IT-Dienstleistung - Niederösterreich

EU-Datenschutz-Grundverordnung: FAQ für IT-Dienstleister

Antworten auf häufig gestellte Fragen

1. Wer zählt zu den Auftragsverarbeitern?

2. Was ist der Unterschied zwischen einem Auftragsverarbeiter und einem Empfänger?

3. Ist der IT-Betreuer/IT-Dienstleister automatisch Auftragsverarbeiter?

4. Muss für die Reparatur eines PCs/Laptops eines Kunden (auf dem personenbezogene Daten gespeichert sind) ein Auftragsverarbeitungsvertrag abgeschlossen werden?

5. Welche Pflichten habe ich nun als Auftragsverarbeiter zu erfüllen, um DSGVO-konform zu sein?

6. Wie kann ein Auftragsverarbeitungsvertrag abschlossen werden? Reicht es, wenn mein Kunde diesen online durch Anklicken bestätigt?

7. Wie sieht es aus, wenn wir Auftragsverarbeiter sind und unsere IT-Dienstleistungen an eine Partnerfirma auslagern?

8. Sind „Provider" Auftragsverarbeiter?

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

10. Muss ein Auftragsverarbeiter mehrere Verarbeitungsverzeichnisse führen?

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

12. Sind Online-Cloud Services (z.B. Dropbox, Google Drive) DSGVO-konform? Ist ein Backup der Daten online auf Microsoft OneDrive oder Dropbox zum Beispiel erlaubt?

13. Darf meine Firma ihre Kontaktdatenbank z.B. im Office 365, also bei Microsoft, speichern? Ist Microsoft damit Auftragsverarbeiter oder nicht? Brauchen wir eine spezielle DSGVO-Vereinbarung bzw. Bestätigung von Microsoft?

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 dabei DSGVO-Vorgaben missachtet werden, z.B. statt echter Löschung bloß Löschmarkierungen einsetzen sind, die Daten „auszublenden"? Inwieweit sind wir als Software-Entwickler dafür verantwortlich, dass unsere Kunden die DSGVO einzuhalten? Werden wir gegenüber dem Kunden ggfs. sogar schadenersatzpflichtig?

15. Muss ich einen Auftragsverarbeitungsvertrag mit z.B. meinem E-Mail-Versand-Unternehmen (Newsletter) abschließen?

16. Wenn meine Kundendaten bei einem externen Anbieter auf einem Server oder E-Mail-System gespeichert sind, inwieweit bin ich für die Einhaltung der DSGVO bei auftretenden Problemen haftbar?

17. Bei E-Mails werden fast immer auch personenbezogene Daten verarbeitet – wie sieht es hier mit Löschfristen aus?

18. Besteht für E-Mails nun die Pflicht, diese immer zu verschlüsseln?

19. Wir betreiben für unseren Kunden eine Website - was ist dabei datenschutzrechtlich zu beachten?

20. Was ist allgemein beim Thema Datensicherheit zu beachten?

21. Ein Laptop wurde gestohlen – sind nun die Datenschutzbehörde und alle Personen, über die Daten auf dem Laptop gespeichert sind, zu informieren, selbst wenn die Daten alle verschlüsselt sind oder auf einem externen Server gespeichert sind?

22. Wer ist beim Betrieb einer Website verantwortlich für die Datenschutzerklärung bzw. -hinweise (z.B. Cookie Hinweis). Der Unternehmer oder der Webdesigner?

23. Ist für den Einsatz von Cookies die Einwilligung der User notwendig? Wie muss ich die User vom Gebrauch der Cookies informieren?

24. Ist die (dynamische) IP-Adresse ein personenbezogenes Datum?

25. Sind anonymisierte Daten personenbezogene Daten?

26. Welche Tätigkeiten im Zusammenhang mit der DSGVO sind von dem Berechtigungsumfang der IT-Dienstleister umfasst? Kann ich Datenschutzbeauftragter gem. Art 37 DSGVO sein?

27. Welche Pflichten ergeben sich aus der DSGVO für den Betriebsrat? Ist der Betriebsrat ebenfalls für die Einhaltung des Datenschutzes verantwortlich?

1. Wer zählt zu den Auftragsverarbeitern?

Auftragsverarbeiter sind die verlängerten Arme der Verantwortlichen, d.h. sie verarbeiten Daten weisungsgebunden und vertraglich gebunden für jemand anderes. „Klassische" Auftragsverarbeiter sind z.B. Clouddienste-Anbieter, Newsletter-Tool-Betreiber oder Dienstleister für Sicherungs-Backups. Zwischen Verantwortlichem und Auftragsverarbeiter ist zwingend ein Auftragsverarbeitungsvertrag abzuschließen (Muster). Achtung: auch innerhalb eines Konzerns müssen gegebenenfalls Auftragsverarbeitungsverträge abgeschlossen werden.

2. Was ist der Unterschied zwischen einem Auftragsverarbeiter und einem Empfänger?

Empfänger ist jede vom Verantwortlichen und der betroffenen Person selbst verschiedene Person, d.h. jeder, dem ich Daten außerhalb des Unternehmens, abgesehen von der betroffenen Person selbst weitergebe. Auftragsverarbeiter sind also ebenfalls Empfänger.

3. Ist der IT-Betreuer/IT-Dienstleister automatisch Auftragsverarbeiter?

Wenn der IT-Betreuer als externer Dienstleister personenbezogene Daten für einen Verantwortlichen verarbeitet (Wartung, Support, etc.), dann ja. Zwischen Verantwortlichem und Auftragsverarbeiter ist dann zwingend ein Auftragsverarbeitungsvertrag abzuschließen (Muster). Beachten Sie, dass die Definition einer „Datenverarbeitung" sehr weit gefasst ist und im Grunde jeden Vorgang (oder jede Vorgangsreihe) im Zusammenhang mit personenbezogenen Daten umfasst.

Zum Beispiel bei 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 also vor, wenn bloß eine theoretische Möglichkeit zum Zugriff auf Daten besteht (empfohlen wird, den tatsächlichen Zugriff in diesem Fall auch vertraglich explizit auszuschließen). Eine Auftragsverarbeitung besteht insbesondere auch dann nicht, 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.). Achtung: auch innerhalb eines Konzerns müssen gegebenenfalls Auftragsverarbeitungsverträge abgeschlossen werden.

4. Muss für die Reparatur eines PCs/Laptops eines Kunden (auf dem personenbezogene Daten gespeichert sind) ein Auftragsverarbeitungsvertrag abgeschlossen werden?

Nur dann, wenn im Rahmen der Reparatur die Verarbeitung von personenbezogenen Daten erforderlich ist oder damit einhergeht. Keine Verarbeitung liegt vor, wenn bloß eine theoretische Möglichkeit zum Zugriff auf Daten besteht (empfohlen wird, den tatsächlichen Zugriff in diesem Fall auch vertraglich explizit auszuschließen). Eine Auftragsverarbeitung besteht insbesondere auch dann nicht, 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.).

5. Welche Pflichten habe ich nun als Auftragsverarbeiter zu erfüllen, um DSGVO-konform zu sein?

Alle Pflichten, die Sie als Auftragsverarbeiter erfüllen müssen, finden Sie hier. Zentral sind aber jedenfalls die Führung eines Verfahrensverzeichnisses, der Abschluss von Auftragsverarbeitungsverträgen und die Einhaltung der erforderlichen Datensicherheitsmaßnahmen.

6. Wie kann ein Auftragsverarbeitungsvertrag abschlossen werden? Reicht es, wenn mein Kunde diesen online durch Anklicken bestätigt?

Nach bisheriger Rechtslage war es so, dass Vereinbarungen zwischen einem Verantwortlichen und einem Auftragsverarbeiter schriftlich abzuschließen sind. Art 28 Abs. 9 DSGVO spricht nun im Gegensatz dazu davon, dass Auftragsverarbeitungsverträge „*schriftlich abzufassen [sind], was auch in einem elektronischen Format erfolgen kann*". Da die DSGVO jedoch keine Definition erhält, was konkret unter einem „*elektronischem Format*" zu verstehen ist, gehen die Meinungen diesbezüglich auseinander. Unter Umständen reicht aber sogar das Anklicken eines Bestätigungsfeldes.

Aus Beweisgründen wird davon abgeraten, einfache E-Mails für den Abschluss von Auftragsverarbeitungsverträgen zu verwenden. Um sicher zu gehen, sollte man dem Empfänger die Erklärung in einem dauerhaften Format übermitteln bzw. bereitstellen. Hier böte sich als Format etwa eine PDF-Datei an, da diese geeignet sein sollte, den Auftragsverarbeitungsvertrag unverändert wiederzugeben. Die Unterschrift einer zeichnungsberechtigten Person könnte hier als Scan aufgenommen werden.

7. Wie sieht es aus, wenn wir Auftragsverarbeiter sind und unsere IT-Dienstleistungen an eine Partnerfirma auslagern?

Wenn die Partnerfirma im Rahmen dieser Auslagerung personenbezogene Daten verarbeitet, ist sie als Sub-Auftragsverarbeiter zu qualifizieren. Sie sollte sich zuerst die Frage stellen, ob Sie überhaupt zur Heranziehung eines Sub-Auftragsverarbeiters berechtigt sind. Dies sollte in dem Auftragsverarbeitungsvertrag zwischen Ihnen und dem Verantwortlichen geregelt sein. Selbst wenn Sie grundsätzlich zur Auslagerung berechtigt sind, müssen Sie Ihren Kunden trotzdem jedenfalls über die Hinzuziehung oder Ersetzung eines Sub-Auftragsverarbeiters informieren. Außerdem müssen Sie mit Ihrer Partnerfirma ebenfalls einen Auftragsverarbeitungsvertrag abschließen, der diesem dieselben Datenschutzpflichten auferlegt, die Sie gegenüber Ihrem Kunden haben.

8. Sind „Provider" Auftragsverarbeiter?

Hier gilt es zu unterscheiden: Provider sind ausschließlich dann Auftragsverarbeiter, wenn sie personenbezogene Daten im Auftrag und auf Weisung für ihre Kunden verarbeiten (z.B. auf Daten zugreifen, Speicherung anbieten, etc.).

Access-Provider: Die reine Datendurchleitung entspricht üblicherweise keiner Datenverarbeitung ist. Manche Juristen vertreten eine solche aufgrund der Zwischenspeicherung beim Durchleiten, dies ist allerdings strittig.

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

Cloud-Dienstleister: Wenn im Rahmen eines Cloud-Services oder der Datensicherheitsmaßnahmen personenbezogene Daten verarbeitet werden, wird ein Auftragsverarbeitungsverhältnis begründet.

Mail-Provider: Ähnlich wie Host-Provider sind diese als Auftragsverarbeiter zu qualifizieren, wenn die Speicherung und der Zugang zu Daten angeboten werden.

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

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

Wird gemeinsam mit dem Verkauf der Software eine Datenwartung bzw. ein Support vereinbart, kann eine Auftragsverarbeitung vorliegen, wenn dafür die Verarbeitung von personenbezogenen Daten erforderlich ist oder damit einhergeht. Keine Verarbeitung liegt vor, wenn bloß eine theoretische Möglichkeit zum Zugriff auf Daten besteht (empfohlen wird, den tatsächlichen Zugriff in diesem Fall auch vertraglich explizit auszuschließen). Gleiches gilt auch bei IT-Dienstleistungen mittels Fernwartung (Remote Support, Screen Sharing, etc.).

10. 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 gegebenenfalls Auftragsverarbeiter für 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 und weniger detailliert als das für Verantwortliche. Ein Muster für Verantwortliche finden Sie hier, für Auftragsverarbeiter hier.

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

Jeder Verantwortliche ist grundsätzlich selbst verpflichtet, seine Datenverarbeitungen in einem Verarbeitungsverzeichnisses (Muster) zu dokumentieren und, sofern erforderlich, Datenschutz-Folgeabschätzungen durchzuführen (Informationen finden Sie hier). Als Auftragsverarbeiter müssen Sie den Verantwortlichen jedoch bei der Einhaltung dieser Pflichten unterstützen (z.B. Sicherheitsmaßnahmen implementieren, Risiken einschätzen), soweit Ihnen die dafür erforderlichen Informationen zur Verfügung stehen. Wie diese Unterstützung konkret aussieht, sollten Sie bestenfalls vertraglich regeln.

Die DSGVO definiert eine Reihe von Pflichten für Auftragsverarbeiter – primär muss ein Vertrag geschlossen werden (nähere Informationen finden Sie hier). Sie können und sollten sich nicht darauf verlassen, dass Ihre Kunden Sie aktiv auf alle gesetzlichen Pflichten hinweisen - Sie sind selbst für deren Einhaltung verantwortlich.

12. Sind Online-Cloud Services (z.B. Dropbox, Google Drive) DSGVO-konform? Ist ein Backup der Daten online auf Microsoft OneDrive oder Dropbox zum Beispiel erlaubt?

Die Nutzung „kostenloser" Speicherdienste sollte im Einzelfall immer genau geprüft werden. Auch abgesehen vom Datenschutzrecht, sollten Sie sich die Frage stellen, ob der gewählte Dienst vertrauensvoll mit Ihren Geschäfts- und Betriebsgeheimnissen umgeht. Cloud-Dienste sind nicht per se „sicher" oder „unsicher", diese Frage hängt immer von den konkreten Umständen ab.

Bitte beachten Sie, dass Cloud-Dienstleister als Auftragsverarbeiter zu qualifizieren sind, wenn sie personenbezogene Daten für einen Verantwortlichen verarbeiten, weshalb 1. ein schriftlicher Auftragsverarbeitungsvertrag abzuschließen ist (Muster), 2. auf die Zuverlässigkeit des Anbieters zu achten ist, 3. Datensicherheitsmaßnahmen einzuhalten sind, 4. betroffene Personen darüber aufzuklären sind und 5. darauf zu achten ist, wo Daten gespeichert werden (EU oder EU-Ausland). Bei einer Weitergabe von Daten an einen Auftragsverarbeiter außerhalb der EU sind die Bestimmungen des internationalen Datenverkehrs einzuhalten: EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr.

13. Darf meine Firma ihre Kontaktdatenbank z.B. im Office 365, also bei Microsoft, speichern? Ist Microsoft damit Auftragsverarbeiter oder nicht? Brauchen wir eine spezielle DSGVO-Vereinbarung bzw. Bestätigung von Microsoft?

Auch Microsoft ist Auftragsverarbeiter, wenn es personenbezogene Daten für seine Kunden verarbeitet (z.B. darauf Zugriff nehmen, Speicherung anbieten, etc.).

Bei Office 365 handelt es sich um eine Cloud-basierte Office-Lösung, bei der Microsoft tatsächlich als Auftragsverarbeiter tätig wird. Microsoft informiert auf seiner Website zu diesem Thema und weist auch aus, dass die Auftragsverarbeitungsverträge von den Volumenlizenzverträgen in den Online-Services-Nutzungsbedingungen umfasst sind. Der elektronische Abschluss dieses Vertrages ist wahrscheinlich ausreichend (dazu näher Frage 5). Weiters wurden Schritte gesetzt um die Datenweitergabe ins EU-Ausland rechtlich abzusichern (Standardvertragsklauseln, Eintragung in die „EU-US Privacy Shield"-Liste).

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 dabei DSGVO-Vorgaben missachtet werden, z.B. statt echter Löschung bloß Löschmarkierungen einsetzen sind, die Daten „auszublenden"? Inwieweit sind wir als Software-Entwickler dafür verantwortlich, dass unsere Kunden die DSGVO einzuhalten? Werden wir gegenüber dem Kunden ggfs. sogar schadenersatzpflichtig?

Schon nach allgemeinem Zivilrecht könnte Sie als professioneller Anbieter in diesem Fall eine Warnpflicht treffen. Gemäß DSGVO besteht für Auftragsverarbeiter jedenfalls die Pflicht, einen Verantwortlichen unverzüglich zu informieren, wenn man der Auffassung ist, dass eine von dem Verantwortlichen erteilte Weisung gegen die DSGVO (oder gegen andere Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten) verstößt. Eine entsprechende Aufklärung des Kunden, dass z.B. ein Löschkonzept notwendig ist, wird daher empfohlen.

15. Muss ich einen Auftragsverarbeitungsvertrag mit z.B. meinem E-Mail-Versand-Unternehmen (Newsletter) abschließen?

Ja, wenn Sie dem Unternehmen dabei personenbezogene E-Mail-Adressen und/oder andere personenbezogene Daten Ihrer Kunden überlassen.
» Weitere Informationen und Muster

16. Wenn meine Kundendaten bei einem externen Anbieter auf einem Server oder E-Mail-System 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, d.h. man könnte mitunter schadenersatzpflichtig werden, wenn bei der Erfüllung eines Vertrages ein Schaden entsteht.

17. Bei E-Mails werden fast immer auch personenbezogene Daten verarbeitet – wie sieht es hier mit Löschfristen aus?

Es gibt keine Sonderregelungen für E-Mails im Hinblick auf Löschfristen. Die zulässige Aufbewahrungsdauer richtet sich je nach Inhalt z.B. nach steuer- oder arbeitsrechtlichen Aufbewahrungspflichten.
» Weitere Informationen
» Eine Aufstellung zulässiger Speicherdauern

18. Besteht für E-Mails nun die Pflicht, diese immer zu verschlüsseln?

Die DSGVO gibt hier leider keine eindeutige Antwort, sondern spricht nur davon, dass „ein dem Risiko angemessenes Schutzniveau" gewährleistet werden muss. Eine Verschlüsselungspflicht besteht wohl jedenfalls, wenn besonders sensible Daten (Art 9 DSGVO - z.B. Daten bzgl. Gesundheit, politischer Meinung oder Religion) übermittelt werden. Die Verschlüsselung dient gleichzeitig als Zugriffs-, Transport- und Übermittlungskontrolle. Eine Alternative kann auch der Schutz von Dateianhängen mittels Passwort sein, z.B. passwortgeschützte PDFs der neuesten Generation. Das Passwort sollte aktuellen Kriterien für sichere Passwörter entsprechen und über einen separaten Kanal der entsprechend berechtigten Bezugsperson übermittelt werden.

19. Wir betreiben für unseren Kunden eine Website - was ist dabei datenschutzrechtlich zu beachten?

Wenn Sie beim Betreiben der Website personenbezogene Daten für Ihren Kunden verarbeiten, sind Sie als Auftragsverarbeiter zu qualifizieren. Maßgeblich ist dabei, ob die beauftragte Tätigkeit „im Zusammenhang mit personenbezogenen Daten" steht oder nicht. Keine Verarbeitung liegt vor, wenn bloß eine theoretische Möglichkeit zum Zugriff auf Daten besteht (empfohlen wird, den tatsächlichen Zugriff in diesem Fall auch vertraglich explizit auszuschließen).

Wenn Sie Auftragsverarbeiter sind, müssen Sie mit Ihrem Kunden (Verantwortlicher) zwingend einen Auftragsverarbeitungsvertrag abschließen (Muster).

Datenschutzrechtlich wichtig sind insbesondere die Informationspflichten, die von dem Verantwortliche zu erfüllen sind. Relevant ist dies etwa bei Webshops, Cookies oder Newslettern.

Sicherheit ist auch beim Betrieb einer Website wichtig, weshalb unbedingt eine SSL-Verschlüsselung verwendet werden sollte (vgl. auch IT-Sicherheitshandbuch, Seite 70f).

» Weitere allgemeine Datenschutzinformationen zu Websites und Webshops

20. Was ist allgemein beim Thema Datensicherheit zu beachten?

Die DSGVO macht bezüglich Datensicherheit keine konkreten Vorgaben, sondern gibt in Art. 32 DSGVO gewisse Richtlinien vor:

Demnach sind

- unter Berücksichtigung des Stands der Technik (was ist am Markt üblich?),
- der Implementierungskosten (was kann das Unternehmen finanziell leisten?) und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung (wie riskant ist die Datenverarbeitung?) sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit (wie wahrscheinlich ist der Fall eines Data Breaches?) und
- der Schwere des Risikos (wie schlimm könnte ein Data Breach ausfallen?) für natürliche Personen

geeignete technische und organisatorische Maßnahmen zu setzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
» Weitere Informationen zur IT- und Datensicherheit

21. Ein Laptop wurde gestohlen – sind nun die Datenschutzbehörde und alle Personen, über die Daten auf dem Laptop gespeichert sind, zu informieren, selbst wenn die Daten alle verschlüsselt sind oder auf einem externen Server gespeichert sind?

Hier stellt sich die Frage, ob ein sogenannter „Data Breach" vorliegt, also eine Verletzung des Schutzes von personenbezogenen Daten. Die Meldung eines solchen Data Breaches an die Behörde bzw. die betroffenen Personen ist dann nicht erforderlich, wenn etwa über eine Verschlüsselung bzw. externe Speicherung der Daten sichergestellt ist, dass trotz Diebstahl des Laptops kein Risiko (z.B. durch unberechtigten Zugriff) für die Rechte der Personen besteht.

22. Wer ist beim Betrieb einer Website verantwortlich für die Datenschutzerklärung bzw. -hinweise (z.B. Cookie Hinweis). Der Unternehmer oder der Webdesigner?

Der Unternehmer, für dessen Zwecke die Website betrieben wird, ist der datenschutzrechtlich Verantwortliche. Sie als Webdesigner sollten ihn jedoch dezidiert warnen, dass hier auch datenschutzrechtliche Belange abzuklären sind. Dazu näher auch Frage 13 und Frage 18.

23. Ist für den Einsatz von Cookies die Einwilligung der User notwendig? Wie muss ich die User vom Gebrauch der Cookies informieren?

Nach der geltenden EU-Richtlinie (e-Privacy-RL), die in Österreich mit § 96 Telekommunikations-Gesetz (TKG) umgesetzt wurde, ist das Abspeichern von Cookies auf dem Endgerät des Kunden, um Daten mit dem Computer des Kunden zu verknüpfen, oft nur dann zulässig, wenn die Einwilligung des Users eingeholt und der User entsprechend informiert wurde. Wenn eine Einwilligung erforderlich ist, muss diese jedenfalls durch ein aktives Verhalten der Nutzer erteilt werden. Unzulässig sind etwa bereits vorangekreuzte Einwilligungskästchen, die der Nutzer erst anklicken muss, um nicht einzuwilligen („Opt-out"). Im Sinne der Rechtssicherheit und auch um den Informationsverpflichtungen nachzukommen, wird die Verwendung eines Cookie-Pop-Up-Fensters vorgeschlagen, das durch Anklicken einer Schaltfläche (z.B. „O.K.") bestätigt werden kann. Wichtig ist, dass Cookies tatsächlich erst dann gesetzt werden, wenn die Einwilligung erteilt wurde. Einwilligungen über allgemeine Browsereinstellung oder konkludent über das Weitersurfen auf einer Webseite sind rechtlich sehr unsicher und werden nicht empfohlen. Weitere Informationen und Muster finden Sie auf der WKO-Webseite hier und hier.

Jedenfalls zustimmungspflichtig sind etwa Tracking-Cookies (die das Online-Verhalten von Nutzern z.B. für Werbezwecke nachverfolgen) oder Analyse-Cookies (die das Verhalten von Besuchern auf der eigenen Webseite analysieren), sobald diese auf dem Endgerät gespeichert werden. Unerheblich ist, ob dabei personenbezogene Daten verarbeitet werden.

Bezüglich Google Analytics sollten Sie die Einstellung wählen, dass die IP-Adressen, welche von Website-Besuchern erfasst werden, vor Übermittlung in die USA derart verkürzt werden, dass sie keiner Person mehr zugeordnet werden können. Die Software sollte eine entsprechende Einstellung enthalten.

Keine Einwilligung muss für Cookies eingeholt werden, die für einen vom Nutzer angefragten Dienst unbedingt erforderlich sind. Dazu zählen etwa „Warenkorb"-Cookies, Cookies zur Speicherung einer individuellen Benutzereinstellung (z.B. Sprache, Darstellung) oder Cookies, die zur Medienwiedergabe erforderlich sind.

24. Ist die (dynamische) IP-Adresse ein personenbezogenes Datum?

Ja, selbst dynamische IP-Adressen können laut einer Entscheidung des Europäischen Gerichtshofs ein personenbezogenes Datum sein. Wenn man IP-Adressen hingegen derart „verkürzt", dass sie keiner natürlichen Person mehr zugeordnet werden können, sind sie nicht mehr als personenbezogene Daten zu qualifizieren und fallen nicht mehr unter den Anwendungsbereich der DSGVO.

25. Sind anonymisierte Daten personenbezogene Daten?

Nein, wenn ein Personenbezug weder direkt noch indirekt hergestellt werden kann (und die Daten auch nicht bloß verschlüsselt oder pseudonymisiert sind), sind die Daten anonym und fallen nicht mehr unter den Anwendungsbereich der DSGVO.

26. Welche Tätigkeiten im Zusammenhang mit der DSGVO sind von dem Berechtigungsumfang der IT-Dienstleister umfasst? Kann ich Datenschutzbeauftragter gem. Art 37 DSGVO sein?

Von dem Berechtigungsumfang des Gewerbes ist unter anderem die Beratung, Erarbeitung und Umsetzung von Informationssicherheit und Sicherungskonzepten im Zusammenhang mit der DSGVO umfasst. Im Rahmen der Bestimmungen der DSGVO und des österreichischen DSG können IT-Dienstleister also auch als Datenschutzbeauftragte tätig sein.
» Das Berufsbild
» Weitere Informationen zum Datenschutzbeauftragten

27. Welche Pflichten ergeben sich aus der DSGVO für den Betriebsrat? Ist der Betriebsrat ebenfalls für die Einhaltung des Datenschutzes verantwortlich?

Nach herrschender Ansicht ist der Betriebsrat bezüglich der Datenverarbeitungen, die er im Rahmen seiner Befugnisse zu eigenen Zwecken vornimmt, selbst „Verantwortlicher" iSd DSGVO. Das heißt, dass der Betriebsrat selbst alle datenschutzrechtlichen Pflichten (z.B. Führung eines Verarbeitungsverzeichnisses) und die Grundsätze der DSGVO (z.B. Datenminimierung) einhalten muss. Es wird empfohlen, den Betriebsrat bei der Erstellung eines Prozesses für den Umgang mit Mitarbeiterdaten zu unterstützen.

Stand: 09.10.2019