EU-Datenschutz-Grundverordnung (DSGVO): Die wichtigsten Fragen und Antworten

Was Unternehmen auf jeden Fall wissen und berücksichtigen sollten

27. Wie weit geht das Recht auf Berichtigung?

28. Muss ich meine Kundendatenbank jetzt jeden Tag updaten?

29. Was umfasst das Auskunftsrecht von Betroffenen?

30. Muss ich beim Auskunftsrecht alle E-Mails dem Anfragenden zusenden?

31. Welche Auswirkungen hat das "Recht auf Vergessenwerden" (Löschung) in der Praxis?

32. Muss ich personenbezogene Daten löschen oder reicht die Einschränkung der Datenverarbeitung?

33. Was passiert, wenn ein Kunde seine Löschung beantragt, aber der Datensatz aufgrund der Aufbewahrungspflicht 7 Jahre aufbewahrt werden muss (z. B. die Rechnung mit den Kundendaten)?

34. Wie lange dürfen Daten gespeichert werden?

35. Wie lange darf ich Daten von Interessenten aufbewahren?

36. Wie können Daten aus Backups oder Datensicherungen gelöscht werden?

37. Muss nachgewiesen werden, dass ein Datensatz gelöscht wurde?

38. In welchem Zeitrahmen muss ich auf Anfragen von betroffenen Personen (z. B. auf Auskunft, auf Löschung, ...) reagieren?

39. Gibt es Ausnahmen, um nicht auf Anfragen von betroffenen Personen reagieren zu müssen?

40. Kann ich ein Entgelt für solche Anfragen verlangen?

41. Muss ich mir jetzt für jede Datenverarbeitung eine Einwilligung holen?

42. Wenn ich eine Einwilligung brauche, wie schaut die aus?

43. Müssen bestehende Kunden erneut einwilligen, kontaktiert werden zu dürfen?

44. Ist bei Kindern etwas speziell zu beachten?

45. Wie kann ich sensible Daten verarbeiten?

46. Wie identifiziere ich die Person?

47. Was genau bedeutet Profiling und was ist zu beachten?

48. Wie ist das Verarbeitungsverzeichnis?

49. Muss ein Auftragsverarbeiter mehrere Verarbeitungsverzeichnisse führen?

50. Müssen einzelne Aktivitäten, z. B. Mail an XY am 1.1.2001 aufgezeichnet werden?

51. Eine Ausnahme von der Verzeichnisführung besteht für KMU mit weniger als 250 Mitarbeitern, wenn "die Verarbeitung nur gelegentlich erfolgt und kein Risiko damit verbunden ist". Was fällt darunter?

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

53. Gibt es für das Verarbeitungsverzeichnis eine Formvorschrift?

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

55. Was bedeutet "ausdrückliche Zustimmung"? Muss das schriftlich erfolgen und mit Unterschrift bestätigt werden?

56. Ist es möglich eine Zustimmung von Kunden über Social Media einzuholen oder über AGB?

57. Müssen alle vorhandenen Kunden, die in Stammkundendatei bereits gespeichert sind, eine Einwilligungserklärung zugesendet oder vorgelegt werden? Wie muss man da vorgehen?

58. Wenn man z. B. Stammdaten von Kunden erhebt, inwiefern muss man dessen Einverständnis dokumentieren/beweisen können?

59. Wann brauche ich einen Datenschutzbeauftragten?

60. Dürfen IT-Leiter, Personalleiter u. Ä. zum Datenschutzbeauftragten bestellt sein?

62. Was ist die Funktion und vor allem die Haftung des Datenschutzbeauftragten?

63. Braucht ein Datenschutzbeauftragter eine verpflichtende Ausbildung und/oder Zertifikat, oder kann man sich das Wissen dazu auch selbstständig aneignen als IT-Dienstleister?

64. Haftet der Datenschutzbeauftragte zukünftig wirklich persönlich für Verfehlungen?

65. Wer kontrolliert Datenschutz? Werden z. B. stichprobenartige Kontrollen gemacht oder wird nur dann nachgefragt/kontrolliert, wenn sich jemand dezidiert beschwert?

66. Welche Strafen sind vorgesehen?

67. Können die Strafen höher als der Unternehmensumsatz sein?

68. Darf ich gesammelte Daten an Werbepartner weitergeben?

69. Was ist ein Datenleck, eine Datenpanne bzw ein data breach?

70. Muss ich in Zukunft verschlüsseln?

71. Was bedeutet ausreichend Schutz?

72. Was bedeutet Privacy by design für den Betrieb?

73. Was bedeutet Privacy by default für den Betrieb?

74. Darf mein Steuerberater meinen Steuerakt überhaupt noch per E-Mail versenden?

75. Darf ich weiterhin Clouds verwenden?

76. Was ist mit mobilen Applikationen?

77. Wie muss ich Daten sichern, die in Papierform festgehalten werden?

78. Wie müssen Mitarbeiter belehrt werden?

79. Datenschutz-Anpassungsgesetz 2018 (DSAG 2018) - Welche Regelungen enthält das Gesetz?

80. Unter welchen Voraussetzungen ist künftig Videoüberwachung zulässig?

81. Besteht die Pflicht zur Kennzeichnung bei der Verwendung von Videokameras?

82. Dürfen Daten zu statistischen Zwecken weiterhin ausgewertet werden?

83. Dürfen Strafregisterauszüge verarbeitet werden?

84. Darf ich nun keine Rechnungen mehr ausstellen, Daten der Bank weitergeben, Überweisungen tätigen, usw?

85. Sind Whistleblower-Hotlines 2018 noch zulässig?

86. Ist der 25.5.2018 fix oder gibt es noch Übergangsfristen, innerhalb deren nicht gestraft wird?

87. Darf ich noch weiterhin Newsletter verschicken?

88. Darf ich Unternehmen kontaktieren, deren Daten ich aus dem Internet (z. B. verpflichtenden Impressum) habe?

89. Was muss ich auf der Website umstellen?

90. Dürfen Daten aus öffentlichen Quellen ohne Einwilligung der Betroffenen verwendet werden?

91. Was sind die wichtigsten Basics, die wirklich jedes Unternehmen haben muss?

92. Wenn ich meinen Unternehmenssitz ins Ausland verlege, bin ich dann auch aus der DSGVO raus?

93. Das klingt alles irrsinnig aufwändig.

94. Brauche ich einen externen Berater oder schaffe ich das alles allein?

95. Wo gibt es weitere Infos?

1. Bin ich von der DSGVO betroffen?

Als Unternehmer – Ja! Immer!

Die Ausnahmen vom Anwendungsbereich der DSGVO sind in der DSGVO abschließend aufgezählt. Eine Ausnahme gibt es für die Datenverarbeitung durch Privatpersonen ausschließlich für „persönliche oder familiäre Tätigkeiten". Alle österreichischen Unternehmen jeder Branche sind von der DSGVO betroffen, auch ARGE, Vereine, Ärzte, KMU, EPU, Schulen etc.

Achtung:
Es ist egal, wie groß das Unternehmen ist, wieviel Daten verarbeitet werden, ob es eine heikle Tätigkeit ist oder nicht – Jedes österreichische Unternehmen ist betroffen!

2. Gibt es Spezialregelungen für KMU?

Nein. Es gibt keine Ausnahme für kleine oder mittelgroße Unternehmen, auch keine Ausnahmen für Ein-Personen-Betriebe.

3. Was sind personenbezogene Daten?

Personenbezogen ist alles, was nur in irgendeiner Art und Weise einen Bezug zu einer natürlichen Person herstellen kann, also z. B. Name (auf Rechnungen, in Datenbanken, ...), Adresse, Telefonnummer, Abbilder, Stimme.

4. Was sind sensible Daten?

Das sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person (z. B. Fingerabdruck, Irisscan, Krankengeschichte, Allergien, Religionsbekenntnis, Fingerprint-Sensoren,...).

5. Ist die Sozialversicherungsnummer ein sensibles Datum?

Da als Gesundheitsdaten und daher sensible Daten auch Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, eingeordnet werden, wird die Sozialversicherungsnummer mit sehr hoher Wahrscheinlichkeit in Zukunft als sensibles Datum einzuordnen sein.

Nach der Datenschutzbehörde ist außerdem die Verwendung der Sozialversicherungsnummer nur für Sozialversicherungszwecke oder bei ausdrücklicher gesetzlicher Erlaubnis zulässig.

6. Gilt die DSGVO auch B2B?

Ja. B2B (business to business) oder B2C (business to consumer) macht keinen Unterschied. Lediglich die Daten einer GmbH oder AG (demnach die Daten der juristischen Person) sind laut DSGVO nicht als personenbezogen einzuordnen.

Die DSGVO sagt hier klar nein, das Datenschutz-Anpassungsgesetz 2018 ist hier leider nicht so eindeutig. Man muss noch abwarten, was die Rechtsprechung dazu sagt.

7. Was versteht man unter "verarbeiten"?

Jede Handhabe mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

8. Welche Datenverarbeitungen sind umfasst?

Jede Verarbeitung (= erheben, erfassen, bearbeiten, speichern, weitergeben, löschen, ...) von personenbezogenen Daten.

9. Gilt die DSGVO nur für elektronische Datenverarbeitung oder zB auch für handschriftliche Aufzeichnungen?

Sofern diese Aufzeichnungen in einem Dateisystem aufbewahrt werden, fällt auch der Papierakt darunter.

Dateisystem ist eine strukturierte Sammlung personenbezogener Daten, die nach bestimmen Kriterien geordnet ist (z. B. alphabetisch, chronologisch,

...).

10. Sind „Altdaten“, d.h. jene Daten, die vor dem 25.5.2018 erfasst wurden, aber noch weiter nach dem 25.5.2018 gespeichert werden, auch betroffen?

Sobald die DSGVO gilt, ist sie einzuhalten. Das gilt auch für "Altdaten".

11. Umfasst die DSGVO nur Datensätze in operativen Systemen (wie CRM, ERP, ...) oder auch auf Backup-Bändern und in E-Mail-Postfächern?

Die DSGVO findet Anwendung auf die Verarbeitung (darunter fällt u.a. auch die Speicherung) von personenbezogenen Daten.

Welche Technologie dabei verwendet wird, ist nicht wesentlich. Es fallen daher auch personenbezogene Daten in den Anwendungsbereich, die in Backups oder in E-Mail-Postfächern gespeichert sind.

12. Wer haftet? Wer ist der Verantwortliche im Unternehmen?

Das Unternehmen selbst. Ist das Unternehmen eine juristische Person (GmbH, AG), haftet dieses in erster Linie. Der **Verantwortliche Beauftragt**e (§ 9 VStG, Geschäftsführer oder bestellte Person) haftet nur ausnahmsweise.

13. Was sind die Folgen für die gemeinsame Datenverarbeitung zwischen Unternehmen die rechtlich verbunden sind (z. B. Mutter- / Tochterunternehmen, Landes-/Bezirksverein)?

Es handelt sich dabei um **Gemeinsame Verantwortliche**, wenn sie gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen. In diesem Fall ist in einer Vereinbarung festzuhalten, wer von ihnen welche gesetzliche Verpflichtung übernimmt (z.B. wer handhabt die Betroffenenrechte, wer kommt den Informationspflichten nach).

In der Vereinbarung kann auch eine Anlaufstelle für die betroffenen Personen angegeben werden. Unabhängig vom Inhalt der Vereinbarung können betroffene Personen ihre Rechte aber gegenüber jedem Einzelnen geltend machen.

Die Vereinbarung ist aber für die interne Aufgabenverteilung und etwaige Regressansprüche gegeneinander wichtig.

14. Kann ich die Haftung mit dem Kunden einvernehmlich ausschließen?

Zu dieser Frage gibt es weder Rechtsprechung noch Literaturmeinungen in Österreich.

Nach deutscher Ansicht ist ein vertraglicher Haftungsausschluss nicht möglich. Die Haftung für DSGVO-widriges Verhalten generell auszuschließen ist mit hoher Wahrscheinlichkeit sittenwidrig (iSd § 879 Abs 1 ABGB).

15. Kann man die Haftung jemand Drittes übertragen?

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 des Datenschutzrechtes verfügen muss (insbesondere beim Thema Datensicherheit sind die Mitarbeiter unbedingt zu schulen!).

Achtung:
Ein gänzliches "Outsourcing" des Themas Datenschutz ist damit nicht möglich. Auch die Verantwortung kann man als Unternehmen nicht gänzlich outsourcen.

Achtung:
Ein allfällig bestellter Datenschutzbeauftragter kann nicht für die Strafen nach der DSGVO in Anspruch genommen werden!

16. Können weiterhin externe Dienstleister für die Datenverarbeitung herangezogen werden?

Externe Dienstleister, die man zur Datenverarbeitung heranzieht, nennt man **Auftragsverarbeiter**. Auftragsverarbeiter können z. B. Cloud-Anbieter, IT-Dienstleister, Buchhalter, Lohnverrechner, Werbeagenturen, Newsletteranbieter etc sein.

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**.

17. Sind Banken, Versicherungen, Finanzamt usw Auftragsverarbeiter?

Die Einordnung, in welcher Rolle jemand datenschutzrechtlich auftritt, ist recht schwierig und muss immer im Einzelfall erfolgen.

Wesentlich sind hier die Fragen: Wer trifft die Entscheidung, was mit den Daten passiert und wer entscheidet über die Mittel und Zwecke der Datenverarbeitung?

Die angesprochenen Parteien sind wohl eher als eigenständige Verantwortliche zu werten und nicht als Auftragsverarbeiter.

18. Inwieweit bin ich für die Einhaltung der DSGVO bei auftretenden Problemen bei externen Anbietern (Auftragsverarbeitern) 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 könnte allerdings die Gehilfenhaftung greifen, d.h. man könnte mitunter schadenersatzpflichtig werden, wenn bei der Erfüllung eines Vertrages ein Schaden entsteht, haftet der Auftragnehmer für das Verschulden seines Erfüllungsgehilfen wie für eigenes Verschulden.

19. Gibt es noch Meldepflichten bei der Datenschutzbehörde?

Nur mehr in 2 Fällen: Wenn ich ein Datenleck feststelle (data breach, siehe unten) und wenn meine Datenverarbeitung sehr riskant ist und ich bei der Datenschutz-Folgenabschätzung zum Ergebnis komme, dass ich das Risiko nicht eindämmen kann.

20. Wie erkenne ich, ob eine Datenverarbeitung riskant ist bzw was ist die Datenschutz-Folgenabschätzung?

Die Datenschutz-Folgenabschätzung ist eine Art Worst-Case-Scenario. Was mache ich mit Daten, welche Daten verarbeite ich, zu welchen Zwecken, welche Risiken gehen damit einher und wie kann ich die Risiken eindämmen.

Eine Folgenabschätzung ist immer dann nötig, wenn ich zum Schluss komme, dass eine Datenverarbeitung riskant ist, z. B. bei einer systematischen und umfassenden Bewertung persönlicher Aspekte (z. B. Profiling nach Art 22 DSGVO), bei einer umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten, bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung).

Wenn ich die Risiken nicht eindämmen kann, muss ich nach wie vor der Behörde melden » siehe auch: **Datenschutz-Folgenabschätzung und vorherige Konsultation**.

21. Wo bekomme ich eine DVR Nummer?

Eine DVR Nummer (Nummer vom Datenverarbeitungsregister) bekommt man bis zum 25.05.2018 bei der **Datenschutzbehörde**. Nach dem 25.5.2018 gibt es keine mehr und sollte die Nummer auch aus Ihren Papieren, Website etc. gestrichen werden.

22. Welche "Betroffenenrechte" gibt es?

- **Informationspflicht** bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

- **Auskunftsrecht**
- Recht auf **Berichtigung**
- Recht auf **Löschung** ("Recht auf Vergessenwerden")
- Recht auf **Einschränkung** der Verarbeitung
- Recht auf **Datenübertragbarkeit**
- **Widerspruchsrecht**

23. Über was muss ich informieren?

Die Informationspflicht geht sehr weit und ist vom Auskunftsanspruch zu trennen, da letzterer erst zu erfüllen ist, wenn eine Anfrage von einer betroffenen Person vorliegt. Informationen hingegen müssen davon unabhängig selbstständig bereitgestellt werden, z. B. mittels einer Datenschutzerklärung.

> **Achtung:**
> Informationen sind direkt bei der Datenerhebung zu geben, wenn diese bei der betroffenen Person direkt erfolgt! Erhält man die Daten anderweitig (z. B. von öffentlichen Quellen, von Marketingunternehmen, von Konzernunternehmen, ...), muss man den Betroffenen innerhalb von einem Monat die Informationen (siehe unten) zur Verfügung stellen.

Wenn die **Daten von der betroffenen Person direkt erhoben** wurden:

- Namen und Kontaktdaten des Verantwortlichen (und ggf. seiner Vertreter),
- ggf. Kontaktdaten des Datenschutzbeauftragten,
- Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung,
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen bzw. eines Dritten sind die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, auszuweisen,
- ggf. Empfänger der Daten,
- falls die Absicht besteht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, muss auch darüber informiert werden, ebenso wie über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission. Weiters ist im Falle von Datenübermittlung vorbehaltlich geeigneter Garantien oder aufgrund von verbindlichen internen Datenschutzvorschriften, bzw. generell aufgrund von besonderen Ausnahmebestimmungen eben auf diese geeigneten oder angemessenen Garantien zu verweisen oder zumindest, wo eine Kopie erhältlich wäre,
- Dauer der Datenspeicherung bzw wenn unmöglich die **Kriterien für die Festlegung** der Dauer,
- **Betroffenenrechte** auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch,
- die Möglichkeit des Widerrufs der Einwilligung,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte,
- ggf über das Bestehen automatisierter Entscheidungsfindung, inkl. aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung (z. B. Profiling).
- Sollen die Daten für einen anderen als den ursprünglichen Zweck weiterverarbeitet werden, müssen vor der Weiterverarbeitung auch Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen erteilt werden.

Wenn die Daten **nicht von der betroffenen Person** direkt erhoben wurden:

- den Namen und die Kontaktdaten des Verantwortlichen (und ggf. seiner Vertreter),
- ggf die Kontaktdaten des Datenschutzbeauftragten,
- Verarbeitungszwecke und Rechtsgrundlagen der Verarbeitung,
- die Kategorien personenbezogener Daten, die verarbeitet werden,
- ggf Empfänger der Daten,
- falls die Absicht besteht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, muss auch darüber informiert werden, ebenso wie über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission. Weiters ist im Falle von Datenübermittlung vorbehaltlich geeigneter Garantien oder aufgrund von verbindlichen internen Datenschutzvorschriften, bzw. generell aufgrund von besonderen Ausnahmebestimmungen eben auf diese geeigneten oder angemessenen Garantien zu verweisen oder zumindest, wo eine Kopie erhältlich wäre,
- Dauer der Datenspeicherung bzw. wenn unmöglich die **Kriterien für die Festlegung** der Dauer,
- im Falle einer Datenverarbeitung aufgrund berechtigter Interessen des Verantwortlichen bzw eines Dritten sind die berechtigten Interessen, die vom Verantwortlichen oder einem Dritten verfolgt werden, auszuweisen,
- **Betroffenenrechte** auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch,
- die Möglichkeit des Widerrufs der Einwilligung,
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde,
- aus welcher Quelle die personenbezogenen Daten stammen (z. B. öffentlich zugängliche Quelle),
- ggf über das Bestehen automatisierter Entscheidungsfindung, inkl. aussagekräftiger Informationen über die involvierte Logik und die Tragweite der Entscheidung (z. B. Profiling).
- Sollen die Daten für einen anderen als den ursprünglichen Zweck weiterverarbeitet werden, müssen vor der Weiterverarbeitung auch Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen erteilt werden.

24. Reicht für die Erfüllung der Informationspflichten eine Verlinkung auf die Website des Unternehmens?

Die Informationen nur auf der Website zu implementieren, aber ansonsten dem Betroffenen keinen Hinweis o.Ä. zu geben, wo sie zu finden sind, wird nicht ausreichen. Empfehlenswert wäre z. B. den Link, der direkt auf die Datenschutzerklärung auf der Website führt, in der E-Mail Signatur u.Ä. zu verankern. Individuelle Muster kann man sich selbst im **Online-Ratgeber** erstellen.

25. Wie kann ich am Telefon informieren?

Telefonisch wird man

1. kaum Zeit haben, alle Informationen "an den Kunden zu bringen" bzw.
2. ist der Nachweis recht schwierig. Es empfiehlt sich wohl in der Praxis auf die Datenschutzerklärung der Website zu verweisen und sich an die Basics zu halten (Wer bin ich, warum rufe ich an,...).

26. In welchem Ausmaß müssen Subunternehmen an Kunden bekanntgegeben werden?

Grundsätzlich sind alle "Empfänger" von Daten bekannt zu geben. Wenn Sie den Subunternehmern Daten weitergeben, sind diese jedenfalls Empfänger. Empfänger ist sehr weit zu interpretieren und erfasst z. B. auch Auftragsverarbeiter.

27. Wie weit geht das Recht auf Berichtigung?

Voraussetzung für den Anspruch ist, dass die Daten unrichtig sind, also mit der Wirklichkeit nicht übereinstimmen (z. B. falsches Geburtsdatum) oder dass die Daten unter Berücksichtigung des Zweckes der Verarbeitung, unvollständig sind.

28. Muss ich meine Kundendatenbank jetzt jeden Tag updaten?

Das ist wohl nicht gemeint, aber wenn Sie erkennen, dass der Kunde z. B. falsch erfasst wurde (Herr statt Frau) o.Ä., sollte das entsprechend korrigiert werden.

Bei älteren Datensätzen kann sich je nach Inhalt die Frage stellen, ob diese noch korrekt sind und ob sie nicht aktualisiert werden sollten.

29. Was umfasst das Auskunftsrecht von Betroffenen?

Das Auskunftsrecht umfasst:

- Kopien der Daten (E-Mails, Briefe, Auszüge aus Datenbanken, udgl.), die konkret verarbeiteten Daten;
- die Verarbeitungszwecke;
- die Kategorien der Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern oder bei internationalen Organisationen (einschließlich Auftragsverarbeiter),
- wenn möglich, die geplante Speicherfrist für die Daten, oder falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- alle verfügbaren Informationen über die Herkunft der Daten (falls die Daten nicht beim Betroffenen selbst erhoben worden sind);
- im Fall von Entscheidungen, die auf einer automatisierten Verarbeitung einschließlich Profiling beruhen, und gegenüber der betroffenen Person rechtliche Wirkungen entfalten oder sie in ähnlicher Weise beeinträchtigen Angaben zu der verwendeten Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung;
- bei internationalen Datentransfers: falls notwendig, die Grundlagen der geeigneten Garantien.

30. Muss ich beim Auskunftsrecht alle E-Mails dem Anfragenden zusenden?

Ja. Eine Besonderheit gibt es dann, wenn z. B. eine Kopie in die Rechte anderer Personen eingreift (z. B. werden Namen anderer Personen genannt). Aus diesem Grund sollten Daten anderer betroffener Personen geschwärzt werden.

31. Welche Auswirkungen hat das "Recht auf Vergessenwerden" (Löschung) in der Praxis?

Das einzig wirklich neue beim Recht auf Vergessenwerden ist die Fristverkürzung von 8 Wochen auf 4 Wochen (verlängerbar um weitere 8 Wochen » siehe **EU-Datenschutz-Grundverordnung (DSGVO): Pflicht zur Berichtigung, Löschung ("Recht auf Vergessenwerden") und zur Einschränkung der Verarbeitung**).

Wenn Sie Daten löschen müssen (Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig,

Einwilligung wurde widerrufen, ein Widerspruch wurde eingelegt, Daten wurden generell unrechtmäßig verarbeitet), müssen diese vollständig gelöscht werden (ein Verschieben oder das Einschränken des Zugriffs reicht nicht aus).

32. Muss ich personenbezogene Daten löschen oder reicht die Einschränkung der Datenverarbeitung?

Wenn ein Löschungsanspruch besteht (siehe oben), dann sind die Daten faktisch zu löschen. Eine Einschränkung reicht nicht aus.

33. Was passiert, wenn ein Kunde seine Löschung beantragt, aber der Datensatz aufgrund der Aufbewahrungspflicht 7 Jahre aufbewahrt werden muss (z. B. die Rechnung mit den Kundendaten)?

Bei der Geltendmachung des Löschungsrechts gibt es einige spezielle Ablehnungsgründe.

Der Anspruch darf daher abgelehnt werden, wenn die Verarbeitung erforderlich ist, z. B. zur Erfüllung einer rechtlichen Verpflichtung, welche die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, notwendig macht.

So kann z. B. die steuerrechtliche Aufbewahrungspflicht nach § 132 Abs 1 BAO geltend gemacht werden: 7 Jahre (darüberhinausgehend solange sie für die Abgabenbehörde in einem anhängigen Verfahren von Bedeutung sind).

Dies muss der betroffenen Person jedoch auch begründet mitgeteilt werden.

34. Wie lange dürfen Daten gespeichert werden?

Zwei hier relevante Grundsätze der DSGVO lauten:

- **Richtigkeit:**
  Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden
- **Speicherbegrenzung:**
  Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

Daneben gibt es noch gesetzliche **Aufbewahrungspflichten** z. B. steuerrechtlich nach § 132 Abs 1 BAO: 7 Jahre (darüberhinausgehend solange sie für die Abgabenbehörde in einem anhängigen Verfahren von Bedeutung sind) wonach selbst eine beantragte Löschung der betroffenen Person innerhalb dieses Zeitraumes abgelehnt werden kann. Dies muss der betroffenen Person jedoch auch begründet mitgeteilt werden.

35. Wie lange darf ich Daten von Interessenten aufbewahren?

Solange die Datenverarbeitung den Grundsätzen der DSGVO entspricht bzw. gesetzliche Aufbewahrungspflichten zutreffen. D.h. Wie lange benötigen Sie die Daten tatsächlich? Gibt es regelmäßigen Kontakt (Zusendung von Werbematerial z. B.)?

Es gibt hier keine gesetzliche Frist. In der Standard- und Musterverordnung ist bei Kundendatenbanken immerhin 3 Jahre ab dem letzten Kundenkontakt als Speicherdauer ausgewiesen gewesen. Das kann man zumindest als eine Art Richtschnur heranziehen.

36. Wie können Daten aus Backups oder Datensicherungen gelöscht werden?

BackUps werden nicht gesondert in der DSGVO behandelt, weswegen auch "alte" Daten gelöscht werden müssen. Aber auch hier ist auf die Grundsätze der DSGVO zu achten. Das bedeutet, dass zumindest beim nächsten Backup die nicht mehr rechtmäßig bzw den Grundsätzen widersprechende verarbeitete Daten jedenfalls nicht mehr gesichert werden dürfen.

Aber selbst bei einem Jahresbackup werden Daten ja gelöscht bzw überschrieben. Daher sollte vor jedem Backup Augenmerk daraufgelegt werden, dass auch nur richtige und notwendige Daten gesichert werden. Denn spätestens mit der ersten technischen bzw. betriebswirtschaftlichen Möglichkeit müssen auch Daten aus Backups entfernt werden.

37. Muss nachgewiesen werden, dass ein Datensatz gelöscht wurde?

Der betroffenen Person gegenüber wird es wahrscheinlich reichen, die Löschung zu bestätigen. Die Datenschutzbehörde kann unter Umständen sogar

die Verarbeitung vor Ort überprüfen.

Bei einer Kontrolle durch die Datenschutzbehörde wird wohl nachgewiesen werden müssen, welchen Ablauf es bei einer Löschung gibt.

Unter Umständen wird die Datenschutzbehörde diesen Ablauf auch kontrollieren und so feststellen, ob Datensätze tatsächlich gelöscht werden. Gegenüber der betroffenen Person muss bestätigt werden, dass die Daten gelöscht sind.

38. In welchem Zeitrahmen muss ich auf Anfragen von betroffenen Personen (z. B. auf Auskunft, auf Löschung, ...) reagieren?

Der Verantwortliche hat den Antrag **unverzüglich** zu erledigen und zu beantworten, in jedem Fall aber binnen eines Monats ab Eingang. Ist die Erledigung des Antrages komplex und liegen mehrfache Anträge der gleichen Person vor, kann die Frist um zwei weitere Monate verlängert werden. Der Verantwortliche muss dies der betroffenen Person unter Angabe von Gründen mitteilen. Wurde der Antrag elektronisch eingebracht, soll auch diese Mitteilung elektronisch übersandt werden (sofern die betroffene Person dem nicht zuvor widersprochen hat). Lehnt der Verantwortliche den Antrag ab, hat er dies der betroffenen Person binnen eines Monats mitzuteilen.

39. Gibt es Ausnahmen, um nicht auf Anfragen von betroffenen Personen reagieren zu müssen?

Offenkundig unbegründete oder – insbesondere im Fall von häufiger Wiederholung – exzessive Anträge einer betroffenen Person kann der Verantwortliche entweder ablehnen oder ein angemessenes Entgelt verlangen. Ein gänzliches Ignorieren von Betroffenenanträgen ist nicht vorgesehen.

Bei der Geltendmachung des **Löschungsrechts** kommen noch einige spezielle Ablehnungsgründe hinzu. Der Anspruch darf daher abgelehnt werden, wenn die Verarbeitung erforderlich ist:

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, welche die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, notwendig macht;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke;
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Kann die Berichtigung oder Löschung der Daten nicht unverzüglich erfolgen, weil dies aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so kann der Auftraggeber die Erledigung dieses Antrages bis zu diesem Zeitpunkt aufschieben und ist die Verarbeitung der Daten einzuschränken.

40. Kann ich ein Entgelt für solche Anfragen verlangen?

Grundsätzlich nein. Ein angemessenes Entgelt kann nur bei offenkundig unbegründeten oder insbesondere wegen ihrer Häufigkeit exzessiven Anträgen verlangt werden.

41. Muss ich mir jetzt für jede Datenverarbeitung eine Einwilligung holen?

Nein, die Einwilligung ist nur eine Grundlage von mehreren. Wenn Sie nur die Daten verarbeiten, die Sie zur Vertragserfüllung benötigen (Rechnungsadresse und Name für Rechnungslegung), brauchen Sie keine Einwilligung.

Weitere Grundlagen wären rechtliche Vorschriften (z. B. Sie müssen die Daten Ihrer Mitarbeiter bei der GKK melden), lebensnotwendige Interesse (z. B. Sie führen Erste-Hilfe-Maßnahmen bei einem kollabierten Mitarbeiter durch und geben Gesundheitsdaten an die Sanitäter weiter), Erfüllung von Aufgaben im öffentlichen Interesse (z. B. Beliehene Rechtsträger) oder das berechtigte Interesse (z. B. Verarbeitung von Name und Adresse zur Zusendung einer postalischen Werbung des eigenen Unternehmens).

42. Wenn ich eine Einwilligung brauche, wie schaut die aus?

Eine "schlichte" Einwilligung kann elektronisch, mündlich, schriftlich oder sogar konkludent abgeschlossen werden. Aus Beweisgründen empfiehlt sich natürlich eine schriftliche.

Beispielsweise so: *„Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich ... (die Datenarten genau aufzählen, z.B. „Name“, „Adresse“ etc.) zum Zweck der ... (genaue Zweckangabe, z.B. „zur Zusendung von Werbematerial über die Produkte der Firma ...“) bei der Firma NN verarbeitet werden und die Daten ... (die Datenarten genau aufzählen, z.B. „Name“, „Adresse“ etc.) zum Zweck der ... (genaue Zweckangabe, z.B. „zur zentralen Abwicklung des Kunden-Beschwerdemanagements“) an ... (genaue Angabe des Übermittlungsempfängers, z.B. Name der Konzernmutter mit Anschrift) weitergegeben werden. Diese Einwilligung kann jederzeit bei ... (Angabe der entsprechenden Kontaktdaten) widerrufen werden.*“

Muster gibt es hier: **EU-Datenschutz-Grundverordnung (DSGVO): Einwilligungserklärung**.

43. Müssen bestehende Kunden erneut einwilligen, kontaktiert werden zu dürfen?

Wenn die bestehenden Einwilligungen den Vorgaben der DSGVO bereits entsprechen, müssen keine neuen Einwilligungen eingeholt werden.

Hier ist insbesondere auf die Belehrung über die jederzeitige Widerrufsmöglichkeit der Einwilligung zu achten.

Prüfen Sie sorgfältig, ob Sie überhaupt eine Einwilligung benötigen, oder Ihre Datenverarbeitung auf eine andere Rechtsgrundlage stützen können.

44. Ist bei Kindern etwas speziell zu beachten?

Bei Angeboten von Diensten der Informationsgesellschaft (z. B. Webshop), die einem Kind direkt gemacht werden, ist eine Datenverarbeitung personenbezogener Daten von Kindern vor Vollendung des 14. Lebensjahres nur dann rechtmäßig, wenn die Einwilligung zur Datenverarbeitung durch Obsorgeberechtigte (va Eltern), für das Kind oder mit deren Zustimmung erteilt wurde.

45. Wie kann ich sensible Daten verarbeiten?

Hier ist eine spezielle Grundlage nötig, wie

- ausdrückliche Einwilligung (konkludent oder schlüssig ist nicht möglich),
- arbeits- oder sozialrechtliche Verpflichtungen,
- für Zwecke der Gesundheitsvorsorge oder Arbeitsmedizin,
- gesetzliche Verpflichtung,
- Schutz lebensnotwendiger Interessen,
- von der Person selbst veröffentlichte Daten,
- Verarbeitung zur Geltendmachung / Ausübung / Verteidigung von Rechtsansprüchen,
- Verarbeitung durch politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht.

46. Wie identifiziere ich die Person?

Nach der DSGVO muss sich die betroffene Person nur dann identifizieren, wenn der Verantwortliche begründete Zweifel an seiner Identität hat (z. B. telefonische Anfrage oder über eine Fantasiemailadresse).

In diesem Fall kann der Verantwortliche zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. Sollte eine Anfrage z. B. von Max.Muster@domain.at kommen und nicht elektronisch signiert sein, wäre es ratsam, z. B. eine Ausweiskopie zu verlangen.

47. Was genau bedeutet Profiling und was ist zu beachten?

Profiling ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte einer Person zu bewerten (z. B. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel).

Profiling per se ist noch nicht problematisch, es muss sich so wie jede anderen Datenverarbeitung auf einen Erlaubnistatbestand stützen (z. B. berechtigtes Interesse bei einem „normalen" Kundenprofil) und die Datenschutzgrundsätze einhalten.

Profiling unterliegt dann besonderen Bestimmungen, wenn vollautomatisierte Entscheidungen im Einzelfall darauf beruhen, und der betroffenen Person gegenüber rechtliche Wirkungen entfalten (z. B. Automatische Vertragsbeendigung bei Inanspruchnahme einer Versicherungsleistung) oder sie ähnlicher Weise erheblich zu beeinträchtigen.

Bei dieser Form des Profilings muss eine spezielle Rechtsgrundlage vorliegen (Vertragsnotwendigkeit, Einwilligung, gesetzliche Vorschrift), die betroffene Person muss darüber informiert werden und sie hat dagegen u.U. ein Widerspruchsrecht.

48. Wie ist das Verarbeitungsverzeichnis?

Das **Verarbeitungsverzeichnis** ist ein Protokoll aller datenschutzrelevanter Vorgänge im Betrieb. Es 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.

49. 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 unter EU-Datenschutz-Grundverordnung (DSGVO): **Muster-Verarbeitungsverzeichnis für Auftragsverarbeiter**.

50. Müssen einzelne Aktivitäten, z. B. Mail an XY am 1.1.2001 aufgezeichnet werden?

Nein, das Verarbeitungsverzeichnis soll einen allgemeinen Überblick über die im Unternehmen vorhandenen Datenverarbeitungen bieten. Hierfür ist der Verarbeitungszweck (z. B. 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.

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.

51. Eine Ausnahme von der Verzeichnisführung besteht für KMU mit weniger als 250 Mitarbeitern, wenn "die Verarbeitung nur gelegentlich erfolgt und kein Risiko damit verbunden ist". Was fällt darunter?

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.

Naturgemäß birgt 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. 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.

52. 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.

53. Gibt es für das Verarbeitungsverzeichnis 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 Excel Dokument oder sogar handschriftlich verfassen.

54. 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.

55. Was bedeutet "ausdrückliche Zustimmung"? Muss das schriftlich erfolgen und mit Unterschrift bestätigt werden?

Die Zustimmungserklärung kann in jeder erdenklichen Form erfolgen, jedoch empfiehlt sich eine schriftliche, da die Zustimmung im Zweifelsfall zu beweisen ist. Ausdrücklich bedeutet, dass keine schlüssige Erklärung möglich ist.

56. Ist es möglich eine Zustimmung von Kunden über Social Media einzuholen oder über AGB?

Die Einwilligung/ Zustimmung kann auf jede mögliche Art eingeholt werden. Zu beachten ist, dass sich aus Gründen der Beweisbarkeit natürlich eine schriftliche Zustimmung empfiehlt.

Lediglich in den AGB darauf hinzuweisen, ist jedoch nicht ausreichend, da es nicht transparent genug ist. Zudem stellt sich die Frage, ob Einwilligungen in AGB überhaupt noch zweckmäßig sind.

Einwilligungserklärungen in AGB zu verpacken war auch bislang schon schwierig bzw. riskant, da argumentiert werden konnte, dass die Einwilligung dort "versteckt" wurde, d.h. nicht transparent genug ist.

Empfehlenswerter wäre, hier eine konkrete Einwilligung für diesen konkreten Zweck mit einer eigenen Unterschrift (mit einem eigenständigen Abhaken einer Checkbox im Onlinekontext) einzuholen.

57. Müssen alle vorhandenen Kunden, die in Stammkundendatei bereits gespeichert sind, eine Einwilligungserklärung zugesendet oder vorgelegt werden? Wie muss man da vorgehen?

Wenn die Kunden bereits eine Einwilligung zur Datenverarbeitung abgegeben haben, die den jetzigen Voraussetzungen im Datenschutzrecht entsprochen haben, dann gelten diese auch nach dem 25.5.2018 weiter ("Ich stimme zu, dass folgende meiner persönlichen Daten, nämlich ... (die Datenarten genau aufzählen, z. B. "Name, Adresse, ...") zum Zweck der ... (genaue Zweckangabe) verarbeitet werden. Diese Zustimmung kann jederzeit ohne Angabe von Gründen unter ... widerrufen werden.").

58. Wenn man z. B. Stammdaten von Kunden erhebt, inwiefern muss man dessen Einverständnis dokumentieren/beweisen können?

Sollte sich ein Kunde an ein Unternehmen wenden und verlangen, sein Einverständnis zu belegen, so empfiehlt sich eine schriftliche Einverständniserklärung.

Auch für den Fall, dass sich der Kunde an die Datenschutzbehörde wendet, ist eine schriftliche Einverständniserklärung von Vorteil.

59. Wann brauche ich einen Datenschutzbeauftragten?

Wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (z. B. Banken, Versicherungen) oder die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung sensibler Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht (z. B. Krankenanstalten).

60. Dürfen IT-Leiter, Personalleiter u. Ä. zum Datenschutzbeauftragten bestellt sein?

Grundsätzlich darf sich jeder mit Datenschutz befassen. Zum Datenschutzbeauftragten dürfen allerdings keine Personen ernannt werden, die eine Funktion haben, die mit den Aufgaben als Datenschutzbeauftragter kollidieren, wie etwa Leiter der IT-Abteilung oder der Rechtsabteilung.

61. Kann ich als EPU mein eigener Datenschutzbeauftragter sein?

Nein, da Sie als Geschäftsinhaber das Kriterium der Unabhängigkeit des Datenschutzbeauftragten nicht erfüllen würden.

62. Was ist die Funktion und vor allem die Haftung des Datenschutzbeauftragten?

Der Datenschutzbeauftragte unterrichtet und berät den Verantwortlichen hinsichtlich dessen Pflichten nach der DSGVO und sonstigen Datenschutzvorschriften.

Er überwacht die Einhaltung der DSGVO und anderer Datenschutzvorschriften, berät im Zusammenhang mit der Datenschutzfolgeabschätzung und ist

das Bindeglied zur Aufsichtsbehörde.

Der Datenschutzbeauftragte haftet lediglich nach den allgemeinen Regeln, nicht aber gegenüber der Behörde für die Strafen.

63. Braucht ein Datenschutzbeauftragter eine verpflichtende Ausbildung und/oder Zertifikat, oder kann man sich das Wissen dazu auch selbstständig aneignen als IT-Dienstleister?

Ein Datenschutzbeauftragter muss ein gewisses Maß an Erfahrung in datenschutzrechtlichen Dingen aufweisen. Konkrete Ausbildungen sind zwar nicht verpflichtend, aber doch empfehlenswert.

64. Haftet der Datenschutzbeauftragte zukünftig wirklich persönlich für Verfehlungen?

Eine Bestellung des Datenschutzbeauftragten zu einem Verantwortlichen nach § 9 VStG ist nicht zulässig.

Der Datenschutzbeauftragte haftet daher nur nach den allgemeinen zivilrechtlichen und allenfalls arbeitsrechtlich relevanten Regeln.

65. Wer kontrolliert Datenschutz? Werden z. B. stichprobenartige Kontrollen gemacht oder wird nur dann nachgefragt/kontrolliert, wenn sich jemand dezidiert beschwert?

Die Datenschutzbehörde kontrolliert eigenständig. Einer Kontrolle muss keine Beschwerde vorangehen.

Bei elektronischen Nachrichten bzw. Anrufen zu Werbezwecken ist das Fernmeldebüro zuständig (vgl. **https://www.bmvit.gv.at/ofb/organisation/nachgeordnet/fmb/index.html**).

66. Welche Strafen sind vorgesehen?

Geldbußen (Verwaltungsstrafe) bis zu 20 Millionen Euro oder 4 % des Konzernumsatzes des vorangegangenen Geschäftsjahres wären möglich, je nachdem, was höher ist.

Diese Strafen stellen Höchststrafen dar. Mindeststrafen sind nicht vorgesehen und prinzipiell kann die Behörde auch bei minderem Grad von Fahrlässigkeit Verwarnungen aussprechen.

67. Können die Strafen höher als der Unternehmensumsatz sein?

Ja, nach dem Verordnungswortlaut ist dies nicht ausgeschlossen.

68. Darf ich gesammelte Daten an Werbepartner weitergeben?

Grundsätzlich werden Sie dafür eine **Einwilligung** benötigen. Für Adressverlage und Direktmarketingunternehmen gelten spezielle Regelungen » siehe **Datenschutz und Direktmarketing**.

69. Was ist ein Datenleck, eine Datenpanne bzw ein data breach?

Wenn die Daten abhandenkommen, verloren gehen, beschädigt werden, angegriffen werden, gestohlen werden, etc.

Datenlecks sind zu melden, sofern ein Risiko für die betroffenen Daten und Personen besteht (z. B. Firmenlaptop wurde im Zug vergessen, Kundendaten sind unverschlüsselt, somit frei zugänglich auf dem Laptop).

Wenn sogar ein hohes Risiko für betroffene Personen besteht (z. B. sind nicht nur "normale" Kundendaten enthalten, sondern auch sensible), sind auch die Betroffenen direkt zu informieren.

70. Muss ich in Zukunft verschlüsseln?

Verschlüsselung bzw. Pseudonymisierung ist in der DSGVO als Datensicherheitsmaßnahme angesprochen.

Grundsätzlich kann aber auch ein Passwortschutz schon eine Verschlüsselungsmaßnahme darstellen.

Es ist nicht vorgeschrieben, E-Mails in Zukunft standardisiert verschlüsseln zu müssen, allerdings sollte man sich sehr wohl überlegen, ob man sensible Daten oder Betriebsgeheimnisse tatsächlich mit E-Mail verschickt, da das ähnlich zu sehen ist, wie wenn man Informationen per Postkarte verschickt.

71. Was bedeutet ausreichend Schutz?

Das richtet sich immer nach dem konkreten Einzelfall, nach dem Stand der Technik und Ihren finanziellen Möglichkeiten.

Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter **www.it-safe.at** verschaffen. Informationen dazu finden Sie im **IT-Sicherheitshandbuch für KMU**.

72. Was bedeutet Privacy by design für den Betrieb?

Privacy by design bedeutet grundsätzlich "Datenschutz durch Technikgestaltung".

Im 08 15 Ottonormalunternehmen wird das Prinzip kaum eine Rolle spielen, sondern trifft hauptsächlich Industrie-, bzw. IT-Unternehmen, welche Technik produzieren und wo Datenschutz eben bereits ab der ersten Planungsphase berücksichtigt werden muss.

Für "Standard"-Betriebe wird dies eher in Richtung Datensicherheit eine Rolle spielen – wie sicher sind die Daten im Betrieb, welche Systeme verwenden Sie, gibt es Möglichkeiten, die Systeme sicherer auszugestalten etc.

73. Was bedeutet Privacy by default für den Betrieb?

Privacy by default bedeutet Datenschutz durch entsprechende Voreinstellungen.

Software z. B. muss so voreingestellt sein, dass sie prinzipiell den größten Schutz bzw die maximale Privatsphäre gewährleistet. Das kann z. B. auch für Personalverwaltungssysteme oder andere interne Applikationen relevant sein.

74. Darf mein Steuerberater meinen Steuerakt überhaupt noch per E-Mail versenden?

E-Mails müssen auf Basis der DSGVO nicht zwingend verschlüsselt versendet werden. Unverschlüsselte E-Mails bieten aber keine Datensicherheit und können von Unbefugten leicht "mitgelesen" werden.

Anzuraten ist daher die Verschlüsselung bei der Handhabe mit heiklen Daten wie Bankverbindungen, Kreditkartendaten usw., aber natürlich auch bei der Handhabe mit sensiblen oder strafrechtlich relevanten Daten.

75. Darf ich weiterhin Clouds verwenden?

Ja, Clouddienstleistungen wurden durch die DSGVO nicht verboten. Sie sollten allerdings bedenken, dass es sich bei dieser Dienstleistung um eine Auftragsverarbeitung handelt, d.h. es ist

1. ein schriftlicher Auftragsverarbeitervertrag zu schließen,
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).

Bei der Weitergabe von Daten an einen Auftragsverarbeiter innerhalb der EU kann grundsätzlich mit einem berechtigten Interesse argumentiert werden. Außerhalb der EU wären die Grundsätze des internationalen Datenverkehrs einzuhalten: **EU-Datenschutz-Grundverordnung und Internationaler Datenverkehr** (z. B. ausdrückliche Einwilligung, Angemessenheitsentscheidung,...).

76. Was ist mit mobilen Applikationen?

Hier ist darauf zu achten, dass diese oftmals auf Ihre Daten am Endgerät zugreifen. Die Frage ist natürlich, ob das wirklich notwendig ist und ob Sie hier mit einem berechtigten Interesse (siehe oben) argumentieren können.

Weiters ist darauf zu achten, dass die Daten, auf die zugegriffen wird, weitergegeben werden, d.h. Sicherheitsmaßnahmen sind definitiv relevant. Wenn Sie sich nicht sicher sind, wie sicher Ihre App ist, sollten Sie sich fragen: Brauchen Sie die App oder gibt es vielleicht andere, sicherere Alternativen?

Achtung:
Die WKO kann keine spezifischen Apps empfehlen, genauso wenig wie pauschal verurteilen. Wichtig ist daher, sich die AGB und Datenschutzbestimmungen der App anzusehen und zu prüfen, ob auf Daten zugegriffen wird, wenn ja, wo die Daten hin bewegt werden (EU, nicht EU) und ob der jeweilige Anbieter zuverlässig ist. Wenn Sie darüber zweifeln, dann sollte die jeweilige App im Zweifel eben nicht herunter geladen werden.

77. Wie muss ich Daten sichern, die in Papierform festgehalten werden?

Versperrbare Schränke, Zutrittsberechtigungen, Zugriffsberechtigungen etc. wären hier anzudenken. Denken Sie dabei auch im eigenen Interesse an Datensicherung und daran, diese räumlich getrennt (z. B. zur Vorsorge bei Feuer) aufzubewahren.

Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter **www.it-safe.at** verschaffen.

78. Wie müssen Mitarbeiter belehrt werden?

Am besten so, dass diese über die Basics im Datenschutz wissen (z. B. wenn ein Kunde ins Geschäft kommt und wissen möchte, welche Daten das Unternehmen über ihn hat, sollte nach dem Ausweis gefragt werden und die Angelegenheit an den Verantwortlichen weiter getragen werden). Am wichtigsten ist, dass die Mitarbeiter eine gewisses Bewusstsein bzgl. Datenschutz bekommen, d.h. erkennen, wenn etwas datenschutzrelevant wird und wissen, wohin sie sich bei datenschutzrechtlichen Fragen wenden können (meistens direkt an den Geschäftsführer / Datenschutzbeauftragten,...). Auch die gängigsten Fehler und Sicherheitslücken sollten bekannt sein » siehe auch: **IT-Sicherheitshandbuch für Mitarbeiter**.

79. Datenschutz-Anpassungsgesetz 2018 (DSAG 2018) - Welche Regelungen enthält das Gesetz?

Nur noch wenige, z. B. zum Datengeheimnis für Mitarbeiter und Subunternehmer, zur Bildverarbeitung (vormals Videoüberwachung), vgl. auch: **Das Datenschutz-Anpassungsgesetz 2018**.

Allerdings sind Erleichterungen enthalten, wie der Vorrang der Bestrafung der juristischen Person, Ermahnungsmöglichkeiten bevor eine Strafe verhängt wird und Datenverarbeitungsmöglichkeiten für strafrechtlich relevante Daten.

80. Unter welchen Voraussetzungen ist künftig Videoüberwachung zulässig?

Wenn die (nunmehr) "Bildverarbeitung" im lebenswichtigen Interesse einer Person ist, die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat, sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.

Jedenfalls erlaubt ist sie, wenn sie dem vorbeugenden Schutz von Personen oder Sachen auf privaten Liegenschaften, die ausschließlich vom Verantwortlichen genutzt werden, dient, und räumlich nicht über die Liegenschaft hinausreicht, mit Ausnahme einer zur Zweckerreichung allenfalls unvermeidbaren Einbeziehung öffentlicher Verkehrsflächen, sie für den vorbeugenden Schutz von Personen oder Sachen an öffentlich zugänglichen Orten, die dem Hausrecht des Verantwortlichen unterliegen, aufgrund bereits erfolgter Rechtsverletzungen oder eines in der Natur des Ortes liegenden besonderen Gefährdungspotenzials erforderlich ist und kein gelinderes geeignetes Mittel zur Verfügung steht, oder sie ein privates Dokumentationsinteresse verfolgt, das nicht auf die identifizierende Erfassung unbeteiligter Personen oder die gezielte Erfassung von Objekten, die sich zur mittelbaren Identifizierung solcher Personen eignen, gerichtet ist.

81. Besteht die Pflicht zur Kennzeichnung bei der Verwendung von Videokameras?

Nach § 13 Abs 5 DSG (neu) ist eine Videoüberwachungsanlage (jetzt Bildverarbeitung genannt) entsprechend zu kennzeichnen.

Aus der Kennzeichnung hat jedenfalls der Verantwortliche eindeutig hervorzugehen, es sei denn, dieser ist den betroffenen Personen nach den Umständen des Falles bereits bekannt.

82. Dürfen Daten zu statistischen Zwecken weiterhin ausgewertet werden?

Die DSGVO sieht eine privilegierte Stellung von wissenschaftlicher und historischer Forschung, Statistik und Archiven im öffentlichen Interesse bei der Verarbeitung personenbezogener Daten als gerechtfertigt an.

Das Datenschutzgesetz i.d.F. des Datenschutz-Anpassungsgesetzes 2018 schafft daher in einer Sonderbestimmung Erleichterungen für die Zulässigkeit derartiger Datenverarbeitungen, die aber nur gelten, sofern nicht spezielle gesetzliche Regelungen (wie etwa das Bundesstatistikgesetz) bestehen » siehe hierzu: **Datenverarbeitung zu Archivzwecken, wissenschaftlichen Forschungszwecken sowie zu statistischen Zwecke**.

83. Dürfen Strafregisterauszüge verarbeitet werden?

Es kommt darauf an.

Die Verarbeitung von personenbezogenen Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen ist unter Einhaltung der Vorgaben der DSGVO und des DSAG zulässig, wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder die Datenverarbeitung aufgrund eines berechtigten Interesses erforderlich ist und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und dem DSAG gewährleistet.

84. Darf ich nun keine Rechnungen mehr ausstellen, Daten der Bank weitergeben, Überweisungen tätigen, usw?

Doch, natürlich. Die DSGVO verhindert keine Tätigkeiten, sie gibt nur den Rahmen vor. D.h. in diesen Fällen werden personenbezogene Daten verarbeitet, d.h. die Verarbeitungsvorgänge müssen im **Verarbeitungsverzeichnis** erfasst werden und müssen die betroffenen Personen darüber **informiert** werden.

85. Sind Whistleblower-Hotlines 2018 noch zulässig?

Ja, das Datenschutz-Anpassungsgesetz hat eine weitergehende Verarbeitung strafrechtlich relevanter Daten vorgesehen. Alle übrigen Voraussetzungen (Rechtsgrundlage, etwaig Betriebsvereinbarung) sind weiterhin natürlich zu erfüllen.

86. Ist der 25.5.2018 fix oder gibt es noch Übergangsfristen, innerhalb deren nicht gestraft wird?

Das Datum ist fix und kann nicht mehr verschoben werden.

87. Darf ich noch weiterhin Newsletter verschicken?

Newsletter, also elektronische Nachrichten zu Werbezwecke, dürfen nach wie vor nur unter den sehr strengen Bedingungen des Telekommunikationsgesetzes versendet werden (vgl. auch **E-Mails**). Entweder, die Zusendung von E-Mails erfolgt mit Einwilligung des Empfängers oder:

- die E-Mail-Adresse des Kunden wird beim Verkauf einer Ware oder einer Dienstleistung erhoben; und
- der Kunde erhält bei Erhebung der E-Mail-Adresse die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen; und
- der Kunde erhält bei jeder Zusendung die Möglichkeit, den Empfang kostenfrei und problemlos abzulehnen; und
- die Zusendung erfolgt zur Direktwerbung für eigene, ähnliche Produkte; und
- der Kunde ist nicht in die sog „ECG-Liste" eingetragen.

> **Achtung:**
> Das Versenden eines Newsletters muss trotzdem in das Verarbeitungsverzeichnis aufgenommen werden (Marketing für eigene Zwecke, Kundenbetreuung, Kundendatenbank, ...) und muss der Empfänger über die Datenverarbeitung informiert werden.

88. Darf ich Unternehmen kontaktieren, deren Daten ich aus dem Internet (z. B. verpflichtenden Impressum) habe?

Nein. Für Anrufe zu Werbezwecke brauchen Sie die vorhergehende Einwilligung dazu. Ebenso bei der elektronischen Nachricht (SMS, Mail, Nachricht über Messengerdienste).

Bei letztere könnte aber im Rahmen einer aufrechten Kundenbeziehung Kontakt aufgenommen werden (vgl. Frage 20).

89. Was muss ich auf der Website umstellen?

Hier sind natürlich einerseits Webtracking-Tools relevant, an deren Zulässigkeit / Informationsverpflichtung / Einwilligungserfordernis sich durch die DSGVO nichts geändert hat » siehe **Checkliste für Cookies und Webanalyse im Webshop**.

Weiters wird die Datenschutzerklärung eine sehr große Rolle spielen, weshalb diese unbedingt ausführlich aktualisiert und ergänzt werden sollte.

90. Dürfen Daten aus öffentlichen Quellen ohne Einwilligung der Betroffenen verwendet werden?

Voraussichtlich ja, aufgrund eines berechtigten Interesses iSd Art 6 Abs 1 lit f DSGVO.

> **Achtung:**
> Über die Datenverwendung (= Verarbeitung) muss die betroffene Person wiederum informiert werden » siehe **EU-Datenschutz-Grundverordnung (DSGVO): Informationspflichten**.

91. Was sind die wichtigsten Basics, die wirklich jedes Unternehmen haben muss?

Jedes Unternehmen wird um die Bestandsanalyse, eine Art „Dateninventur" aller relevanter datenschutzrechtlichen Vorgänge im Unternehmen nicht herumkommen. Das kann man auch nutzen, um sich einen Überblick zu verschaffen, zu eruieren, ob man Einsparungspotential hat uÄ. Jedes Unternehmen braucht jedenfalls ein Verarbeitungsverzeichnis und eine ordentliche vollständige Datenschutzerklärung. Und jedes Unternehmen muss in Zukunft Datenschutz ernst nehmen.

92. Wenn ich meinen Unternehmenssitz ins Ausland verlege, bin ich dann auch aus der DSGVO raus?

Nein. Der Anwendungsbereich ist so weit gefasst, dass auch Unternehmen mit Sitz in Drittstaaten, die sich auf die EU ausrichten und personenbezogene Daten europäischer Staatsbürger verarbeiten, sich an die Grundsätze der DSGVO halten müssen.

93. Das klingt alles irrsinnig aufwändig.

Mehr eine Aussage als eine Frage, aber natürlich eine wichtige Anmerkung.

Ja – die Bestandsanalyse ist aufwändig. Ja – Das Verzeichnis zu erstellen und die Informationspflichten vollständig zu erfüllen, wird aufwändig.

Aber es handelt sich hier einmal um einen Einmalaufwand. All diese Dinge sind nach dem 25.5.2018 zwar grundsätzlich ajour zu halten, aber es wird einfacher fallen.

Das Problem ist, dass viele dieser Dinge bereits hätten erfüllt werden müssen, da auch das österreichische DSG 2000 schon sehr strenge Regelungen vorgesehen hat.

94. Brauche ich einen externen Berater oder schaffe ich das alles allein?

Mit den Inhalten auf **www.wko.at/datenschutz** und den jeweiligen Musterdokumenten schaffen Sie die Umstellung sicher!

Wenn Sie trotzdem jemand Externes damit betrauen wollen/müssen, können Sie als KMU Förderungen über **www.kmudigital.at** in Anspruch nehmen.

95. Wo gibt es weitere Infos?

Unter **www.wko.at/datenschutz** finden Sie alle unsere Inhalte.

Unter **www.wko.at/datenschutzservice** finden Sie zudem alle Inhalte der Fachorganisationen und Bundesländer.

www.it-safe.at enthält alles Wissenswerte zum Thema IT- und Datensicherheit

Stand: 23.04.2018