeht, was diese Firmen mit meinen Daten machen. Klingt logisch - nur wie sieht das in der Praxis aus?
9. Ist der IT-Betreuer automatisch Auftragsverarbeiter und muss er explizit vom Kunden beauftragt werden?
10. Wir nutzen für die Buchhaltung sowie die Fakturierung Cloud-Services von verschiedenen Anbietern - was ist hierfür konkret zu tun?
11. Wie geht man vor, wenn man zB die Lohnverrechnung extern erstellen lässt - müssen hier Vereinbarungen mit den Mitarbeitern oder dem Lohnverrechnungspartner erstellt werden, dass man die Daten übermitteln darf?
12. Ich nutze einen Dienst eines externen Anbieters, um Daten zu speichern, zB Apple "Kontakte". Diese Daten werden auch in einer Cloud gespeichert - ich habe darüber jedoch keine Info, was dieser Anbieter mit den Daten macht. Stellt das für mich ein Problem dar?
13. Muss ich irgendwas Neues beachten, wenn ich externe Anbieter (in meinem Fall Mailchimp) für die Speicherung von personenbezogenen Daten (Name, E-Mail, ggf GebDatum)?
14. Wir sind eine Software-Entwicklungsfirma und erstellen individuelle Kundenlösungen, keine Standardprodukte. Also Software-Lösungen auf Basis Lasten-/Pflichtenheft, welche wir von unseren Kunden vorgegeben bekommen. Was wenn hier Vorgabe von der DSGVO missachtet werden, zB keine Funktionen für Löschungen (sondern nur Löschmarkierungen, ohne tatsächlich zu löschen und Daten nur auszublenden) - sind wir als Software-Entwickler hier verantwortlich, dafür zu sorgen, dass auch bei unserem Kunden die DSGO einzuhalten sind und ggf. sogar später vom Kunden reklamiert werden könnten, dass wir diese Funktionen nicht bereitgestellt haben, obwohl sie im Lastenheft nicht gefordert waren?
15. Dass sich der Verantwortliche um persönliche und auch sensible Daten kümmern muss ist mir klar - inwiefern muss sich ein Auftragsverarbeiter um die persönlichen Daten eines Verantwortlichen kümmern? Beispiel: Unternehmen outsourcen deren gesamte IT-Infrastruktur in ein Rechenzentrum in OÖ welches von einem anderen Unternehmen betrieben wird.
16. Muss ich einen Auftragsverarbeitungsvertrag mit zB meinem E-Mail-Versand-Unternehmen (Newsletter) abschließen?
17. Was ist, wenn mein Lieferant mir nicht bestätigt, dass er sich an die neue Verordnung hält?
18. Ist es notwendig, meinem externen, vertraglich gebundenen EDV-Dienstleister eine Verschwiegenheitserklärung unterschreiben zu lassen? Wie würde hier eine Einbindung in den Datenschutz aussehen?
19. Wir verwenden überwiegend Datenspeicher von "den Großen". Ich gehe davon aus, dass die Daten auf Google Drive und Amazon (s3) zwar "sicher" abgespeichert sind, es jedoch an uns als Unternehmen liegt, Zugriffe auf relevanten Daten entsprechend zu verwalten.
20. Was müssen wir als Hersteller einer Kassensoftware beachten und worauf müssen wir unsere Kunden (Einzelhandel) hinweisen, wenn Sie unsere Kassensoftware benutzen und dort Kundendaten ("Stammkunden") verwaltet werden?
21. Dürfen Kundendaten wie Adresse, Telefonnummer, Mailadresse ohne Kundenzustimmung an den Paketdienstleister vom Händler der Waren mit diesem versendet weitergegeben werden?
22. Ist es überhaupt noch zulässig, Daten in der Cloud abzulegen, etwa, wenn man Adressbuchdienste von Google oder Apple nutzt (Adressbuch am Smartphone)? Das Risiko dieser Daten ist ja nicht abschätzbar.

23. Wie muss mit personenbezogenen Daten bei externen Dienstleistern umgegangen werden (z.B. SAAS z.B. SAP, CRM)? Wer hat eine Hol-/Bringschuld, wenn Personen von Kunden austreten und somit Daten evtl. zu löschen sind?
24. Wenn meine Kundendaten bei einem externen Anbieter auf einem Server oder Mailsystem gespeichert sind: Inwieweit bin ich für die Einhaltung der DSGVO bei auftretenden Problemen haftbar?
25. Ist die Bank, über die die Löhne der Angestellten überwiesen werden, ein Auftragsverarbeiter und muss mit dieser eine Vereinbarung getroffen werden?
26. Ist die GKK ein Auftragsverarbeiter und muss mit dieser eine Vereinbarung getroffen werden?
27. Ist aus datenschutzrechtlicher Sicht ein Kreditinstitut bei der Erbringung von Bankgeschäften im Verhältnis zu seinen Bankkunden Auftragsverarbeiter (laut Art 28 DSGVO)?
28. Muss für die Reparatur von PC/Laptop eines Kunden (auf dem personenbezogene Daten gespeichert sind) eine Art Auftragsverarbeitervertrag abgeschlossen werden?
29. Was muss man beachten, wenn man seine Newsletter über ein Programm wie zB Mailchimp versendet?
30. Website: Ist jeder selber verantwortlich, dass auf der Website die korrekten Daten stehen oder kann die Werbeagentur, die die Website erstellt hat auch belangt werden?
31. Was muss ich konkret tun, um weiterhin Evernote als meine digitale Ablage nach DSGVO nutzen zu können?
32. Wie ist das im Falle von Social Media Management. Wenn man für eine Firma/Brand Social Media Management als Externe betreibt und damit auch Nachrichten von Endkunden über Messenger erhält und diese bearbeitet. Wer muss die Zustimmung einholen? Die Brand oder ich als Externe?
33. Muss ein Auftragsverarbeiter mehrere Verarbeitungsverzeichnisse führen?
34. Darf ich Programme von Firmen nicht verwenden, wenn die Firma nicht im Privacy shield eingetragen ist und die DS Erklärung nicht den DSGVO Normen entspricht?
35. Wenn ich meine geschäftlichen Unterlagen in einer Cloud speichere, brauche ich hier eine Zustimmung meiner Kunden?
36. Sind Provider Auftragsverarbeiter?
37. Sind Handwerksbetriebe Auftragsverarbeiter?
38. Ich bekomme von Handwerksbetrieben plötzlich Auftragsverarbeiterverträge zum Unterschreiben geschickt. Sind das überhaupt Auftragsverarbeiter?
39. Sind Verkäufer, die eine Datenverarbeitungs-Software anbieten, Auftragsverarbeiter?
40. Sind Inkassounternehmen Auftragsverarbeiter?
41. Sind Telekommunikationsunternehmen Auftragsverarbeiter?

---

1. Wer zählt zu den Auftragsverarbeitern?

Auftragsverarbeiter sind die verlängerten Arme der Verantwortlichen. Dh sie verarbeiten weisungsgebunden und vertraglich gebunden Daten für jemand anderes. „Klassische" AV sind z.B. Clouddienste-Anbieter, Werbeadressenverarbeitung durch einen Newsletter-Tool Betreiber, Auslagerung der Backup-Sicherheitsspeicherung, Datenträgerentsorgung durch einen Dienstleister.

2. Was ist der Unterschied zu Empfängern?

Empfänger ist jeder vom Verantwortlichen und der betroffenen Person selbst unterschiedliche Person, dh jedem, den ich Daten außerhalb des Unternehmens, abgesehen von der betroffenen Person selbst, weitergebe. Auch Auftragsverarbeiter sind Empfänger. Mitarbeiter des Verantwortlichen gelten in der Regel nicht als Empfänger.

3. Worauf muss man achten falls man sich entscheidet dieses Thema out zu sourcen? Ist das überhaupt erlaubt oder möglich?

Jedem Unternehmen steht es frei, sich von externer Seite in Datenschutz-Angelegenheiten beraten zu lassen. Besteht eine Pflicht zur Bestellung eines Datenschutzbeauftragten, kann dies auch durch Bestellung einer unternehmensfremden Person geschehen (z.B. Anwälte, Unternehmensberater, IT-Dienstleister,...).

Allerdings sollte beachtet werden, dass (je nach Branche und Intensität der Datenverarbeitung) jeder Mitarbeiter über bestimmte Kenntnisse im Datenschutz verfügen muss (insbesondere beim Thema Datensicherheit sind die Mitarbeiter unbedingt zu schulen, vgl IT-Sicherheitshandbuch für Mitarbeiter). Ein gänzliches „Outsourcing" des Themas Datenschutz ist damit nicht möglich. Auch die Verantwortung kann man als Unternehmen nicht gänzlich outsourcen.

4. Unser Unternehmen wird evtl. die Stammkundendaten an einen externen Anbieter auslagern. Was ist hier zu beachten, wenn wir die bestehenden Daten "mitnehmen" möchten?

Zunächst sollte geprüft werden, ob die bestehende Datenverarbeitung überhaupt rechtskonform ist. Eine Auslagerung im Sinne von Outsourcing ist grundsätzlich möglich. Der Verantwortliche darf jedoch nur solche Auftragsverarbeiter („Dienstleister") beauftragen, die eine datenschutzkonforme Verarbeitung gewährleisten. Zwischen Verantwortlichem und Auftragsverarbeiter ist eine Vereinbarung abzuschließen, die einen bestimmten Mindestinhalt aufweisen muss. Ein Muster dafür finden Sie z.B. hier.

5. Als IT Unternehmen verarbeiten wir Daten für andere. Inwieweit müssen wir für unsere Kunden Prozesse protokollieren, Folgeabschätzungen machen? Können wir als Dienstleister davon ausgehen, dass Kunden auf uns aktiv zugehen und uns informieren was diese von uns benötigen?

Die DSGVO definiert eine Reihe von Pflichten des Auftragsverarbeiters – primär muss ein Vertrag geschlossen werden (Muster finden Sie hier). Sie können und sollten sich nicht darauf verlassen, dass Kunden aktiv auf Sie zugehen, Sie müssen das selbst veranlassen. Weiters treffen Sie als Dienstleister auch andere Pflichten, wie z.B. Sicherheitsmaßnahmen implementieren, Risiken einschätzen, aber auch den Verantwortlichen/ Kunden bei seinen Pflichten gegenüber Betroffenen und bei der Datenschutz-Folgeabschätzung unterstützen, bzw für diesen eine „abgespecktere" Version des Verarbeitungsverzeichnisses über die Verarbeitungstätigkeiten für den Verantwortlichen/ Kunden erstellen. Wie diese Unterstützung konkret aussieht, sollten Sie bestenfalls vertraglich regeln.

Ein Muster für diese Form des Verarbeitungsverzeichnisses finden Sie online.

6. Sind Online-Cloud Services (z.B. Dropbox, Google Drive) geeignet für die neue DSGVO? Ist ein Backup der Daten online auf Microsoft Onedrive oder Dropbox zum Beispiel erlaubt?

Aufgrund der ständigen Änderungen von Nutzungsbedingungen und datenschutzrelevanten Vorgaben insbesondere bei großen Anbietern ist es uns leider nicht möglich, eine allgemein gültige Aussage zu treffen. Jedenfalls gilt: Die Nutzung „kostenloser" Dienste für Unternehmensinformationen sollte immer im Einzelfall geprüft werden. Unbedingt sollte auch geprüft werden, ob ein derartiger kostenloser Dienst auch geschäftliche genutzt werden kann oder nur privat. Sie müssen sich die Frage stellen, ob ein Unternehmen diesen Diensten seine (allenfalls nicht-personenbezogenen) Geschäfts- und Betriebsgeheimnisse anvertrauen können. Clouddienstleistungen wurden durch die DSGVO nicht verboten. Sie sollten allerdings bedenken, dass es sich bei dieser Dienstleistung um eine Auftragsverarbeitung handelt, dh es ist 1. ein schriftlicher Auftragsverarbeitervertrag zu schließen (Muster finden Sie hier), 2. auf die Zuverlässigkeit des Anbieters zu achten, 3. Datensicherheitsmaßnahmen einzuhalten, 4. betroffene Personen darüber aufzuklären, 5. darauf zu achten, wo Daten gespeichert werden (EU oder EU-Ausland). Die Weitergabe von Daten an einen Auftragsverarbeiter innerhalb der EU ist grundsätzlich unproblematisch. Außerhalb der EU wären die Grundsätze des internationalen Datenverkehrs einzuhalten: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr (z.B. ausdrückliche Einwilligung, Angemessenheitsentscheidung,...).

7. Darf eine Firma die Kontaktdatenbank z.B. im Office 365, also bei Microsoft speichern? Ist MS damit Auftragsverarbeiter oder "nur" Provider, brauchen wir eine spezielle DSGVO Vereinbarung bzw. Bestätigung von Microsoft?

Aufgrund der ständigen Änderungen von Nutzungsbedingungen und datenschutzrelevanten Vorgaben insbesondere bei großen Anbietern ist es uns leider nicht möglich, eine allgemein gültige Aussage zu treffen. Jedenfalls gilt: Provider können auch Auftragsverarbeiter sein, wenn diese personenbezogenen Daten für ihren Kunden verarbeiten (z.B. darauf Zugriff nehmen, Speicherung anbieten, etc).

Bei Office 365 handelt es sich um eine cloudbasierte Office-Lösung, Microsoft ist hier als Auftragsverarbeiter zu werten. Microsoft informiert auf seiner Website zu diesem Thema und weist auch aus, dass die Auftragsverarbeiterverträge innerhalb der Volumenlizenzverträge in den Online Services-Nutzungsbedingungen enthalten sind. Ein elektronischer Abschluss eines solchen Vertrages reicht nach derzeitigem Stand aus. Weiters wurden Schritte gesetzt um die Datenweitergabe ins EU-Ausland abzusichern (Standardvertragsklauseln, Eintragung in der EU-US Privacy Shield List).

8. Es wurde immer wieder gesagt, man muss mit dem Dienstanbieter (dem Auftragsverarbeiter) einen Vertrag machen. Heißt das also, ich muss mit WhatsApp (Facebook), Google, Apple uvm einen Vertrag schließen, aus dem hervorgeht, was diese Firmen mit meinen Daten machen. Klingt logisch - nur wie sieht das in der Praxis aus?

Vielen US-amerikanischen Anbietern ist dieses Problem mittlerweile bewusst, und sie haben entsprechende Verfahren entwickelt. Hier die Beispiele von Microsoft und Amazon. In der Praxis sieht es meist so aus, dass Ihre Nutzungsverträge (-bedingungen) mit den jeweiligen Anbietern upgedatet werden und Sie diese elektronisch akzeptieren müssen. Nach derzeitigem Stand reicht dieses Verfahren aus. Es muss jedenfalls geprüft werden, ob der Dienst, den Sie konkret verwenden, zu geschäftlichen Zwecken genutzt werden darf (z.B. bei kostenlosen Modellen ist die Nutzung oft auf privat eingeschränkt).

9. Ist der IT-Betreuer automatisch Auftragsverarbeiter und muss er explizit vom Kunden beauftragt werden?

Wenn der IT-Betreuer ein externes Unternehmen ist und Ihre personenbezogenen Daten verarbeitet (Wartung, Support,...), dann ja. Er muss von Ihnen als Verantwortlicher beauftragt werden (Vertrag nicht vergessen, Muster).

Beispiel IT-Dienstleistungen vor Ort an Endgeräten des Verantwortlichen: Maßgeblich ist, ob eine beauftragte Tätigkeit „im Zusammenhang mit personenbezogenen Daten" steht oder nicht. Keine Verarbeitung liegt vor, wenn bloß eine theoretische Möglichkeit zum Zugriff auf Daten besteht und der Zugriff auch vertraglich ausgeschlossen wurde. Keine Auftragsverarbeitung besteht insbesondere dann, wenn Auftragsgegenstand bloß die Erhaltung und Weiterentwicklung von Funktionalitäten von Anwendungen ist, ohne dass dafür die Verarbeitung von personenbezogenen Daten erforderlich ist oder damit einhergeht. Gleiches gilt auch bei IT-Dienstleistungen mittels Fernwartung (Remote Support, Screen Sharing, etc).

10. Wir nutzen für die Buchhaltung sowie die Fakturierung Cloud-Services von verschiedenen Anbietern - was ist hierfür konkret zu tun?

Clouddienstleistungen wurden durch die DSGVO nicht verboten. Sie sollten allerdings bedenken, dass es sich bei dieser Dienstleistung um eine Auftragsverarbeitung handelt, dh es ist 1. ein schriftlicher Auftragsverarbeitervertrag zu schließen (Muster finden Sie hier), 2. auf die Zuverlässigkeit des Anbieters zu achten, 3. Datensicherheitsmaßnahmen einzuhalten, 4. betroffene Personen darüber aufzuklären, 5. darauf zu achten, wo Daten gespeichert werden (EU oder EU-Ausland). Die Weitergabe von Daten an einen Auftragsverarbeiter innerhalb der EU ist grundsätzlich unproblematisch. Außerhalb der EU wären die Grundsätze des internationalen Datenverkehrs einzuhalten: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr (z.B. ausdrückliche Einwilligung, Angemessenheitsentscheidung,...).

11. Wie geht man vor, wenn man z.B. die Lohnverrechnung extern erstellen lässt - müssen hier Vereinbarungen mit den Mitarbeitern oder dem Lohnverrechnungspartner erstellt werden, dass man die Daten übermitteln darf?

Mit den Mitarbeitern müssen Sie keine Vereinbarungen schließen, da die Weitergabe der Daten der Mitarbeiter durch die Vereinbarung mit dem Partner abgedeckt ist, welcher für Sie die Lohnverrechnung durchführt. Allerdings sind die Mitarbeiter im Rahmen der Datenschutzerklärung über die externe Lohnverrechnung zu informieren (Muster finden Sie hier).

12. Ich nutze einen Dienst eines externen Anbieters, um Daten zu speichern, z.B. Apple "Kontakte". Diese Daten werden auch in einer Cloud gespeichert - ich habe darüber jedoch keine Info, was dieser Anbieter mit den Daten macht. Stellt das für mich ein Problem dar?

Diverse US-amerikanische IT-Anbieter haben sich bereits auf die DSGVO vorbereitet. Apple hat (Stand 14. Mai 2018) bereits diesbezügliche Informationen auf der Website veröffentlicht, hat nun allerdings ausgewiesen, dass die Nutzung der iCloud nur für private Zwecke vereinbart wird (Stand 12. Juli 2018, Nutzungsbedingungen der iCloud: „Außerdem stimmst du zu, dass der Dienst nur für den privaten Gebrauch bestimmt ist (...)".) Das bedeutet, dass dieser Dienst für die betriebliche Verwendung nicht gedacht ist und daher auch keine der DSGVO entsprechende Vereinbarung abgeschlossen werden wird. Es sollte daher eine andere (Cloud-)Lösung für den Betrieb gefunden werden. Da Sie die Verantwortung trifft, sich „zuverlässigen" Anbietern/ Auftragsverarbeitern zu bedienen, ist es immer sinnvoll, die Nutzungs- und Datenschutzbedingungen der jeweiligen Dienste zu überprüfen.

Die wichtigsten Punkte sind hierbei nochmals:

1. Auftragsverarbeitervertrag (Muster finden Sie hier),
2. Zuverlässigkeit des Anbieters,
3. Datensicherheitsmaßnahmen,
4. Information an betroffene Personen, dass Sie Daten an Clouddiensteanbieter weitergeben,
5. Speicherort der Daten (-weitergabe) überprüfen (EU oder EU-Ausland). Die Weitergabe von Daten an einen Auftragsverarbeiter innerhalb der EU ist grundsätzlich unproblematisch. Außerhalb der EU wären die Grundsätze des internationalen Datenverkehrs einzuhalten: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr

13. Muss ich irgendwas Neues beachten, wenn ich externe Anbieter (in meinem Fall Mailchimp) für die Speicherung von personenbezogenen Daten (Name, E-Mail, ggf GebDatum)?

Sie müssen eine DSGVO-konforme Vereinbarung mit Ihren Auftragsverarbeitern abschließen(Muster finden Sie hier). Es ist zu beachten:

1. Auftragsverarbeitervertrag (Muster finden Sie hier),
2. Zuverlässigkeit des Anbieters,
3. Datensicherheitsmaßnahmen,
4. Information an betroffene Personen, dass Sie Daten an Clouddiensteanbieter weitergeben,
5. Speicherort der Daten (-weitergabe) überprüfen (EU oder EU-Ausland). Die Weitergabe von Daten an einen Auftragsverarbeiter innerhalb der EU ist grundsätzlich unproblematisch. Außerhalb der EU wären die Grundsätze des internationalen Datenverkehrs einzuhalten: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr

14. Wir sind eine Software-Entwicklungsfirma und erstellen individuelle Kundenlösungen, keine Standardprodukte. Also Software-Lösungen auf Basis Lasten-/Pflichtenheft, welche wir von unseren Kunden vorgegeben bekommen. Was wenn hier Vorgabe von der DSGVO missachtet werden, z.B. keine Funktionen für Löschungen (sondern nur Löschmarkierungen, ohne tatsächlich zu löschen und Daten nur auszublenden) - sind wir als Software-Entwickler hier verantwortlich, dafür zu sorgen, dass auch bei unserem Kunden die DSGO einzuhalten sind und ggf. sogar später vom Kunden reklamiert werden könnten, dass wir diese Funktionen nicht bereitgestellt haben, obwohl sie im Lastenheft nicht gefordert waren?

Als professioneller Anbieter in diesem Segment könnte Sie nach österreichischem Recht eine Warnpflicht treffen. Eine entsprechende schriftliche Aufklärung des Kunden, z.B. dass ein Löschungskonzept notwendig ist, wäre daher jedenfalls empfehlenswert.

15. Dass sich der Verantwortliche um persönliche und auch sensible Daten kümmern muss ist mir klar - inwiefern muss sich ein Auftragsverarbeiter um die persönlichen Daten eines Verantwortlichen kümmern? Beispiel: Unternehmen outsourcen deren gesamte IT-Infrastruktur in ein Rechenzentrum in OÖ welches von einem anderen Unternehmen betrieben wird.

Zwischen Verantwortlichem und Auftragsverarbeiter muss eine DSGVO-konforme Vereinbarung abgeschlossen werden, die auch alle Pflichten des Auftragsverarbeiters enthält (Muster finden Sie hier). Wenn Sie Daten für Ihren Kunden/ den Verantwortlichen verarbeiten, müssen Sie sich auch „kümmern", dh Sicherheitsmaßnahmen einhalten, Risiken analysieren etc.

16. Muss ich einen Auftragsverarbeitungsvertrag mit zB meinem E-Mail-Versand-Unternehmen (Newsletter) abschließen?

Ja, wenn Sie dem Unternehmen E-Mail-Adressen und/oder andere personenbezogene Daten Ihrer Kunden überlassen (Muster finden Sie hier).

17. Was ist, wenn mein Lieferant mir nicht bestätigt, dass er sich an die neue Verordnung hält?

Zunächst ist zu prüfen, was mit Lieferant gemeint ist, bzw ob der Lieferant/ Vertragspartner in einer Art und Weise Daten für Sie verarbeitet, die einer Auftragsverarbeitung entsprechen (= Daten werden im Auftrag eines Verantwortlichen, auf dessen Weisung, Entscheidung etc hin verarbeitet und das nicht nur als Nebenaspekt des eigentlichen Auftrags). Verweigert jemand, der Ihr Auftragsverarbeiter ist, den Abschluss eines Auftragsverarbeitervertrags, verstößt eine weitere Zusammenarbeit gegen die DSGVO. Dh Sie sollten sich in diesem Fall jemand anderes suchen.

18. Ist es notwendig, meinem externen, vertraglich gebundenen EDV-Dienstleister eine Verschwiegenheitserklärung unterschreiben zu lassen? Wie würde hier eine Einbindung in den Datenschutz aussehen?

Ein Muster mit dem Mindestinhalt eines Auftragsverarbeitervertrags finden Sie hier.

19. Wir verwenden überwiegend Datenspeicher von "den Großen". Ich gehe davon aus, dass die Daten auf Google Drive und Amazon (s3) zwar "sicher" abgespeichert sind, es jedoch an uns als Unternehmen liegt, Zugriffe auf relevanten Daten entsprechend zu verwalten.

Die Nutzung „kostenloser" Dienste für Unternehmensinformationen sollte immer im Einzelfall geprüft werden, insb auch, ob die Nutzung zu geschäftlichen Zwecken durch den Anbieter erlaubt wird. Sie müssen sich die Frage stellen, ob ein Unternehmen diesen Diensten seine (allenfalls nicht-personenbezogenen) Geschäfts- und Betriebsgeheimnisse anvertrauen können. Clouddienstleistungen wurden durch die DSGVO nicht verboten. Sie sollten allerdings bedenken, dass es sich bei dieser Dienstleistung um eine Auftragsverarbeitung handelt, dh es ist 1. ein schriftlicher Auftragsverarbeitervertrag zu schließen (Muster finden Sie hier), 2. auf die Zuverlässigkeit des Anbieters zu achten, 3. Datensicherheitsmaßnahmen einzuhalten, 4. betroffene Personen darüber aufzuklären, 5. darauf zu achten, wo Daten gespeichert werden (EU oder EU-Ausland). Die Weitergabe von Daten an einen Auftragsverarbeiter innerhalb der EU ist grundsätzlich unproblematisch. Außerhalb der EU wären die Grundsätze des internationalen Datenverkehrs einzuhalten: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr (z.B. ausdrückliche Einwilligung, Angemessenheitsentscheidung,...). Diverse US-amerikanische IT-Anbieter haben sich bereits auf die DSGVO vorbereitet (hier an den Beispielen Microsoft und Amazon oder auch Google.

20. Was müssen wir als Hersteller einer Kassensoftware beachten und worauf müssen wir unsere Kunden (Einzelhandel) hinweisen, wenn Sie unsere Kassensoftware benutzen und dort Kundendaten ("Stammkunden") verwaltet werden?

Kassensoftware ist eigentlich nicht darauf ausgerichtet, personenbezogene Daten zu verarbeiten. Wird dies angeboten, sollte die Software in der Lage sein, die Vorgaben der DSGVO umsetzen zu können. Wie der Kunde die Software konkret einsetzt, liegt nicht mehr in der Verantwortung des Herstellers.

21. Dürfen Kundendaten wie Adresse, Telefonnummer, Mailadresse ohne Kundenzustimmung an den Paketdienstleister vom Händler der Waren mit diesem versendet weitergegeben werden?

Ein Zusteller ist ein zivilrechtlicher Erfüllungsgehilfe (= er macht das in Ihrem Auftrag), die Datenverarbeitung (Name und Adresse des Empfängers) ist nur ein Nebenaspekt der eigentlichen Tätigkeit (= Zustellung), weshalb im Regelfall von keinem Auftragsverarbeitungsverhältnis ausgegangen wird. Die Weitergabe der Daten an den Zusteller sind im Rahmen der Vertragserfüllung möglich und muss keine zusätzliche Einwilligung eingeholt werden. Informationspflichten werden vom Zusteller wohl nicht erforderlich sein, da dies als unverhältnismäßiger Aufwand eingeordnet werden kann.

22. Ist es überhaupt noch zulässig, Daten in der Cloud abzulegen, etwa, wenn man Adressbuchdienste von Google oder Apple nutzt (Adressbuch am Smartphone)? Das Risiko dieser Daten ist ja nicht abschätzbar.

Ja, Sie dürfen nach wie vor Daten auch in Clouds ablegen. Wie bisher (!) gilt aber auch hier, dass Sie „sicherer Clouds" verwenden sollten, dh sich Fragen stellen sollten, ob die Daten sicher sind, ob der Anbieter Sicherheitsmaßnahmen anbietet, ob Daten weitergegeben werden (z.B. außerhalb der EU), wer auf Daten zugreifen kann. Manche Anbieter werben z.B. mit Gütesiegeln oder Zertifizierungen, dh man kann ein gewisses Vertrauen in diese Anbieter setzen. Viele der angesprochenen IT-Anbieter haben sich außerdem bereits auf die DSGVO vorbereitet (hier an den Beispielen Microsoft und Amazon oder auch Google. Sie müssen allerdings jedenfalls prüfen, ob der Cloud-Dienst auch zu betrieblichen Zwecken verwendet werden kann und ob ein Auftragsverarbeitervertrag (Muster) abgeschlossen wird. Wenn diese Fragen mit nein beantwortet werden, muss für die betriebliche Nutzung ein anderer Dienst gewählt werden (vgl auch Frage 12).

23. Wie muss mit personenbezogenen Daten bei externen Dienstleistern umgegangen werden (z.B. SAAS z.B. SAP, CRM)? Wer hat eine Hol-/ Bringschuld, wenn Personen von Kunden austreten und somit Daten evtl. zu löschen sind?

Die Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter hat zwingend eine Regelung zu enthalten, was nach Ende der Dienstleistung mit den Daten zu geschehen hat.

24. Wenn meine Kundendaten bei einem externen Anbieter auf einem Server oder Mailsystem gespeichert sind: Inwieweit bin ich für die Einhaltung der DSGVO bei auftretenden Problemen haftbar?

Auch für das Datenschutzrecht gilt das Verschuldensprinzip. Trifft den Verantwortlichen daher gar kein Verschulden an der rechtswidrigen Datenverarbeitung durch einen anderen, kann er auch nicht haftbar gemacht werden. Der Verantwortliche darf jedoch nur solche Auftragsverarbeiter beauftragen, die eine datenschutzkonforme Verarbeitung gewährleisten. Zivilrechtlich gesehen (nicht die Strafen nach der DSGVO!) könnten evtl die Regeln der Gehilfenhaftung greifen, dh man könnte mitunter schadenersatzpflichtig werden, wenn bei der Erfüllung eines Vertrages ein Schaden entsteht.

25. Ist die Bank, über die die Löhne der Angestellten überwiesen werden, ein Auftragsverarbeiter und muss mit dieser eine Vereinbarung getroffen werden?

Alle Datenübermittlungen sind im Einzelfall zu prüfen, ob es sich um Datenweitergaben an Auftragsverarbeiter oder Verantwortliche handelt. Die Bank der Mitarbeiter ist in diesem Fall nicht als Auftragsverarbeiter zu qualifizieren, wenn Sie hier nur das vereinbarte Gehalt auf das vom Mitarbeiter bekannt gegebene Konto überweisen.

26. Ist die GKK ein Auftragsverarbeiter und muss mit dieser eine Vereinbarung getroffen werden?

Die Gebietskrankenkassen sind Verantwortliche, weil sie die Daten nicht im Auftrag des Arbeitgebers verarbeiten, sondern zu eigenen Zwecken, wofür die entsprechenden Rechtsgrundlagen existieren. Das gilt in gleicher Weise ab 1.1.2020 für die Österreichische Gesundheitskasse.

27. Ist aus datenschutzrechtlicher Sicht ein Kreditinstitut bei der Erbringung von Bankgeschäften im Verhältnis zu seinen Bankkunden Auftragsverarbeiter (laut Art 28 DSGVO)?

Bankgeschäfte iSd § 1 Bankwesengesetz (BWG), die Kreditinstitute aufgrund ihrer Konzession erbringen (zB Girogeschäft, Einlagengeschäft, Zahlungsverkehr, etc.) sind keine Auftragsverarbeitungen iSd des Artikel 28 Datenschutzgrundverordnung (DSGVO). Dafür sind die Kreditinstitute selbst als Verantwortliche tätig. Es muss daher kein Vertrag über eine Auftragsverarbeitung abgeschlossen werden.

28. Muss für die Reparatur von PC/Laptop eines Kunden (auf dem personenbezogene Daten gespeichert sind) eine Art Auftragsverarbeitervertrag abgeschlossen werden?

Wenn Sie Zugriff im Zuge dieser Reparaturarbeit auf die Daten nehmen und es sich nicht um eine reine Hardware Angelegenheit handelt, dann ja.

29. Was muss man beachten, wenn man seine Newsletter über ein Programm wie zB Mailchimp versendet?

Der jeweilige Anbieter ist Ihr Auftragsverarbeiter, dh Sie müssen einen Auftragsverarbeitervertrag (EU-Datenschutz-Grundverordnung (DSGVO): Mustervertrag für die Auftragsverarbeitung) abschließen. Ansonsten sollten Sie beachten, dass Daten nicht außerhalb der EU übermittelt werden bzw wenn das passiert, dann zumindest in einen sicheren Drittstaat (EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr).

30. Website: Ist jeder selber verantwortlich, dass auf der Website die korrekten Daten stehen oder kann die Werbeagentur, die die Website erstellt hat auch belangt werden?

Wenn damit die Datenschutzerklärung gemeint war, dann ist grundsätzlich der Unternehmer, der Daten über die Website verarbeitet, dafür selbst verantwortlich. Wenn Sie als Agentur eine Website für den Kunden erstellen, sollte Sie aber im Rahmen Ihrer Warnpflicht als Auftragsverarbeiter schriftlich hinweisen, dass eine DSGVO-konforme DS-Erklärung erstellt werden sollte, über Cookies informiert werden sollte, etc.

31. Was muss ich konkret tun, um weiterhin Evernote als meine digitale Ablage nach DSGVO nutzen zu können?

Evernote arbeitet unseres Wissens auch cloudbasiert. Externe Dienstleister, die man zur Datenverarbeitung heranzieht, nennt man Auftragsverarbeiter. Die DSGVO definiert eine Reihe von Pflichten des Auftragsverarbeiters – primär muss ein Vertrag geschlossen werden (Muster finden Sie hier). Weiters treffen den Dienstleister auch andere Pflichten, wie z.B. Sicherheitsmaßnahmen implementieren, Risiken einschätzen, aber auch den Verantwortlichen/ Kunden bei seinen Pflichten gegenüber Betroffenen und bei der Datenschutz-Folgeabschätzung unterstützen, bzw für diesen eine „abgespecktere" Version des Verarbeitungsverzeichnisses über die Verarbeitungstätigkeiten für den Verantwortlichen/ Kunden erstellen. Wie diese Unterstützung konkret aussieht, sollten bestenfalls vertraglich geregelt werden. Ein Muster für diese Form des Verarbeitungsverzeichnisses finden Sie online.

32. Wie ist das im Falle von Social Media Management. Wenn man für eine Firma/Brand Social Media Management als Externe betreibt und damit auch Nachrichten von Endkunden über Messenger erhält und diese bearbeitet. Wer muss die Zustimmung einholen? Die Brand oder ich als Externe?

Wenn Sie als Auftragsverarbeiter für Ihren Kunden tätig sind, selber also keine Entscheidung über die Zwecke und Mittel der Datenverarbeitung treffen und die Anfragen nur im Sinne des Kunden beantworten, ist dafür der Kunde selbst (die Brand) zuständig.

33. Muss ein Auftragsverarbeiter mehrere Verarbeitungsverzeichnisse führen?

Ja. Sie sind als Auftragsverarbeiter in einer Doppelposition, Sie sind einerseits Verantwortlicher für das eigene Unternehmen und die „eigenen Daten" (Mitarbeiterdaten, Lieferanten, Vertragspartner) und andererseits Auftragsverarbeiter für die Daten, die Sie im Auftrag Ihrer Kunden verarbeiten. Sie müssen daher einerseits für sich selbst als Unternehmen und Verantwortlicher und andererseits für Ihre Kunden und als Auftragsverarbeiter Verzeichnisse führen. Das Verarbeitungsverzeichnis für Auftragsverarbeiter ist aber etwas kürzer, da die Vollversion nach wie vor der Verantwortliche hat. Muster finden Sie hier: EU-Datenschutz-Grundverordnung (DSGVO): Muster-Verarbeitungsverzeichnis für Auftragsverarbeiter.

34. Darf ich Programme von Firmen nicht verwenden, wenn die Firma nicht im Privacy shield eingetragen ist und die DS Erklärung nicht den DSGVO Normen entspricht?

Wenn sie hier nicht nur deren Produkte verwenden, sondern auch Daten an diese Unternehmen weitergeben und Sie das dezidiert wissen, dann nein.

35. Wenn ich meine geschäftlichen Unterlagen in einer Cloud speichere, brauche ich hier eine Zustimmung meiner Kunden?

Das bloße Abspeichern in der Cloud ist noch kein Problem, da der Clouddiensteanbieter als Ihr Auftragsverarbeiter auftritt und aufgrund dieser vertraglichen Bindung keine selbstständige Grundlage für die Weitergabe an diesen notwendig ist. Wenn aber die Daten zB außerhalb Europas gespeichert werden und in keinen sicheren Drittstaat übermittelt werden, dann kann es sein, dass Sie die Zustimmung brauchen (vgl EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr).

36. Sind Provider Auftragsverarbeiter?

Provider können auch Auftragsverarbeiter sein, wenn diese personenbezogenen Daten für ihren Kunden verarbeiten (zB darauf Zugriff nehmen, Speicherung anbieten, etc).

Access-Providern: Die reine Datendurchleitung entspricht im Üblichen keiner Datenverarbeitung ist. Manche Juristen vertreten eine solche aufgrund der Zwischenspeicherung beim Durchleiten, was allerdings strittig ist.

Host-Providern: Wenn eine Datenspeicherung angeboten wird (= Verarbeitung), dann liegt ein Auftragsverarbeitungsverhältnis vor. Wenn lediglich die bloße Hardware vermietet wird („leere 4 Wände", „Rechenzentrumsmiete") liegt keine Auftragsverarbeitung vor.

Cloud-Dienstleister: Das Anbieten der Speicherung und Datensicherheitsmaßnahmen lässt einen Auftragsverarbeitungsvertrag notwendig machen.

Mailprovider: Ähnlich wie Host-Provider sind diese als Auftragsverarbeiter zu qualifizieren, da die Speicherung und der Zugang angeboten wird.

37. Sind Handwerksbetriebe Auftragsverarbeiter?

Ein datenschutzrechtliches Auftragsverarbeiterverhältnis ist nicht mit einem zivilrechtlichen Auftrag gleichzusetzen, z.B. erhält ein Handwerksbetrieb von der Hausverwaltung personenbezogene Daten wie Name und Adresse der Wohnungsmieter, um eine Reparatur in deren Wohnung durchführen zu können, liegt zwar zivilrechtlich ein Werkvertrag vor, datenschutzrechtlich ist das allerdings nicht als Auftragsverarbeitung zu werten. Die personenbezogenen Daten werden in diesem Fall nur weitergeben um den eigentlichen Auftrag (= Reparatur in der Wohnung) durchführen zu können. Die Datenverarbeitung ist hier nur als Nebenaspekt zu sehen. Der Handwerksbetrieb ist daher kein Auftragsverarbeiter.

Die Datenverarbeitung durch einen Auftragsverarbeiter muss im Interesse des Verantwortlichen erfolgen, dh der Auftragsverarbeiter ist als „verlängerter Arm" des „Herrn der Daten" (= Verantwortlicher) zu sehen.

38. Ich bekomme von Handwerksbetrieben plötzlich Auftragsverarbeiterverträge zum Unterschreiben geschickt. Sind das überhaupt Auftragsverarbeiter?

Wenn Sie zivilrechtliche Aufträge (z.B. Werkvertrag) an andere Unternehmen erteilen, sind diese nicht automatisch datenschutzrechtliche Auftragsverarbeiter

39. Sind Verkäufer, die eine Datenverarbeitungs-Software anbieten, Auftragsverarbeiter?

Der Verkauf einer Datenverarbeitungsanlage (z.B. Software) ist datenschutzrechtlich nicht als Auftragsverarbeitung zu qualifizieren.

Wird aber eine Datenwartung bzw ein Support zum Verkauf der Software vereinbart, kann in diesem Fall eine Auftragsverarbeitung vorliegen, wenn der Support-Anbieter auf die Daten Zugriff nehmen kann.

40. Sind Inkassounternehmen Auftragsverarbeiter?

Das Inkassoinstitut ist ab Fallübergabe üblicherweise selbst verantwortlich für die Datenverarbeitung, da grundsätzlich selbst über Zwecke und Mittel der Datenverarbeitung entschieden wird (z.B. wann, wie werden Mahnungen geschrieben, Spesen verrechnet, usw).

41. Sind Telekommunikationsunternehmen Auftragsverarbeiter?

Telekom-Unternehmen sind wie Access Provider idR keine Auftragsverarbeiter.

Stand: 11.10.2019