Datensicherheit nach der EU-Datenschutz-Grundverordnung - FAQ

Antworten auf die wichtigsten Fragen

Viele Informationen zum Thema „Datenschutz und IT-Sicherheit“ finden Sie unter www.it-safe.at.

Wir empfehlen Ihnen insbesondere:

Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO

IT-Sicherheitshandbuch für KMU

IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter

Online-Ratgeber it-safe

ACHTUNG: Hier handelt es sich nicht nur um ein juristisches, sondern auch vorwiegend technisches Thema! Bei Zweifelsfragen empfiehlt sich die Kontaktaufnahme mit einem technischen Experten.

1. Könnten Sie vielleicht "wenn mit den Daten was passiert" genauer definieren? „Können Sie Beispiele dafür nennen, wann ich nach DGSVO tätig werden muss bzw. dafür, was mit Daten „passieren“ kann?
2. Müssen Webseiten die ein Kontaktformular anbieten eine https Verbindung haben oder reicht eine http Verbindung?
3. Genügt es, einen PC mit einem Passwort bei der Anmeldung zu schützen, oder muss das Passwort schon vor dem Hochfahren eingegeben werden (um die Festplatte zu schützen)?
4. Wie schaut es mit Firewalls/Routern aus, die meisten kleinen Firmen, haben ja keine richtige Firewall, sondern oft nur das Modem des Anbieters.
5. Ist die Dropbox sicher?
6. Ist Tresorit sicher?
7. Wann bzw. in welchen Fällen ist eine end-to-end Verschlüsselung im E-Mail Verkehr mit Kunden, Lieferanten etc. notwendig?
8. Ist in Zukunft ein Android-Handy (Stichwort Google Datenkrake schreibt alles mit) in puncto Datensicherheit noch mit gutem Gewissen verwendbar?
9. Anonymisierung von Daten: Wie groß muss die Gruppe der ausgewerteten Personen sein, damit ich diese Anonymität gewährleiten kann?
10. Kann ich mich darauf verlassen, dass alle Anbieter, die Cloudservices in Österreich anbieten (Apple, Evernote, Microsoft), sich an die DSGVO halten müssen und ich diese Services daher nutzen darf?
11. Setzt die neue DSGVO auch IT sicherheitstechnische Vorkehrungen (z.B. für Onlineshops) voraus? Im Punkt Serverstandort, Datenverschlüsselung, Firewall, etc.)
12. Bezüglich Anonymisierung, gibt es dazu Fristen, wann diese Anonymisierung bei einer Speicherung von personenbezogenen Daten durchgeführt werden muss?
13. Was bedeutet ausreichend Schutz? Reicht es z.B. passwortgeschützte Zugänge zu Datenbanken zu haben? Firewalls schützen vor Zugriffen - ist das ausreichend? Schutz vor Diebstahl - reichen abgesperrte Büros, ... usw.
14. Muss ich als Steuerberater gewährleisten, dass Mitarbeiter nicht mittels USB Stick illegal Daten absaugen können? Also die Möglichkeit generell sperren?
15. Ich bin Einzelunternehmer und Versicherungsmakler. Reicht es, wenn ich meine Daten nur bei mir zu Hause (mein PC, mein Handy usw) aufbewahre und darauf achte oder muss ich weitere Schritte setzen?
16. Ist Microsoft Onedrive Business sicher genug?
17. Wie müssen vertrauliche Projektdaten von Kunden behandelt/geschützt werden? Gibt es einen Standard dafür?
18. Finanzdienstleister, oft EPU, haben lokal (Laptop) Kundendaten gespeichert, die für Beratungen im Außendienst notwendig sind. Wie kann man

diese, auch unterwegs, gegen Diebstahl (z.B. durch Trojaner) schützen. Wie verhält es sich mit archivierten Mails mit Kundendaten bzw. Auftragsbestätigungen etc.?

19. Gibt es zuverlässige, allgemein gültige Kriterien nach denen ich beurteilen kann, ob ich mit meinen technischen und organisatorischen Maßnahmen das Auslangen finde. Gibt es sowas wie einen Mindestanforderungskatalog?
20. Wie schütze ich jetzt konkret meine Kundendaten, also zum Beispiel die Adressen die im Outlook gespeichert sind?
21. Ich bin ein EPU und verarbeite normale personenbezogene Daten (gespeicherte Aufträge, Adressen...). Frage: Genügt es diese Daten mit einer Verschlüsselungssoftware zu schützen?
22. Wie wird das Risiko bewertet, dass Kunden- bzw. Buchhaltungsdaten - wie bei so vielen (Home-)Office - offen bzw. in einem unversperrten Schrank stehen (kein Kundenverkehr)? Stichwort Einbruch aber auch generell, wobei versperrter Schrank wohl Aufmerksamkeit auf sich zieht.
23. Können Sie Software oder Programme empfehlen, die für den Datenschutz geeignet sind? Inwiefern sind Clouds "sicher"?
24. Ist ein PC mit XP noch Stand der Technik?
25. Erwachsenenbildungseinrichtung, ca. 1000 E-Mail-Adressen. Genügt es diese auf externe Festplatten zu speichern?
26. Wir sind eine IT Firma und haben Kundendaten wie Passwörter usw. auf unseren Server gespeichert. Auf welche Vorsichtsmaßnahmen müssen wir achten.
27. Gibt es eine Verpflichtung zur Verschlüsselung von Daten in der Cloud?
28. Welche Sicherheitslevels sind vor allem für Kleinunternehmer vorgeschrieben? Wie habe ich zB Kundenfotos auf einer Festplatte zu lagern? Verschlüsselt?
29. Darf mein Steuerberater meinen Steuerakt überhaupt noch per E-Mail versenden?
30. Müssen die Daten bei einem Smartphone mit zusätzlicher Software geschützt werden, weil Drittanbieter darauf zugreifen könnten (WhatsApp, Facebook, etc.)?
31. Wir haben nur Unternehmen als Kunden und daher nur Unternehmensdaten in der Kartei. Wir haben jedoch auch beispielsweise (teilweise private) Handynummern der Mitarbeiter - mit Namen verknüpft - der Unternehmen im System gespeichert. Müssen diese Nummern und Namen speziell geschützt werden, da dies ja personenbezogen Daten sind?
32. Wie muss ich Daten/ Adressen sichern, die in schriftlicher Form festgehalten werden?
33. Ich habe meine Registrierkasse bei hello-cash (Speicherung von Daten auf deren Server). Was muss/kann ich da zur Datensicherung machen?
34. Wenn man zu Hause/Homeoffice einen Mini Server (My Cloud) zur Speicherung der Kundendaten verwendet, ist das dann "sicher"? Wenn z. B. ein Einbrecher den Server mitnimmt, wären die Daten weg. Wie ist so ein Risiko einzuschätzen? Soll man die Kundendaten noch zusätzlich z. B. in einer Cloud absichern?
35. Was kann man zu normalen Personendaten (Name, Titel, Funktion, Adresse, E-Mail) in Excel-Listen sagen? Ist das riskant'
36. Ist die Einführung eines Informationssicherheitsmanagementsystems nach ISO 27001 eine angemessene Vorbereitung auf die DSGVO wenn das Unternehmen keine sensiblen personenbezogene Daten verarbeitet?

---

1. Könnten Sie vielleicht "wenn mit den Daten was passiert" genauer definieren? „Können Sie Beispiele dafür nennen, wann ich nach DGSVO tätig werden muss bzw. dafür, was mit Daten „passieren“ kann?

Wenn die Daten abhandenkommen, verloren gehen, beschädigt werden, angegriffen werden, gestohlen werden, etc. Jede Art von Datenleck.

2. Müssen Webseiten die ein Kontaktformular anbieten eine https Verbindung haben oder reicht eine http Verbindung?

Bei HTTPS-Websites wird die Verbindungen verschlüsselt. Sie müssen nicht, es ist allerdings empfehlenswert, insbesondere, wenn über diese Website personenbezogene Daten verarbeitet werden. Jedenfalls ist bei der Angabe von Kontendaten oÄ auf eine https-Verschlüsselung zu achten.

3. Genügt es, einen PC mit einem Passwort bei der Anmeldung zu schützen, oder muss das Passwort schon vor dem Hochfahren eingegeben werden (um die Festplatte zu schützen)?

Das richtet sich wie jede Datensicherheitsmaßnahme nach dem Einzelfall. Die Eingabe des Benutzernamens und Passworts im Anmeldebildschirm ist auf jeden Fall zu empfehlen, bietet vor dem Zugriff Unbefugter aber nur bedingt Schutz.

4. Wie schaut es mit Firewalls/Routern aus, die meisten kleinen Firmen, haben ja keine richtige Firewall, sondern oft nur das Modem des Anbieters.

Eine entsprechend konfigurierte Firewall zählt zu den Basismaßnahmen der IT-Sicherheit. Genauere Infos zu den verschiedenen Varianten erhalten Sie in unserem IT-Sicherheitshandbuch auf Seite 62.

5.Ist die Dropbox sicher?

Wir können und werden keine Aussage über die Sicherheit von spezifischen Anbietern treffen. Sicher ist ein Anbieter dann, wenn er Datensicherheitsmaßnahmen implementiert hat, wenn Sie wissen, wer auf die Daten zugreift, ob die Daten weitergegeben werden, wenn Sie wissen, wo die Daten gespeichert sind, etc. Bei Dropbox handelt es sich um einen US-Cloudspeicheranbieter. Sehen Sie sich jedenfalls die Datenschutzrichtlinien an und achten Sie darauf Ihre Nutzereinstellungen auf einen möglichst sicheren Standard zu setzen. Bei vielen Anbietern gibt es auch eine Business-Lösung (auch bei dropbox), die Standardanwendung ist oft nur für private Daten gedacht und ausgelegt.

6. Ist Tresorit sicher?

Wir können und werden keine Aussage über die Sicherheit von spezifischen Anbietern treffen. Sicher ist ein Anbieter dann, wenn er Datensicherheitsmaßnahmen implementiert hat, wenn Sie wissen, wer auf die Daten zugreift, ob die Daten weitergegeben werden, wenn Sie wissen, wo die Daten gespeichert sind, etc.

7. Wann bzw. in welchen Fällen ist eine end-to-end Verschlüsselung im E-Mail Verkehr mit Kunden, Lieferanten etc. notwendig?

Emails müssen auf Basis der DSGVO nicht zwingend verschlüsselt werden, das ist so nirgends ausgewiesen. Man kann sich aber aus Gründen der Datensicherheit dafür entschließen. Sinnvoll ist die Verschlüsselung jedenfalls bei der Handhabe mit heiklen Daten wie Bankverbindungen, Kreditkartendaten usw, aber natürlich auch bei der Handhabe mit sensiblen oder strafrechtlich relevanten Daten.

Je wichtigere und sensiblere Daten (zB Bankdaten, Kreditkartendaten) die Mail enthält, desto ist eine Verschlüsselung anzuraten. Oft kann es aber ausreichen, die übermittelten Dokumente zu schützen. Die Datei kann dabei zum Beispiel als Archiv-Datei (Zip) gepackt und mit einem Kennwort versehen werden. Das Kennwort zum Entpacken der Datei muss dann natürlich auf einem anderen Weg übermittelt werden (zB telefonisch).

Hinweise zu Verschlüsselung

8. Ist in Zukunft ein Android-Handy (Stichwort Google Datenkrake schreibt alles mit) in puncto Datensicherheit noch mit gutem Gewissen verwendbar?

Wir können und werden keine Aussage über die Sicherheit von spezifischen Anbietern treffen. Sicher ist ein Anbieter dann, wenn er Datensicherheitsmaßnahmen implementiert hat, wenn Sie wissen, wer auf die Daten zugreift, ob die Daten weitergegeben werden, wenn Sie wissen, wo die Daten gespeichert sind, etc.

9. Anonymisierung von Daten: Wie groß muss die Gruppe der ausgewerteten Personen sein, damit ich diese Anonymität gewährleiten kann?

Der Personenbezug darf keinesfalls mehr herstellbar sein. Das kann ab 5 Personen schon der Fall sein, das kann aber manchmal auch erst ab 50 Personen der Fall sein.

10. Kann ich mich darauf verlassen, dass alle Anbieter, die Cloudservices in Österreich anbieten (Apple, Evernote, Microsoft), sich an die DSGVO halten müssen und ich diese Services daher nutzen darf?

Es sollten sich alle Anbieter in der EU an die DSGVO halten. Sie müssen mit Ihren Dienstleistern (Auftragsverarbeitern) schriftlich einen Vertrag abschließen, in welchem u.a. auch gewährleistet ist, dass der Anbieter die Bestimmungen einhält und Datensicherheitsmaßnahmen implementiert hat. Anbieter österreichischer Cloud-Lösungen mit einem Speicherort der Daten im Inland finden Sie in der Austrian Cloud.

11. Setzt die neue DSGVO auch IT sicherheitstechnische Vorkehrungen (z.B. für Onlineshops) voraus? Im Punkt Serverstandort, Datenverschlüsselung, Firewall, etc.)

Sie weist keine spezifischen Vorkehrungen aus, außer, dass Verschlüsselung oder Pseudonymisierung im Einzelfall eine gute Maßnahme sein kann. Gerade bei Online-Shops ist aber zu bedenken, dass hier neben personenbezogenen Daten wie Name, Adresse und dergleichen, auch Bezahldaten wie etwa die Kreditkartennummer verarbeitet und online verwaltet werden. Daher sind Online-Shops sind ein besonders beliebtes Ziel von Kriminellen, um zB per Phishing an Zugangsdaten und in weiterer Folge beispielsweise an Kreditkartendaten zu gelangen. Der Shop-Betreiber ist rechtlich dafür verantwortlich, dass diese Daten entsprechend geschützt werden. Überdies erschüttern Vorfälle wie Datenverlust das Vertrauen der Kunden von Online-

Shops besonders massiv. Jedenfalls muss aktuelle Software eingesetzt werden und Sicherheitspatches und Updates zeitnah installiert werden. Entsprechende Verschlüsselungs- oder Authentifizierungsverfahren sind anzudenken und Firewalls einzusetzen. Auch ist intern organisatorisch auf Berechtigungskonzepte und die organisatorische Absicherung zu achten. Die konkret zu ergreifenden Maßnahmen werden durch den jeweils aktuellen Stand der Technik bestimmt.

Wir empfehlen dafür den Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO.

12. Bezüglich Anonymisierung, gibt es dazu Fristen, wann diese Anonymisierung bei einer Speicherung von personenbezogenen Daten durchgeführt werden muss?

Es gibt keine Fristen bzgl Anonymisierung.

13. Was bedeutet ausreichend Schutz? Reicht es z.B. passwortgeschützte Zugänge zu Datenbanken zu haben? Firewalls schützen vor Zugriffen - ist das ausreichend? Schutz vor Diebstahl - reichen abgesperrte Büros, ... usw.

Das richtet sich immer nach dem konkreten Einzelfall, nach dem Stand der Technik, Ihren finanziellen Möglichkeiten usw. Wir empfehlen dafür den Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO und das IT-Sicherheitshandbuch für KMU.

14. Muss ich als Steuerberater gewährleisten, dass Mitarbeiter nicht mittels USB Stick illegal Daten absaugen können? Also die Möglichkeit generell sperren?

Ja. Sie sind verpflichtet, dafür zu sorgen, dass die Bestimmungen des Datenschutzrechtes eingehalten werden. Zumindest sollten die Mitarbeiter geschult sein, Sie sollten Sie über das Datengeheimnis entsprechend aufklären und zumindest zumutbare Maßnahmen treffen. Manche Unternehmen unterbinden die Möglichkeit USB-Sticks zu verwenden, dies ist aber rechtlich nicht verpflichtend. Überdies finden Mitarbeiter mit kriminellen Absichten zweifellos auch andere Methoden um Daten „abzusaugen". Hier hilft nur eine entsprechende Sorgfalt bei der Personalauswahl und entsprechende Schulungsmaßnahmen und entsprechende Rechtevergabe (wer darf was). Wir empfehlen als Schulungsunterlage für das IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter sowie den Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO.

15. Ich bin Einzelunternehmer und Versicherungsmakler. Reicht es, wenn ich meine Daten nur bei mir zu Hause (mein PC, mein Handy usw) aufbewahre und darauf achte oder muss ich weitere Schritte setzen?

Sie müssen darauf achten die Bestimmungen des Datenschutzrechts einzuhalten. Ein Handy kann leicht abhandenkommen, hier sind als Mindeststandards PIN-Eingabe oder uU auch Verschlüsselung von Daten zu nennen, bei Diebstahl ist die Möglichkeit der Fernlöschung durch eine Sicherheits-App empfehlenswert. Tipps für die Sicherheit Ihres Smartphones. Bei der Datenaufbewahrung zu Hause ist zB auf räumliche Trennung der Datensicherung zu achten um bspw. bei Feuerschaden weiterhin auf diese zugreifen zu können. 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.

16. Ist Microsoft Onedrive Business sicher genug?

Wir können und werden keine Aussage über die Sicherheit von spezifischen Anbietern treffen. Sicher ist ein Anbieter dann, wenn er Datensicherheitsmaßnahmen implementiert hat, wenn Sie wissen, wer auf die Daten zugreift, ob die Daten weitergegeben werden, wenn Sie wissen, wo die Daten gespeichert sind, etc.

17. Wie müssen vertrauliche Projektdaten von Kunden behandelt/geschützt werden? Gibt es einen Standard dafür?

Sie müssen die Vorgaben des Datenschutzrechts einhalten. Welche Maßnahmen im Einzelfall zu setzen sind, ist sehr unterschiedlich. 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.

18. Finanzdienstleister, oft EPU, haben lokal (Laptop) Kundendaten gespeichert, die für Beratungen im Außendienst notwendig sind. Wie kann man diese, auch unterwegs, gegen Diebstahl (z.B. durch Trojaner) schützen. Wie verhält es sich mit archivierten Mails mit Kundendaten bzw. Auftragsbestätigungen etc.?

Hinweise zum Umgang mit mobilen Geräten finden Sie im IT-Sicherheitshandbuch für KMU auf Seite 52.
Tipps für die Sicherheit Ihres Smartphones

19. Gibt es zuverlässige, allgemein gültige Kriterien nach denen ich beurteilen kann, ob ich mit meinen technischen und organisatorischen Maßnahmen das Auslangen finde. Gibt es sowas wie einen Mindestanforderungskatalog?

Wir empfehlen Ihnen dafür unseren Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO, unser IT-Sicherheitshandbuch für KMU und unseren Online-Ratgeber it-safe.

20. Wie schütze ich jetzt konkret meine Kundendaten, also zum Beispiel die Adressen die im Outlook gespeichert sind?

Hinweise zur Verschlüsselung von Daten, Datensicherung, etc. finden Sie im Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO.

21. Ich bin ein EPU und verarbeite normale personenbezogene Daten (gespeicherte Aufträge, Adressen...). Frage: Genügt es diese Daten mit einer Verschlüsselungssoftware zu schützen?

Es ist sicher ein guter Schritt, er hilft Ihnen allerdings nichts im Hinblick auf Beschädigungen oder Datenverlust. Datensicherung ist auch ein sehr wesentliches Thema! Hinweise zur Verschlüsselung von Daten, Datensicherung, etc. finden Sie im Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO.

22. Wie wird das Risiko bewertet, dass Kunden- bzw. Buchhaltungsdaten - wie bei so vielen (Home-)Office - offen bzw. in einem unversperrten Schrank stehen (kein Kundenverkehr)? Stichwort Einbruch aber auch generell, wobei versperrter Schrank wohl Aufmerksamkeit auf sich zieht.

Sie müssen dafür Sorge tragen, dass kein Unbefugter (zB Putzfrau, ev. auch Familienmitglieder, Besuch, etc.) an die Daten gelangt. Auch für Einbruch, Feuer oder Wasserschaden ist Vorsorge zu tragen. Vergessen Sie auch nicht auf die Datensicherung (räumlich getrennt von den ursprünglichen Daten). Ein versperrter Schrank kann zB der Einsicht durch nicht befugte Mitarbeiter, Reinigungskräften uÄ entgegenwirken.

23. Können Sie Software oder Programme empfehlen, die für den Datenschutz geeignet sind? Inwiefern sind Clouds "sicher"?

Nein, wir können keine Anbieter bevorzugen.

24. Ist ein PC mit XP noch Stand der Technik?

XP ist von Microsoft selbst als unsicheres System deklariert worden und damit – falls eine Internetverbindung besteht – zweifellos nicht mehr Stand der Technik.

Stichtag für das Ende der Sicherheits-Updates für Windows 7 ist der 14. Januar 2020. Wir empfehlen daher bis dahin zum Wechsel des Systems.

25. Erwachsenenbildungseinrichtung, ca. 1000 E-Mail-Adressen. Genügt es diese auf externe Festplatten zu speichern?

Im Hinblick auf Datensicherung ist das zumindest ein guter erster Schritt. Sie müssen dabei neben Datensicherung aber auch beachten, dass Sie die Daten vor Unbefugten schützen. Informationen dazu erhalten Sie auf www.it-safe.at. Einen sehr guten Überblick über den Stand der Technik und Marktüblichkeit können Sie sich unter www.it-safe.at verschaffen.

26. Wir sind eine IT Firma und haben Kundendaten wie Passwörter usw. auf unseren Server gespeichert. Auf welche Vorsichtsmaßnahmen müssen wir achten.

Informationen dazu erhalten Sie auf www.it-safe.at. Wir empfehlen insbesondere unseren Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO und das IT-Sicherheitshandbuch für KMU.

27. Gibt es eine Verpflichtung zur Verschlüsselung von Daten in der Cloud?

Die gibt es nicht, es wäre allerdings eine Überlegung wert, da Sie sehr viel im Punkt Datensicherheit erfüllen würden.

28. Welche Sicherheitslevels sind vor allem für Kleinunternehmer vorgeschrieben? Wie habe ich zB Kundenfotos auf einer Festplatte zu lagern? Verschlüsselt?

Sie müssen auch als Kleinunternehmen ALLE Vorgaben der DSGVO beachten, das heißt entsprechende technische und organisatorische Maßnahmen treffen. Wir empfehlen insbesondere unseren Leitfaden für technische und organisatorische Maßnahmen im Rahmen der DSGVO und das IT-Sicherheitshandbuch für KMU.

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

Emails müssen auf Basis der DSGVO nicht zwingend verschlüsselt werden, das ist so nirgends ausgewiesen. Unverschlüsselte E-Mails bieten keine Datensicherheit und können von Unbefugten leicht „mitgelesen" werden. Unbedingt 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.

30. Müssen die Daten bei einem Smartphone mit zusätzlicher Software geschützt werden, weil Drittanbieter darauf zugreifen könnten (WhatsApp, Facebook, etc.)?

Ein derartiges Sicherungssystem, das die Daten davor schützt, dass Apps, deren Berechtigungen auf Ihre Daten Sie ja selbst frei gegeben haben, dennoch nicht darauf zugreifen können, ist mir nicht bekannt. Achten Sie daher bei Apps unbedingt darauf, welche Rechte Sie abgeben und installieren Sie nur vertrauenswürdige Apps.

31. Wir haben nur Unternehmen als Kunden und daher nur Unternehmensdaten in der Kartei. Wir haben jedoch beispielsweise auch Beispielsweise (teilweise private) Handynummern der Mitarbeiter - mit Namen verknüpft - der Unternehmen im System gespeichert. Müssen diese Nummern und Namen speziell geschützt werden, da dies ja personenbezogen Daten sind?

Die DSGVO gilt sowohl B2C als auch B2B, dh auch Unternehmensdaten sind davon erfasst und müssen entsprechend geschützt werden.

32. Wie muss ich Daten/ Adressen sichern, die in schriftlicher Form festgehalten werden?

Schriftlich meint hier wohl auf Papier. Versperrbare Schränke, Zutrittsberechtigungen, Zugriffsberechtigungen etc. wären hier anzudenken. Denken Sie dabei auch im eigenen Interesse an Datensicherung und daran, diese räumlich getrennt (zB zur Vorsorge bei Feuer) aufzubewahren. Auch eine entsprechende Entsorgung (Shreddern) kann hier wichtig sein. Informationen dazu erhalten Sie in unserem IT-Sicherheitshandbuch für KMU.

33. Ich habe meine Registrierkasse bei hello-cash (Speicherung von Daten auf deren Server). Was muss/kann ich da zur Datensicherung machen?

Wenn bzw falls Sie mit der Registrierkassa personenbezogene Daten erfassen, handelt es sich bei Ihrem Anbieter um einen sogenannten "Auftragsverarbeiter", sprich er verarbeitet Daten für Sie auf Ihre Entscheidung hin (Speicherung am Server). In diesem Fall müssen Sie einen schriftlichen Auftragsverarbeitervertrag (gewisse standardisierte Datenschutz-Klauseln) mit ihm abschließen, um Ihre Verpflichtungen auch entsprechend abzudecken und schriftlich zu fixieren. Muster finden Sie hier. Üblicherweise wird Ihnen der Anbieter ohnehin in den nächsten Wochen etwas in der Art zukommen lassen. Falls nicht, sollten Sie einmal nachhaken.

34. Wenn man zu Hause/Homeoffice einen Mini Server (My Cloud) zur Speicherung der Kundendaten verwendet, ist das dann "sicher"? Wenn z. B. ein Einbrecher den Server mitnimmt, wären die Daten weg. Wie ist so ein Risiko einzuschätzen? Soll man die Kundendaten noch zusätzlich z. B. in einer Cloud absichern?

Sie haben die Frage schon selbst beantwortet. Wenn das Ihr einziges Sicherungssystem ist und der Server kommt abhanden (wie auch immer), dann sind auch Ihre Daten weg. Überlegen Sie sich, wie lange Ihr Unternehmen ohne die darauf gespeicherten Daten arbeiten kann, wie hoch das Risiko ist, dass diese abhandenkommen und welche Konsequenzen sich daraus ergeben. Eine weitere (räumlich getrennte) Datensicherung ist unbedingt empfehlenswert.

35. Was kann man zu normalen Personendaten (Name, Titel, Funktion, Adresse, E-Mail) in Excel-Listen sagen? Ist das riskant'

Wohl eher nicht. Datensicherheitsmaßnahmen sind aber entsprechend den allgemeinen Vorschriften dennoch zu implementieren.

36. Ist die Einführung eines Informationssicherheitsmanagementsystems nach ISO 27001 eine

angemessene Vorbereitung auf die DSGVO wenn das Unternehmen keine sensiblen personenbezogene Daten verarbeitet?

ISO/IEC 27001 und DSGVO haben unterschiedliche Zwecke. Während die ISO/IEC 27001 eine Zertifizierung des Informationssicherheitsmanagements darstellt, zielt die DSGVO darauf ab, personenbezogene Daten zu schützen. ISO-27001 zertifizierte Unternehmen erfüllen daher nicht automatisch die DSGVO, haben jedoch aufgrund ihrer umfassenden Dokumentation des Informationssicherheitssystems eine ausgezeichnete Basis für die DSGVO, die meist nur mehr adaptiert werden muss.

Zu achten ist aber insbesondere darauf, dass bei der ISO als freiwillige Zertifizierung der Anwendungsbereich eingeschränkt werden kann (zB nur bestimmte Bereiche des Unternehmens). während die DSGVO als gesetzliche Regelung immer für alle Datenverarbeitungsvorgänge im Unternehmen gilt.

Stand: 25.10.2019