Einstieg in die EU-Datenschutz-Grundverordnung - FAQ

Antworten auf die wichtigsten Fragen

Achtung: Wir haben hier nicht die Möglichkeit einen gesamten betrieblichen Ablauf darzustellen – zu diesen Zwecken gibt es die Informationsprodukte auf www.wko.at/datenschutz, auf welche direkt in den jeweiligen Fragen verwiesen wird!

1. Was meinen Sie mit personenbezogenen Datensatz? Was sind persönliche bzw. schützenswerte Daten?
2. Was muss ich konkret als Kleinunternehmen/Händler tun, der normale Kundendaten (Namen, Adressen, Tel., Mail, und zusätzlich ev. Geburtsdaten, Vorlieben, etc.) von Kunden speichert?
3. Was ist mit den Online-Unternehmen? Also z.B. Shop Betreiber, der natürlich SM-Werbung macht, AdWords schaltet und Verkäufe über den Online-Shop umsetzt?
4. Wir sind ein Sportverein und veröffentlichen auf unserer Website z.B., Namen, Größe, Gewicht, Geburtsdaten und Bilder unserer Sportler. Wie müssen wir korrekt vorgehen?
5. Was mache ich mit Kontaktdaten welche sich schon seit 30 Jahren in meiner EDV gestützten Datenbank sind - sind die Daten eines Ansprechpartners in einem Kundenkontakt als persönliche Daten oder als Firmendaten zu behandeln?
6. Sind die beruflichen Kontaktdaten eines Kunden als Personendaten anzusehen?
7. Was muss z.B. ein praktischer Arzt machen, um die DSGVO zu erfüllen?
8. Was bedeutet die DSVO für eine Schule, die persönliche Daten (inkl. Leistungsbeurteilungen) auf einem Server speichern?
9. Gibt es bei der neuen Datenschutzregelung Unterschiede zwischen Kleinunternehmer und GmbH?
10. Zählen als persönliche Daten auch die Kontaktdaten bei den Geschäftspartnern z.B. Durchwahl, Handynummer oder Email-Adresse des Sachbearbeiters oder des Angestellten?
11. Was sind die Minimalanforderungen an Unternehmensberater: EPU ohne Mitarbeiter(innen, nur ein Notebook und ein Handy, Adressen in einer Exceltabelle und in Kontakteordnern, bzw. Kontakte in diversen sozialen Netzwerken). Keine weiteren Anwendungen.
12. Wenn im Unternehmen ausschließlich Standardanwendungen durchgeführt werden, muss der Betrieb zusätzliche Vorbereitungen treffen?
13. Gelten die Vorschriften nur für elektronische Datenverarbeitung oder z.B. auch für handschriftliche Aufzeichnungen?
14. Als Business Coach habe ich meine Daten von meinen Kunden nur auf Papier (mit Ausnahme der E-Mail-Adresse). Was ist hier zu tun? Zugriff habe nur ich als Unternehmenseigentümer.
15. Wie ist es mit Ordner, die ersichtlich im Büro stehen. Auf den Ordner stehen Namen von Kunden, das kann jeder sehen?
16. Habe ich "weniger" Schwierigkeiten wenn ich Daten über die Position von Personen habe, aber ich nicht weiß wer diese Personen sind (Name, usw.)?
17. Wie sind Visitenkarten handzuhaben?
18. Daten verarbeiten bedeutet elektronisch - oder? Wenn ich Kundenkarteien auf altmodischen Kartons in einer Box habe, dann nicht?
19. Was, wenn der Kunde keine natürliche Person, sondern es sich um B2B handelt. Trifft hier auch die DSGVO zu?
20. Was muss ein KMU mit den personenbezogenen Daten tun? Abspeichern? Einreichen bei Behörden?
21. Sind Daten von juristischen Personen ebenfalls personenbezogene Daten (z.B. Kundendaten im Großhandel)? Gelten dieselben Regeln zwischen mir als GesmbH und meinen Kunden die Einzelunternehmer sind? Sind diese wie natürliche Personen zu behandeln?
22. Sind EPU als Unternehmen anzusehen, oder als Privatpersonen?
23. Wenn statt des Namens nur Initialen gespeichert werden, ändert das etwas?
24. Wenn man Bilder und Videos betrachtet, wann gilt eine Person in einem Bild bzw. Video als personenbezogen Daten?
25. Welche betrieblichen Änderungen kommen auf uns zu?
26. Was ist mit den Daten von Unternehmen (Adressen, Kontakte, Gesprächsnotizen u.s.w.). Unterliegen die denselben Bestimmungen?
27. Gilt die DSGVO nur für Unternehmen? Oder auch für meinen Umgang mit Personendaten als Privatperson?

---

1. Was meinen Sie mit personenbezogenen Datensatz? Was sind persönliche bzw. schützenswerte Daten?

Personenbezogen ist alles, was nur in irgendeiner Art und Weise einen Bezug zu einer natürlichen Person herstellen kann, also z.B. Name, Adresse, Telefonnummer, aber auch Abbilder, Fingerabdrücke, Gesundheitsdaten, usw.

2. Was muss ich konkret als Kleinunternehmen/Händler tun, der normale Kundendaten (Namen, Adressen, Tel., Mail, und zusätzlich ev. Geburtsdaten, Vorlieben, etc.) von Kunden speichert?

Sie müssen auch als kleiner Händler ALLE Vorgaben der DSGVO beachten. Beginnen sollten Sie einmal mit einer Art „Dateninventur", schauen Sie sich an, wo und wie Sie überall im Betrieb personenbezogene Daten verarbeiten und gehen Sie dann z.B. am besten schrittweise unsere Checkliste bzw. unseren Onlineratgeber durch.

3. Was ist mit den Online-Unternehmen? Also z.B. Shop Betreiber, der natürlich SM-Werbung macht, AdWords schaltet und Verkäufe über den Online-Shop umsetzt?

Auch Sie verarbeiten personenbezogene Daten, dh die Bestimmungen der DSGVO sind für Sie anwendbar. Auf Websites kommen allerdings auch andere Bestimmungen aus anderen Rechtsgebieten zur Anwendung, Näheres hierzu finden Sie im Wirtschafts- und Gewerberecht auf WKO.at.

4. Wir sind ein Sportverein und veröffentlichen auf unserer Website z.B., Namen, Größe, Gewicht, Geburtsdaten und Bilder unserer Sportler. Wie müssen wir korrekt vorgehen?

Sie müssen auch als Verein ALLE Vorgaben der DSGVO beachten. Bei der Veröffentlichung von Daten auf der Website empfiehlt es sich eine Einwilligung für genau diese Datenarten und Zwecke und Veröffentlichung von den betroffenen Sportlern einzuholen.

5. Was mache ich mit Kontaktdaten welche sich schon seit 30 Jahren in meiner EDV gestützten Datenbank sind - sind die Daten eines Ansprechpartners in einem Kundenkontakt als persönliche Daten oder als Firmendaten zu behandeln?

Bei jeder Datenverarbeitung sind bestimmte Grundsätze zu beachten Sind die Daten aktuell und richtig? Habe ich eine Rechtsgrundlage für die Datenverarbeitung? Speichere ich nur solche Daten, die ich auch tatsächlich noch benötige? Ist eine angemessene Sicherheit für die personenbezogenen Daten gewährleistet? Im Hinblick auf 30 Jahre alte Kontaktdaten stellt sich hier insbesondere die Frage ob diese Daten noch aktuell sind. Sind sie das nicht, sind sie zu löschen.

Es gibt zwar eine Ausnahme vom Anwendungsbereich der DSGVO für Datenverarbeitungen, welche **ausschließlich** zu persönlichen oder familiären Zwecken erfolgt, sobald jedoch ein Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird, findet die DSGVO vollumfänglich Anwendung. Der Ansprechpartner bei einem Kundenkontakt hat eher Bezug zur beruflichen Tätigkeit.

6. Sind die beruflichen Kontaktdaten eines Kunden als Personendaten anzusehen?

Ja.

7. Was muss z.B. ein praktischer Arzt machen, um die DSGVO zu erfüllen?

Sie müssen auch als Arzt ALLE Vorgaben der DSGVO beachten. Beginnen sollten Sie einmal mit einer Art „Dateninventur", schauen Sie sich an, wo und wie Sie überall im Betrieb personenbezogene Daten verarbeiten und gehen Sie dann z.B. am besten schrittweise unsere Checkliste bzw. unseren Onlineratgeber durch.

8. Was bedeutet die DSVO für eine Schule, die persönliche Daten (inkl. Leistungsbeurteilungen) auf einem Server speichern?

Auch als Schule sind ALLE Vorgaben der DSGVO zu beachten. Leistungsbeurteilungen sind allerdings wohl Kerngeschäft einer Bildungseinrichtung, weshalb man hier wohl davon ausgehen soll, dass eine vertragliche oder gesetzliche Grundlage besteht. Hinsichtlich der Speicherung auf „einem Server" sind genauso Datensicherheitsmaßnahmen einzuhalten (wo ist dieser Server, wie ist er gesichert, wer hat Zugriff, usw).

9. Gibt es bei der neuen Datenschutzregelung Unterschiede zwischen Kleinunternehmer und GmbH?

Nein. Es kann nur sein, dass die Daten der GmbH (demnach die Daten der juristischen Person) nicht als personenbezogen einzuordnen sind. Die DSGVO sagt hier klar nein, das österreichische Datenschutzgesetz ist hier leider nicht so eindeutig. Man muss noch abwarten, was die Rechtsprechung dazu sagt.

10. Zählen als persönliche Daten auch die Kontaktdaten bei den Geschäftspartnern z.B. Durchwahl, Handynummer oder Email-Adresse des Sachbearbeiters oder des Angestellten?

Ja.

11. Was sind die Minimalanforderungen an Unternehmensberater: EPU ohne Mitarbeiter(innen, nur ein Notebook und ein Handy, Adressen in einer Exceltabelle und in Kontakteordnern, bzw. Kontakte in diversen sozialen Netzwerken). Keine weiteren Anwendungen.

Sie müssen auch als EPU ALLE Vorgaben der DSGVO beachten. Beginnen sollten Sie einmal mit einer Art „Dateninventur", schauen Sie sich an, wo und wie Sie überall im Betrieb personenbezogene Daten verarbeiten und gehen Sie dann z.B. am besten schrittweise unsere Checkliste bzw unseren Onlineratgeber durch.

12. Wenn im Unternehmen ausschließlich Standardanwendungen durchgeführt werden, muss der Betrieb zusätzliche Vorbereitungen treffen?

Unabhängig davon, ob Sie mit Standardanwendungen jene nach der Standard- und Musterverordnung 2004 – StMV 2004 meinen, welche bislang nicht meldepflichtige Anwendungen aufzählte, oder „Standardanwendungen" iSv simplen Office-Anwendungen, müssen Sie ALLE Vorgaben der DSGVO beachten. Beginnen sollten Sie einmal mit einer Art „Dateninventur", schauen Sie sich an, wo und wie Sie überall im Betrieb personenbezogene Daten verarbeiten und gehen Sie dann z.B. am besten schrittweise unsere Checkliste bzw unseren Onlineratgeber durch.

13. Gelten die Vorschriften nur für elektronische Datenverarbeitung oder z.B. 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,...).

14. Als Business Coach habe ich meine Daten von meinen Kunden nur auf Papier (mit Ausnahme der E-Mail-Adresse). Was ist hier zu tun? Zugriff habe nur ich als Unternehmenseigentümer.

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,...), dh Sie müssen – auch wenn nur Sie darauf Zugriff haben – alle Bestimmungen der DSGVO einhalten.

15. Wie ist es mit Ordner, die ersichtlich im Büro stehen. Auf den Ordner stehen Namen von Kunden, das kann jeder sehen?

Sofern diese Ordner ein Dateisystem darstellen, fallen auch diese in die DSGVO. Dateisystem ist eine strukturierte Sammlung personenbezogener Daten, die nach bestimmen Kriterien geordnet ist (z.B. alphabetisch, chronologisch,...), dh Sie müssen alle Bestimmungen der DSGVO einhalten. Ob es sinnvoll ist, dass die Ordner so ausgewiesen sind, dass jeder, der Zutritt zu Ihrem Büro hat, auch sieht, welche Kunden Sie betreuen, ist schon aus der Kundenbetreuung heraus wohl zu verneinen. Besser wäre es natürlich, die Kundenakten so abzulegen, dass diese nicht für jeden ersichtlich sind.

16. Habe ich "weniger" Schwierigkeiten wenn ich Daten über die Position von Personen

habe, aber ich nicht weiß wer diese Personen sind (Name, usw.)?

Zu befürchten ist, dass man aufgrund der Position einer Person im Unternehmen schon Rückschlüsse auf die Person selbst ziehen kann. Dh es wäre ein indirekt personenbezogener Datensatz und es wären dieselben Regeln anzuwenden, wie bei direkt personenbezogenen Datensätzen, wie Namen.

17. Wie sind Visitenkarten handzuhaben?

Visitenkarten sind dann, wenn Sie diese elektronisch abspeichern oder in einer gewissen Ordnung aufbewahren, ebenfalls von der DSGVO erfasst.

18. Daten verarbeiten bedeutet elektronisch - oder? Wenn ich Kundenkarteien auf altmodischen Kartons in einer Box habe, dann nicht?

Doch, wenn diese Kundenkarteien in Kartons oder in der Box nach einem gewissen Ordnungssystem abgelegt sind.

19. Was, wenn der Kunde keine natürliche Person, sondern es sich um B2B handelt. Trifft hier auch die DSGVO zu?

Ja. B2B oder B2C macht keinen Unterschied.

20. Was muss ein KMU mit den personenbezogenen Daten tun? Abspeichern? Einreichen bei Behörden?

Nichts dergleichen. Sie tun das, was Sie aufgrund Ihrer Vertragsbeziehung mit dem jeweils Betroffenen vereinbart haben, wozu Sie gesetzlich verpflichtet sind oÄ. Sie arbeiten tagtäglich mit personenbezogenen Daten (z.B. Rechnungsausstellung an einen Kunden). All diese Vorgänge sind in Zukunft zu protokollieren. Das Protokoll (= Verarbeitungsverzeichnis), ist allerdings nirgends zu veröffentlichen, es muss nur der Behörde bei einer allfälligen Prüfung offen gelegt werden.

21. Sind Daten von juristischen Personen ebenfalls personenbezogene Daten (z.B. Kundendaten im Großhandel)? Gelten dieselben Regeln zwischen mir als GesmbH und meinen Kunden die Einzelunternehmer sind? Sind diese wie natürliche Personen zu behandeln?

Gute Frage. Nach der DSGVO sind Daten juristischer Personen (= GmbH, AG, nicht aber schlichtweg Unternehmen!!!), nicht erfasst. Im österreichischen Datenschutzgesetz sind sie tlw erfasst. Es bleibt abzuwarten, wie hier von der Rechtsprechung entschieden wird.

22. Sind EPU als Unternehmen anzusehen, oder als Privatpersonen?

Es sind Unternehmen, aber keine juristischen Personen. Die Daten von Einzelunternehmern sind genauso personenbezogene Daten wie die von Privatpersonen.

23. Wenn statt des Namens nur Initialen gespeichert werden, ändert das etwas?

Wenn die Person dahinter rückführbar ist, leider nein. Wenn das Datum dadurch anonymisiert worden wäre, dann ja.

24. Wenn man Bilder und Videos betrachtet, wann gilt eine Person in einem Bild bzw. Video als personenbezogen Daten?

Wenn die Person erkennbar ist.

25. Welche betrieblichen Änderungen kommen auf uns zu?

Das Verarbeitungsverzeichnis ist völlig neu, ebenso die eigenständige Risikoanalyse, die Datenschutz-Folgenabschätzung, der Datenschutzbeauftragte in manchen Fällen, es gibt neue Regelungen bei den Rechten betroffener Personen und der Meldepflichten von Datenschutzverletzungen, usw.

26. Was ist mit den Daten von Unternehmen (Adressen, Kontakte, Gesprächsnotizen u.s.w.). Unterliegen die denselben Bestimmungen?

Ja.

27. Gilt die DSGVO nur für Unternehmen? Oder auch für meinen Umgang mit Personendaten als Privatperson?

Sie gilt nur im geschäftlichen Umfeld. Die private Datenverarbeitung (z.B. privates Video, privates Telefonverzeichnis usw) unterliegen nicht der DSGVO.

28. Zählt zu den personenbezogene Daten auch das Geburtsdatum?

Das Geburtsdatum ist ein personenbezogener Datensatz.

29. Was muss man bezüglich im Datenschutz in ERP-Systemen beachten?

Enterprise-Resource-Planning-Systeme enthalten zum Teil personenbezogene Daten, dh es wird auch in die DSGVO fallen, dh Sie müssen sich überlegen, welche Sicherheitsmaßnahmen Sie für das System implementiert haben, wie die Risiken sind, wer darauf Zugriff hat usw. Die Umsetzung der Datenschutz-Grundsätze (z.B. Datenminimierung, Speicherbegrenzung) kann je nach System eine Herausforderung sein, aber müssen auch hier implementiert werden. Wichtig ist auch darauf zu achten, dass die Datenverarbeitung in diesem System entsprechend im Verarbeitungsverzeichnis protokolliert wird.

Stand: 19.03.2019