Verarbeitungsverzeichnis nach der EU-Datenschutz-Grundverordnung - FAQ

Antworten auf die wichtigsten Fragen

1. Wie soll so ein Verarbeitungsverzeichnis genau ausschauen, und was gehört da genau eingetragen?
2. Brauche ich nur ein Verarbeitungsverzeichnis? Oder sonst auch noch andere schriftliche Unterlagen/Nachweise?
3. Das Verzeichnis müssen wir wohl auch nur für "unsere" Daten führen, nicht für die Daten die im Rahmen unserer Dienstleistungen für unsere Kunden erhoben werden (z.B. Webshops)?
4. Müssen Aktivitäten, also zum Beispiel Newsletter nr, xy am xy usw, aufgezeichnet werden.
5. Im Rahmen von Hacker-Abwehr werden von Servern IP Adressen gespeichert (z.B. um bei DDOS-Attacken diese sperren zu können). Inwieweit fallen diese Daten unter die notwendige Protokollierung?
6. Eine Ausnahme von der Verzeichnisführung besteht, wenn "die Verarbeitung nur gelegentlich erfolgt". Was ist "gelegentlich"?
7. Bitte um Beispiele wann Unternehmen unter 250 Mitarbeiter kein Verzeichnis für Verarbeitungstätigkeiten anlegen müssen (wenn kein Risiko für Rechte und Freiheiten der betroffenen Personen durch Datenverarbeitung besteht), was heißt das zum Beispiel?
8. Kann oder soll man die IT Dokumentation in die Dokumentation aufnehmen?
9. Wie protokolliert man alle Daten? Wir haben 4 Ordner allein mit Zulassungsscheine, wo überall Adressen usw. drinnen stehen?
10. Welche Software oder Tools gibt es die man zur Aufzeichnung nutzen kann?
11. Muss ich als Personaler jeden Bewerber in das Verzeichnis schreiben?
12. Muss man in diesem Verarbeitungsverzeichnis auch zB den Ordner anführen, in dem die Rechnung von dem Kunden aufbewahrt wird mit Name Adresse etc.?
13. Darf ich fragen, ob ich als Auftragsverarbeiter diesen Prozess ebenfalls in meinem Unternehmen dokumentieren muss oder ob dies durch die Dokumentation im datenverarbeitenden Unternehmen erledigt ist?
14. Warum muss ich ein Verzeichnis führen obwohl ich nur 5 Mitarbeiter habe und kein Risiko birgt. Siehe Artikel 30 Verzeichnis von Verarbeitungstätigkeiten Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.
15. Müssen in einem EPU beide Verarbeitungsverzeichnisse (für Verantwortliche + Auftragsverarbeiter) von derselben Person geführt werden?
16. Wir haben drei Firmen unter einem Dach mit einer gemeinsamen IT-Infrastruktur. Kann man das Datenanwendungsverzeichnis für alle drei Firmen gemeinsam erstellen?
17. Aus meiner Datenbank generiere ich eine Excelliste mit personenbezogenen Daten, um z.B. einen oder mehrere Gesichtspunkte genauer zu analysieren. Was muss ich aus datenschutzrechtlicher Sicht bzgl. dieser Excel Datei tun/dokumentieren?
18. Wir haben keine Kunden, bei denen personenbezogene Daten verarbeitet werden (ausschließlich Unternehmen als Kunden). Die einzigen personenbezogenen Daten sind die der Mitarbeiter. Müssen wir auch ein Verarbeitungsverzeichnis erstellen?
19. Wie oft muss das Verarbeitungsverzeichnis aktualisiert werden oder nur muss es nur einmal erstellt werden?
20. Wir verwenden Im Betrieb u.a. einen Outlooksystem, welches Kundendaten (Name, Tel, Anschrift) automatisch auf Handys synchronisiert, dh diese Situation dokumentiere ich im Verarbeitungsverzeichnis?
21. Muss ich jedes Mal wenn ich ein Mail mit Kundendaten weiterleite ein Protokoll darüber verfassen? Oder nur einmal, dass ich sowas tue?
22. Muss man jede Verwendung von Daten, wenn diese Verwendet werden aufzeichnen? Wenn ja, wie?
23. Wie ist Dokumentationspflicht im Verarbeitungsverzeichnis in Bezug auf elektronisch erfasste Dokumente (Geschäftsbriefe, Protokolle, etc.), die Texte und Daten beliebiger Art enthalten können?

24. Ich halte als EPU Vorträge ab. Wenn ein Kunde betreffend eines Vortrags anfragt und ich an diesem Termin keine Zeit habe gebe ich den Auftrag an KollegInnen weiter. In diesem Fall wird zB dem Kunden gesagt, ich kann nicht aber Kollegin XY könnte und ich gebe deren Nummer weiter bzw. meldet diejenige sich beim Kunden. Vorab wird natürlich gefragt ob ich seine Nummer weitergeben darf. Wie muss ich hier mit der Protollierung verfahren?
25. Wenn ich Kunden in Deutschland habe, muss ich dann ein eigenes Verzeichnis für Deutschland führen? Ich habe nur in Österreich einen Standort.
26. Gibt es für die Dokumentation eine Formvorschrift?
27. Darf ich meine Kundenliste im Excel weiter für meine Newsletter nutzen? Die Kundenliste beinhaltet Stammkunden und Laufkunden meines Betriebs.
28. Muss das Datenverarbeitungsverzeichnis öffentlich gemacht werden, oder reicht es dieses "griffbereit" zu haben?
29. Muss ich als Auftragsverbeiter (IT-Dienstleister) pro Kunden ein Verfahrensverzeichnis führen? Oder reicht eines, wo ich die Datenzwecke, -kategorien, -typen allgemein erfasse?
30. Wie funktioniert dies, wenn ich die Daten dem Steuerberater weitergebe (Buchhaltung, Steuerabwicklung..)wie wird dies vermerkt? Zum Verarbeitungsverzeichnis: Sind hier genau die einzelnen Vorgänge aufzulisten, die im Unternehmen vor sich gehen unter Nennung der Daten oder reichen "Stichwörter" zu den einzelnen Vorgängen
31. Gibt es ein Muster von einem Verarbeitungsverzeichnis?
32. Ich bin freiberufliche Physiotherapeutin, notiere Gesundheitsdaten, Namen, Adressen und Telefonnummer der Patienten schriftlich auf Papier, nur die Buchhaltung und Rechnungen laufen über den PC. Wie soll da das Verarbeitungsverzeichnis aussehen?
33. Auch Löschungen sind ja zu protokollieren? Wie protokolliere ich aber die Löschung eines konkreten Empfängers aus einem Newsletterverteiler, ohne die Daten in der Protokollierung zu nennen, also dort zu speichern? Und was ist mit Sicherungsbackups, in denen die Daten ja (noch lange) enthalten sein werden?
34. Muss ich alle Quellen aufzeichnen woher ich Firmendaten zB USTID Nummern habe?

---

1. Wie soll so ein Verarbeitungsverzeichnis genau ausschauen, und was gehört da genau eingetragen?

Unter diesen Links finden Sie ein Muster zum Verarbeitungsverzeichnis für den Verantwortlichen und den Auftragsverarbeiter, daraus ist auch ersichtlich, was tatsächlich eingetragen werden muss.

Das Verarbeitungsverzeichnis muss folgende Informationen enthalten: Den Zweck der Verarbeitung, die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland, die vorgesehene Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung.

2. Brauche ich nur ein Verarbeitungsverzeichnis? Oder sonst auch noch andere schriftliche Unterlagen/Nachweise?

Diese Frage ist so allgemein nicht abschließend zu beantworten.

Falls Sie personenbezogene Daten an unternehmensexterne Stellen übermitteln (beispielsweise externe Lohnverrechnung, IT-Dienstleister,...) so ist beispielsweise ein Vertrag mit diesen sogenannten Auftragsverarbeitern abzuschließen. Ein Muster finden Sie hier.

Darüber hinaus kann auch die Information und Einwilligungserklärung der Betroffenen schriftlich gestaltet werden.

3. Das Verzeichnis müssen wir wohl auch nur für "unsere" Daten führen, nicht für die Daten die im Rahmen unserer Dienstleistungen für unsere Kunden erhoben werden (z.B. Webshops)?

Es gibt zwei unterschiedliche Arten von Verarbeitungsverzeichnis, die sich hauptsächlich im Umfang unterscheiden:

Für „Ihre" Daten haben Sie das Verarbeitungsverzeichnis des Verantwortlichen zu führen. Dieses Verzeichnis ist umfangreicher, da der Verantwortliche derjenige ist, der über die Zwecke und Mittel der Datenverarbeitung entscheidet. Aus diesem Grund hat er mehr (alle?!) Informationen über die Datenverarbeitung und muss diese im Verzeichnis angeben.

Für die Daten Ihrer Kunden gelten Sie als Auftragsverarbeiter. Sie verarbeiten diese Daten also nur im Auftrag Ihrer Kunden (die selber Verantwortliche der Daten sind). Das Verzeichnis ist hier weniger umfangreich, da sie nicht alle Informationen über die Datenverarbeitung verfügen.

4. Müssen Aktivitäten, also zum Beispiel Newsletter nr, xy am xy usw, aufgezeichnet werden?

Nein, das Verarbeitungsverzeichnis soll einen allgemeinen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten. Hierfür ist der Verarbeitungszweck (zB Marketing oder Newsletterversand) allgemein anzugeben. Sollte sich an den Datenverarbeitungen im Unternehmen **nichts** ändern, ist dieses einmal zu erstellen und muss danach nicht mehr geändert werden.

5. Im Rahmen von Hacker-Abwehr werden von Servern IP Adressen gespeichert (z.B. um bei DDOS-Attacken diese sperren zu können). Inwieweit fallen diese Daten unter die notwendige Protokollierung?

Auch eine IP-Adresse ist ein personenbezogenes Datum und unterliegt daher der DSGVO. Dass die IP-Adresse gespeichert wird ist daher im Verarbeitungsverzeichnis unter „Kategorie der verarbeiteten Daten" anzugeben.

6. Eine Ausnahme von der Verzeichnisführung besteht, wenn "die Verarbeitung nur gelegentlich erfolgt". Was ist "gelegentlich"?

Der Begriff „gelegentlich" ist in der DSGVO nicht näher erläutert. Gemeint dürften Verarbeitungen sein, die nur sporadisch, wenn gerade Gelegenheit besteht, erfolgen. Als Beispiel wird das Anfertigen von Fotografien auf einem Firmenevent genannt.

Diese Ausnahmebestimmung ist jedoch insgesamt nicht sehr praxisrelevant. Es ist daher zum jetzigen Zeitpunkt davon auszugehen, dass grundsätzlich jedes Unternehmen, das eine Kundendatenbank führt oder eine Mitarbeiterverwaltung betreibt, ein Verarbeitungsverzeichnis benötigt.

7. Bitte um Beispiele wann Unternehmen unter 250 Mitarbeiter kein Verzeichnis für Verarbeitungstätigkeiten anlegen müssen (wenn kein Risiko für Rechte und Freiheiten der betroffenen Personen durch Datenverarbeitung besteht), was heißt das zum Beispiel?

Gleich vorweg: Diese Ausnahmebestimmung ist nicht sehr praxisrelevant. Der Gesetzestext spricht hier allgemein vom „Risiko für Rechte und Freiheiten der betroffenen Personen", er schränkt hier nicht auf ein „hohes" oder „besonderes" Risiko ein. Naturgemäß birgt jedoch jede Verarbeitung personenbezogener Daten ein Risiko, wodurch wiederum alle Datenverarbeitungen verzeichnet werden müssten. Man muss also wohl davon ausgehen, dass der Gesetzgeber hier doch ein „besonderes Risiko" gemeint hat. Als eine in diesem Sinne riskante Datenverarbeitung wurde in der Literatur beispielsweise das Scoring genannt, also die Bewertung der Kreditwürdigkeit durch den Kreditschutzverband in Österreich. Es ist daher zum jetzigen Zeitpunkt davon auszugehen, dass grundsätzlich jedes Unternehmen, das eine Kundendatenbank führt oder eine Mitarbeiterverwaltung betreibt, ein Verarbeitungsverzeichnis benötigt.

8. Kann oder soll man die IT Dokumentation in die Dokumentation aufnehmen?

Im Verarbeitungsverzeichnis müssen allgemein die technisch-organisatorischen Maßnahmen beschrieben werden, die den Schutz der personenbezogenen Daten gewährleisten.

9. Wie protokolliert man alle Daten? Wir haben 4 Ordner allein mit Zulassungsscheine, wo überall Adressen usw. drinnen stehen?

Es ist nicht erforderlich, dass tatsächlich jeder einzelne Datensatz in das Verarbeitungsverzeichnis eingetragen wird. Dieses soll keine Datenbank mit allen im Unternehmen vorhandenen Daten darstellen, sondern der Datenschutzbehörde einen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten.

Aus diesem Grund enthält das Verfahrensverzeichnis auch nur die Kategorien der personenbezogenen Daten (nicht „Max Mustermann, 01.01.1980,...", sondern „Name, Geburtsdatum,...").

Es ist nicht notwendig, dass der genaue Ort der Datenspeicherung angeführt wird.

10. Welche Software oder Tools gibt es die man zur Aufzeichnung nutzen kann?

Seitens der WKO finden Sie Muster für das Verarbeitungsverzeichnis für den Verantwortlichen und den Auftragsverarbeiter.

Wir können keine Anbieter bevorzugen, es gibt jedoch bereits einige, welche mit Lösungen (tlw auch Cloud-Lösungen) am Markt auftreten.

11. Muss ich als Personaler jeden Bewerber in das Verzeichnis schreiben?

Es ist nicht erforderlich, dass tatsächlich jeder einzelne Datensatz in das Verarbeitungsverzeichnis eingetragen wird. Dieses soll keine Datenbank mit allen im Unternehmen vorhandenen Daten darstellen, sondern der Datenschutzbehörde einen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten.

Aus diesem Grund enthält das Verfahrensverzeichnis auch nur die Kategorien der personenbezogenen Daten (nicht „Max Mustermann, 01.01.1980,…", sondern „Name, Geburtsdatum,…").

12. Muss man in diesem Verarbeitungsverzeichnis auch zB den Ordner anführen, in dem die Rechnung von dem Kunden aufbewahrt wird mit Name Adresse etc.?

Nein! Das Verarbeitungsverzeichnis soll lediglich einen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten. Hierbei ist es nicht notwendig, dass der genaue Ort der Datenspeicherung angeführt wird. Sie können das natürlich machen um die Daten im Einzelfall schneller auffinden zu können.

13. Darf ich fragen, ob ich als Auftragsverarbeiter diesen Prozess ebenfalls in meinem Unternehmen dokumentieren muss oder ob dies durch die Dokumentation im datenverarbeitenden Unternehmen erledigt ist?

Nein, auch der Auftragsverarbeiter muss ein Verzeichnis führen. Dieses unterscheidet sich jedoch im Umfang vom Verarbeitungsverzeichnis des Verantwortlichen, da der Auftragsverarbeiter naturgemäß nicht alle Informationen über die Datenverarbeitung besitzt. Ein Muster finden Sie hier.

14. Warum muss ich ein Verzeichnis führen obwohl ich nur 5 Mitarbeiter habe und kein Risiko birgt. Siehe Artikel 30 Verzeichnis von Verarbeitungstätigkeiten Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt.

Die genannte Ausnahmebestimmung ist leider nicht sehr praxisrelevant, da die einzelnen Voraussetzungen einerseits eher unklar und andererseits nicht häufig vorkommen:

Der Gesetzestext spricht hier allgemein vom „Risiko für Rechte und Freiheiten der betroffenen Personen", er schränkt hier nicht auf ein „hohes" oder „besonderes" Risiko ein. Naturgemäß birgt jedoch jede Verarbeitung personenbezogener Daten ein Risiko, wodurch wiederum alle Datenverarbeitungen verzeichnet werden müssten. Man muss also wohl davon ausgehen, dass der Gesetzgeber hier doch ein „besonderes Risiko" gemeint hat. Auch der Begriff „gelegentlich" ist in der DSGVO und in den Erwägungsgründen nicht näher erläutert. Gemeint dürften Verarbeitungen sein, die nur sporadisch, wenn gerade Gelegenheit besteht, erfolgen. Als Beispiel wird das Anfertigen von Fotografien auf einem Firmenevent genannt. Es ist daher zum jetzigen Zeitpunkt davon auszugehen, dass grundsätzlich jedes Unternehmen, das eine Kundendatenbank führt oder eine Mitarbeiterverwaltung betreibt, ein Verarbeitungsverzeichnis benötigt.

15. Müssen in einem EPU beide Verarbeitungsverzeichnisse (für Verantwortliche + Auftragsverarbeiter) von derselben Person geführt werden?

Ja, jedes Unternehmen kann für unterschiedliche personenbezogene Daten gleichzeitig Verantwortlicher und Auftragsverarbeiter sein.

Ich bin beispielsweise als IT-Dienstleister Verantwortlicher im Sinne der DSGVO für die personenbezogenen Daten meiner eigenen Kunden/Auftraggeber. Programmiere ich einen Webshop und habe zur Wartung Zugriff auf die Bestelldaten, so verarbeite ich für meinen Kunden personenbezogene Daten seiner Kunden. Im Hinblick auf diese Daten bin ich daher Auftragsverarbeiter. Wen Sie konkret im Betrieb oder außerhalb des Betriebes mit der Erstellung beauftragen, ist Ihre Entscheidung.

16. Wir haben drei Firmen unter einem Dach mit einer gemeinsamen IT-Infrastruktur. Kann man das Datenanwendungsverzeichnis für alle drei Firmen gemeinsam erstellen?

Grundsätzlich ist jedes Unternehmen verpflichtet ein eigenes Verarbeitungsverzeichnis zu führen. Sind die Datenverarbeitungen jedoch in den Unternehmen zum Teil ident, kann man diese natürlich einmal formulieren und für die anderen Verarbeitungsverzeichnisse übernehmen.

17. Aus meiner Datenbank generiere ich eine Excelliste mit personenbezogenen Daten, um z.B. einen oder mehrere Gesichtspunkte genauer zu analysieren. Was muss ich aus datenschutzrechtlicher Sicht bzgl. dieser Excel Datei tun/dokumentieren?

Diese Datenverarbeitung ist im Verarbeitungsverzeichnis anzuführen. Hierbei sind der Zweck der Verarbeitung, die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland, die vorgesehene Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung anzugeben.

18. Wir haben keine Kunden, bei denen personenbezogene Daten verarbeitet werden (ausschließlich Unternehmen als Kunden). Die einzigen personenbezogenen Daten sind die der Mitarbeiter. Müssen wir auch ein Verarbeitungsverzeichnis erstellen?

Ja, denn auch die personenbezogenen Daten von Mitarbeitern werden durch die DSGVO geschützt. Darüber hinaus werden nach der derzeitigen Rechtslage in Österreich auch juristische Personen durch die DSGVO geschützt. Diese Situation ist nicht gewollt, allerdings aufgrund einer fehlenden Zweidrittelmehrheit im Nationalrat entstanden. Es bleibt abzuwarten, ob dieser Punkt bis zum 25. Mai 2018 bereinigt werden kann.

19. Wie oft muss das Verarbeitungsverzeichnis aktualisiert werden oder nur muss es nur einmal erstellt werden?

Sollte sich in der Datenverarbeitung in Ihrem Unternehmen nichts ändern – beispielsweise keine neuen Datenverarbeitungen, Datenkategorien oder Empfänger hinzukommen -, so muss das Verarbeitungsverzeichnis nur einmal erstellt werden.

Sobald sich hinsichtlich der im Unternehmen vorhandenen Datenverarbeitungen etwas ändert, ist das Verarbeitungsverzeichnis zu aktualisieren.

20. Wir verwenden Im Betrieb u.a. einen Outlooksystem, welches Kundendaten (Name, Tel, Anschrift) automatisch auf Handys synchronisiert, dh diese Situation dokumentiere ich im Verarbeitungsverzeichnis?

Der genaue Vorgang ist nicht im Verarbeitungsverzeichnis anzugeben. Im Verarbeitungsverzeichnis müssen jedoch unter anderem die Kategorien von Empfängern (Auftragsverarbeiter und sonstige Empfänger der Daten) genannt werden. Hierbei dient Outlook als Auftragsverarbeiter (es verarbeitet die personenbezogenen Daten in Ihrem Auftrag). Dies ist im Verarbeitungsverzeichnis anzuführen.

21. Muss ich jedes Mal wenn ich ein Mail mit Kundendaten weiterleite ein Protokoll darüber verfassen? Oder nur einmal, dass ich sowas tue?

Nein, es ist nicht jede einzelne tatsächlich durchgeführte Datenverarbeitung anzugeben. Das Verarbeitungsverzeichnis dient lediglich als Überblick über die im Unternehmen vorhandenen Datenverarbeitungen.

22. Muss man jede Verwendung von Daten, wenn diese Verwendet werden aufzeichnen? Wenn ja, wie?

Nein, es ist nicht jede einzelne tatsächlich durchgeführte Datenverarbeitung anzugeben. Das Verarbeitungsverzeichnis dient lediglich als Überblick über die im Unternehmen vorhandenen Datenverarbeitungen.

23. Wie ist Dokumentationspflicht im Verarbeitungsverzeichnis in Bezug auf elektronisch erfasste Dokumente (Geschäftsbriefe, Protokolle, etc.), die Texte und Daten beliebiger Art enthalten können?

Im Verarbeitungsverzeichnis sind der Zweck der Verarbeitung, die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland, die vorgesehene Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung anzugeben.

Es ist jedoch weder anzugeben, wo die personenbezogenen Daten tatsächlich gespeichert werden noch der Inhalt der Dokumente.

24. Ich halte als EPU Vorträge ab. Wenn ein Kunde betreffend eines Vortrags anfragt und ich an diesem Termin keine Zeit habe gebe ich den Auftrag an KollegInnen weiter. In diesem Fall wird zB dem Kunden gesagt, ich kann nicht aber Kollegin XY könnte und ich gebe deren Nummer weiter bzw. meldet diejenige sich beim Kunden. Vorab wird natürlich gefragt ob ich seine Nummer weitergeben darf. Wie muss ich hier mit der Protollierung verfahren?

Im Verarbeitungsverzeichnis sind unter anderem die Kategorien von Empfängern anzugeben. In diesem Fall würde ich beim Verarbeitungszweck „Rechnungswesen und Geschäftsabwicklung" bei den möglichen Empfängern „KollegInnen im Anlassfall und nach vorheriger Rücksprache mit der betroffenen Person" anführen.

25. Wenn ich Kunden in Deutschland habe, muss ich dann ein eigenes Verzeichnis für Deutschland führen? Ich habe nur in Österreich einen Standort.

Nein. Aufgrund des Territorialitätsprinzips gilt für Unternehmen, die eine Niederlassung in Österreich haben das österreichische Datenschutzgesetz sowie die DSGVO. Ein Verarbeitungsverzeichnis muss in Ihrem Fall nur am Ort Ihrer Niederlassung – also in Österreich – geführt werden.

26. Gibt es für die Dokumentation eine Formvorschrift?

Das Verarbeitungsverzeichnis ist schriftlich zu führen. Die DSGVO lässt auch ein elektronisches Verarbeitungsverzeichnis zu. Abgesehen davon sind in der DSGVO keine Formvorschriften über Verarbeitungsverzeichnisse enthalten. Sie können dieses also in einem Word- oder Exceldokument oder sogar handschriftlich verfassen.

27. Darf ich meine Kundenliste im Excel weiter für meine Newsletter nutzen? Die Kundenliste beinhaltet Stammkunden und Laufkunden meines Betriebs.

Diese Frage kann keinesfalls eindeutig und abschließend beantwortet werden, da hierbei viele unterschiedliche Aspekte zu beachten sind:

Beginnend mit den bei jeder Datenverarbeitung einzuhaltenden **Grundsätzen** ergeben sich viele Fragen: Sind die Daten aktuell und richtig? Habe ich eine Rechtsgrundlage für die Datenverarbeitung? Ist eine angemessene Sicherheit für die personenbezogenen Daten gewährleistet? Als mögliche Rechtsgrundlage der Datenverarbeitung kommt bei Newslettern einerseits die Einwilligung, andererseits das berechtigte Interesse des Verantwortlichen in Betracht.

Ihre Frage könnte auch auf die Sicherheit der personenbezogenen Daten abspielen: Hierbei sind geeignete technische und organisatorische Maßnahmen zu treffen. Der Ort an welchen die Excel-Liste gespeichert ist, sollte daher beispielsweise passwortgeschützt sein; haben viele Personen Zugriff auf den Computer sollte die Excel-Liste passwortgeschützt sein.

Zusätzlich ist beim Versand von Newslettern das Telekommunikationsgesetz (§ 107 TKG) zu beachten.

28. Muss das Datenverarbeitungsverzeichnis öffentlich gemacht werden, oder reicht es dieses "griffbereit" zu haben?

Nein, das Verarbeitungsverzeichnis ist ein bloß „internes" Dokument, das lediglich der Datenschutzbehörde vorgewiesen werden muss, wenn diese danach fragt.

29. Muss ich als Auftragsverbeiter (IT-Dienstleister) pro Kunden ein Verfahrensverzeichnis führen? Oder reicht eines, wo ich die Datenzwecke, -kategorien, -typen allgemein erfasse?

Grundsätzlich muss zumindest pro Verantwortlichen ein eigenes Stammblatt (Punkt B im Muster) geführt werden. Es gibt Meinungen in der Literatur, die bei Auftragsverarbeitern im Massengeschäft (Cloud Service-Provider, Hosting-Anbieter, Software-as-a-Service-Plattformen) an dieser Stelle die Angaben auf die bloße Kategorie von Verantwortlichen beschränken, um das Verzeichnis handhabbar zu erhalten. Sofern eine Anfrage der Aufsichtsbehörde nach dem Verzeichnis der Verarbeitungstätigkeit eingeht, sollte dieser Punkt erläutert werden. Der Auftragsverarbeiter wird jedenfalls eine Übermittlung der Liste der Verantwortlichen anbieten müssen.

30. Wie funktioniert dies, wenn ich die Daten dem Steuerberater weitergebe (Buchhaltung, Steuerabwicklung..)wie wird dies vermerkt? Zum Verarbeitungsverzeichnis: Sind hier genau die einzelnen Vorgänge aufzulisten, die im

Unternehmen vor sich gehen unter Nennung der Daten oder reichen "Stichwörter" zu den einzelnen Vorgängen?

Im Verarbeitungsverzeichnis sind unter anderem die Kategorien von Empfängern (Auftragsverarbeiter, andere Verantwortliche, sonstige Empfänger) anzugeben. Der Steuerberater wäre daher unter diesem Punkt anzugeben. Im Muster ist dies beispielsweise unter Punkt C.4.a. anzuführen).

Das Verarbeitungsverzeichnis soll einen allgemeinen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten. Jeder Unternehmer sollte sich zuerst überlegen, zu welchen Zwecken er Daten verarbeitet. Anschließend sollten für jeden Zweck die Kategorien von betroffenen Personen, die Kategorien der verarbeiteten Dategrun, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland, die vorgesehene Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung angegeben werden.

Ein Beispiel in welchem auch der Umfang der Dokumentation ersichtlich ist, finden Sie hier.

31. Gibt es ein Muster von einem Verarbeitungsverzeichnis?

Ja. Das Muster für das Verarbeitungsverzeichnis des Verantwortlichen finden Sie hier.

Das Muster für Auftragsverarbeiter finden Sie hier.

32. Ich bin freiberufliche Physiotherapeutin, notiere Gesundheitsdaten, Namen, Adressen und Telefonnummer der Patienten schriftlich auf Papier, nur die Buchhaltung und Rechnungen laufen über den PC. Wie soll da das Verarbeitungsverzeichnis aussehen?

Hierbei sind mehrere Punkte zu beachten:

1. Die DSGVO findet auch auf die analoge Verarbeitung personenbezogener Daten Anwendung, wenn diese einer Ordnung unterliegen. Wenn die Kundenkarten daher beispielsweise alphabetisch, geographisch oder nach dem Datum des erstmaligen Kontaktes geordnet sind, unterliegen sie der DSGVO. Lediglich Akten in Papierform, die nicht nach bestimmten Kriterien geordnet werden, unterliegen nicht der Verordnung.
2. Das Verarbeitungsverzeichnis soll einen allgemeinen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten. Jeder Unternehmer sollte sich zuerst überlegen, zu welchen Zwecken er Daten verarbeitet. Anschließend sollten für jeden Zweck die Kategorien von betroffenen Personen, die Kategorien der verarbeiteten Daten, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland, die vorgesehene Speicherdauer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung angegeben werden

Ein Muster finden Sie hier.

33. Auch Löschungen sind ja zu protokollieren? Wie protokolliere ich aber die Löschung eines konkreten Empfängers aus einem Newsletterverteiler, ohne die Daten in der Protokollierung zu nennen, also dort zu speichern? Und was ist mit Sicherungsbackups, in denen die Daten ja (noch lange) enthalten sein werden?

Im Verarbeitungsverzeichnis ist lediglich die vorgesehene Frist für die Löschung zu protokollieren. Jeder einzelne Löschvorgang muss nicht verzeichnet werden.

Das österreichische Datenschutzgesetz hat für den Fall, dass die Löschung aus Backups aus wirtschaftlichen oder technischen Gründen nicht unverzüglich erfolgen kann, festgelegt, dass die Löschung auch zu einem späteren Zeitpunkt vorgenommen werden kann. Die Verarbeitung der Daten ist jedoch bis zum Löschungszeitpunkt einzuschränken (bloße Speicherung der personenbezogenen Daten, keine anderen Formen der Verarbeitung).

34. Muss ich alle Quellen aufzeichnen woher ich Firmendaten zB USTID Nummern habe?

Im Verarbeitungsverzeichnis sind nicht alle Datenquellen aufzuzeichnen, allerdings muss im Rahmen der Informationspflichten bzw beim Auskunftsersuchen über die Herkunft der Daten Bescheid gegeben werden können.

Stand: 23.04.2018