FAQs zur DSGVO:

Häufige Fragen kurz und bündig beantwortet.

Wir beantworten unten einige der oft gestellten Fragen zur Datenschutz-Grundverordnung:
(mit Klick auf die Frage, gelangen Sie direkt zur Antwort!)

a) Kann man **auf die DSGVO** mit Kunden **verzichten**?
b) Sind **soziale Medien** (Facebook, WhatsApp und Co.) **noch erlaubt?**
c) Darf man Daten **in Cloud-Systemen speichern?**
d) Frage: **Was sind TOMs?** Was muss ich tun, um die Sicherheit herzustellen?
e) **Cookies** künftig auf Homepages **erlaubt?** Was regelt die ePrivacy-Verordnung?
f) Gilt die DSGVO auch **für Mitarbeitende?**
g) Wer braucht einen Datenschutzbeauftragten?
h) Unterschied zwischen **Datenschutzbeauftragtem und Datenschutzkoordinator?**
i) Was versteht man unter **Profiling,** was als Hinweis genannt wird, dass man einen Datenschutzbeauftragten benötigt? **Ist Sortieren in einer Excel-Datei** schon Profiling?
j) Muss der Datenschutzbeauftragte ein Angestellter sein?
k) Braucht man **als Finanzdienstleister, Vermögensberater, Agent, Makler** per se einen Datenschutzbeauftragten? Oder reicht ein Datenschutzkoordinator?
l) Der Vermittler bekommt Daten und leitet diese an Partner (Versicherung, WPF) weiter. Oder er erfasst diese Daten direkt im System des Versicherers oder WPF. **Wer haftet für die Daten? Wer muss Auskunft (dem Kunden etc.) geben?**
m) Wie erfüllt man die **Informationspflichten** aufgrund der DSGVO? Eigene Datenschutz-, Cookie-Erklärung, Kontakte zu Dritten..
n) **Sind USB-Sticks künftig noch erlaubt?** (können Viren enthalten, verloren gehen)
o) Gilt die DSGVO nur für elektronische Datenverarbeitung oder **auch für Papierakten?**

a) Frage: Kann ich mit dem Kunden vereinbaren, dass wir auf die Umsetzung der DSGVO verzichten oder der Kunde auf bestimmte Rechte aus der DSGVO verzichtet?

Antwort: **Nein.** Diese Möglichkeit wird bei Diskussionen immer wieder angesprochen. Aber: Das Recht auf Datenschutz ist ein verfassungsmäßig geschütztes Recht. Man kann auch nicht per Vertrag auf seine Menschenrechte verzichten. Derartige Vertragsregelungen wären unserer Ansicht nach sittenwidrig.

b) Frage: Sind soziale Medien wie Facebook/WhatsApp ab 25.5.2018 noch erlaubt?

Antwort: Wer als Unternehmer absolut sichergehen will, **verbietet generell die Nutzung von Social Media** oder sperrt den Zugriff im Büro, um Datenschutzverletzungen zu vermeiden.

Nicht erst seit dem Datenskandal im US-Wahlkampf (Cambridge Analytica hat sich über Facebook Zugang zu Informationen von rund 84 Millionen Facebook-Nutzern besorgt, daraus Profile erstellt) ist bekannt, dass Facebook und WhatsApp große Datenschutzprobleme verursachen.

Der **Datenschutzbeauftragte des Landes Thüringen warnt**:
„99 Prozent der deutschen WhatsApp-Nutzer verhielten sich ‚deliktisch', weil sie dem Dienst Zugang zu den Daten ihrer Kontakte geben", denn wer WhatsApp nutze, erlaube dem Dienst, **alle Kontaktdaten seines Smartphones auszulesen.**

Es gibt eine Menge solcher Social Media-Programme, die ähnlich wie Facebook vorgehen. Daher: Zumindest die beruflichen Kontakte dürfen sicher nicht abgeglichen werden, weil hierzu die Zustimmung vom Kunden, vom Partner, vom Mitarbeitende etc. fehlt. Zumindest aber muss man im Rahmen einer Internet Policy, die von jedem Mitarbeiter zu unterschreiben ist, auf die Gefahren hinweisen und diesen oben beschriebenen Abgleich der Daten jedenfalls ausdrücklich verbieten.

c) Frage: Darf man Daten in Cloud-Systemen speichern?

Antwort: In einer **europäischen Cloud:** Ja. Dennoch sollten Sie eine Datenverarbeitungserklärung mit dem Cloud-Anbieter abschließen oder sich ein entsprechendes Dokument von dessen Homepage herunterladen.
Bei **US-Cloud-Anbietern** ist Vorsicht geboten, denn dort gelten Datenschutzregeln, die mit unseren nicht vergleichbar sind. Daher gilt für europäische Daten, die auf US-Servern liegen, fast kein Datenschutz. Folge: Amerikanische Server gelten grundsätzlich als nicht sicher (aus Sicht der DSGVO). Es sei denn, der Anbieter unterwirft sich dem „Privacy Shield-Abkommen".
Ob ein ausländisches Unternehmen den „Privacy Shield" akzeptiert hat, kann man hier prüfen:
https://www.privacyshield.gov/welcome

Tipp: Bei der Cloud-Lösung sollte man darauf achten, dass es eine **EUROPÄISCHE Cloud** ist und die **Übertragung zur Cloud verschlüsselt** erfolgt.
Microsoft bietet zwar diese Lösung auch in Europa an, aber nicht für alle Office-Lösungen.

Man sollte abklären und sich schriftlich bestätigen lassen, dass nur Cloud-Server in Europa verwendet werden. Denn in den USA gelten Datenschutzregeln, die mit unseren nicht vergleichbar sind. Daher gelten europäische Daten, die auf US-Servern liegen, als nicht geschützt. Außer der Anbieter unterwirft sich dem „Privacy Shield-Abkommen".

d) Frage: Was sind TOMs? Was muss ich tun, um die Sicherheit herzustellen?

Antwort: TOM ist die Abkürzung für „**T**echnische und **O**rganisatorische **M**aßnahmen".

Definiert werden die technisch organisatorischen Maßnahmen, die Sie setzen müssen, im Artikel 32 der DSGVO. Verantwortliche und Auftragsverarbeiter haben dafür zu sorgen, dass „geeignete technische und organisatorische Maßnahmen" implementiert sind, die sicherstellen, dass „ein angemessenes Schutzniveau gewährleistet ist".

Diese Maßnahmen **sollen sicherstellen, dass** die Vertraulichkeit, Integrität, Verfügbarkeit und Sicherheit der Daten und damit der Systeme gegeben ist.

Für den Verantwortlichen sind dabei der Stand der Technik, die Implementierungskosten und das Risiko (Eintrittswahrscheinlichkeit und Schadenshöhe) zu berücksichtigen.

Dabei ist etwa die **Raumsituation** (Gebäudesicherung, einbruchssichere Türen, versperrbare Räume/Schränke, Videoüberwachung usw.) zu prüfen.

Software: Hier gehören etwa das Vergeben von sicheren Passwörtern auf PCs/besondere Admin-Rechte bei Server-Zugriffen und das Aufzeichnen von Zugriffen etc. hinein. Ebenso die Verschlüsselung von Dateien, die Sie via E-Mail-Versenden! Dazu neueste Software, Virenschutz, Firewall etc.

Auch müssen Sie die **regelmäßige Speicherung** Ihrer Daten auf verschiedenen Medien an verschiedenen Orten und ein **Verfahren für den GAU** (größtmöglich anzunehmender Unfall, etwa Hackerangriff) und das Wiederherstellen der Daten und das Informieren der Datenschutzbehörde und aller Betroffenen definieren und dokumentieren.

e) Frage: Dürfen künftig Cookies auf Homepages verwendet werden? Was regelt die ePrivacy-Verordnung?

Antwort: Dazu ist vieles **noch nicht definitiv geregelt**. EDV-Experten meinen dazu, dass technische Cookies, die für das Funktionieren der Homepage nötig sind, auch weiterhin verwendet werden dürfen. Aber **Tracking-Cookies**, die dazu dienen, das Nutzerverhalten erfassen und auswerten zu können, werden nach dem 25.5.2018 **nicht mehr erlaubt** sein. Außer der Nutzer wird genau darauf hingewiesen und stimmt dem ausdrücklich zu. Wichtig: Keinesfalls darf das Häkchen bei „Ich stimme zu" schon gesetzt sein (wie das bisher üblich war), das verbietet der Grundsatz der DSGVO „privacy by design"!

Cookies sind kleine Textdateien, die auf dem Rechner des Besuchers einer Website abgelegt werden und z.B. dafür sorgen, dass die Bestellung im Warenkorb gespeichert wird.
Aber Cookies helfen dem Betreiber auch, den Besucher wiederzuerkennen und ihm individuelle Werbung anzubieten. Damit gelingt es großen Konzernen wie Amazon, Google, Facebook & Co., über die Jahre ein umfangreiches Bild einer Person und deren Vorlieben zu erstellen.

Hier liegen die Gefahren der Cookies für den Datenschutz. Auch bedenklich ist es, wenn personenbezogene Daten, die sich in den Cookies verstecken (Name, IP-Adresse, besuchte Websites etc.) auf amerikanische Server übertragen werden (Google Analytics Cookies an Google-Server in den USA).

Daher musste man schon bisher über die Nutzung von Web-Analyse-Tools wie Google Analytics auf der eigenen Homepage informieren.

Die DSGVO erwähnt das Wort Cookies explizit nicht.
Dazu wird es eine ePrivacy-Verordnung geben, die die neuen Regeln für den Umgang der digitalen Medien und elektronischen Kommunikationsdienste mit der DSGVO regeln soll.

Ein wichtiger Punkt dieser ePrivacy-Verordnung soll das Thema „Webtracking und Cookies" sein. Die EU erwartet sich, dass die Einholung der Zustimmung benutzerfreundlich, einfach und transparent sein soll. Tracking soll standardmäßig nicht erlaubt und die Datenschutz-freundlichste Variante voreingestellt sein. Dies bedeutet für die Praxis, dass neue Geräte, neue Browser so ausgeliefert werden, dass Cookies oder ähnliche (Tracking-)Techniken standardmäßig deaktiviert sind. Eine Änderung ist nur mit einem unmissverständlichen Opt-in, also einer bewussten Zustimmung der User, möglich.

f) Frage: Gilt die DSGVO auch für Mitarbeitende?
Antwort: Ja. Verarbeiten Sie etwa Name, Adresse, Kontodaten, Sozialversicherungsnummer, religiöses Bekenntnis, die Windows-Lizenz-Nummer/IP-Nummer, die Inventarnummer des Pc der Mitarbeitenden, dann sind das alles personenbezogene Daten und fallen somit unter die DSGVO.

g) Frage: Wer muss einen Datenschutzbeauftragten bestellen? Aufgaben?
Bisher war in die Bestellung eines Datenschutzbeauftragten nicht nötig. Doch ab dem 25.05.2018 müssen Unternehmen prüfen, ob ein Datenschutzbeauftragter zu bestellen ist.

Unternehmen müssen einen Datenschutzbeauftragten bestellen, wenn

- die **Kerntätigkeit** 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.
  Beispiele: **Banken, Versicherungen,** Kreditauskunfteien und Berufsdetektive,

- die **Kerntätigkeit** des Unternehmens in der umfangreichen Verarbeitung **sensibler Daten** oder von Daten über **strafrechtliche** Verurteilungen oder Straftaten besteht (z.B. Krankenanstalten).

Bei der genauen Auslegung dieser Definition wird wieder auf **die „Art. 29-Gruppe" verwiesen**, über die wir bereits im Kapitel „Verfahrensverzeichnis" berichtet haben.

Muss ein Datenschutzverantwortlicher bestellt werden, sind seine **Kontaktdaten auf der Homepage zu veröffentlichen und der Datenschutzbehörde mitzuteilen.**
Wird – trotz Verpflichtung – kein Datenschutzbeauftragter bestellt, droht eine **Strafe** von bis zu EUR 10 Mio. oder 2 % des letztjährigen weltweiten Jahresumsatzes.

h) Frage: Was ist der Unterschied zwischen Datenschutzbeauftragtem und Datenschutzkoordinator?

Antwort: Wenn die Voraussetzungen erfüllt sind, ist ein Datenschutzbeauftragter rechtswirksam zu bestellen und der Datenschutzbehörde zu melden. Er ist in die Organisation entsprechend zu integrieren und der einzige Ansprechpartner für die Datenschutzbehörde.

Der DS-Koordinator hat intern ähnliche Aufgaben wie der DS-Beauftragte, er kümmert sich um die Umsetzung der DSGVO intern und ist intern und nach außen, also auch für die Behörde, der Ansprechpartner für DSGVO-Angelegenheiten. Er muss nicht der Behörde gemeldet werden.

i) Frage: Was versteht man unter Profiling, was als Hinweis genannt wird, dass man einen Datenschutzbeauftragten benötigt? Ist Sortieren in einer Excel-Datei schon Profiling?

Antwort: Nein. Profiling liegt vor, wenn man **große Datenmengen automatisiert verarbeitet und daraufhin Maßnahmen setzt.** Sortieren einer Excel-Datei ist kein Profiling.

Begründung: Profiling ist im Erwägungsgrund 71 der DSGVO definiert als „jegliche Form automatisierten Verarbeitens personenbezogener Daten unter Bewertung der

– persönlichen Aspekte in Bezug auf eine natürliche Person …, insbesondere zur

– Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage,

– Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten,

– Aufenthaltsort oder Ortswechsel der betroffenen Person, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt".

j) Frage: Ich muss einen Datenschutzbeauftragten installieren. Muss das ein Angestellter sein?

Antwort: Nein, das kann auch eine externe Person oder ein Unternehmen sein. Es kann durchaus sinnvoll sein, diese Funktion auszulagern. Nicht nur, weil ein Datenschutzbeauftragter einen de facto Kündigungsschutz hat. Sondern vor allem deshalb, weil man dieses Spezialwissen zur DSGVO nicht neu erfinden und lange aufbauen muss.

k) Frage: Braucht man als Finanzdienstleister, Vermögensberater, Agent, Makler per se einen Datenschutzbeauftragten? Oder reicht ein Datenschutzkoordinator?

Antwort: Das lässt sich aus der Ferne nicht zu 100 % beurteilen. Grundsätzlich herrscht die Ansicht, dass in den meisten Fällen ein DS-Koordinator reicht. Aber eine 100 %-ige Aussage kann man nur im Einzelfall treffen. Die Beurteilung hängt ganz stark von der Menge der personenbezogenen Daten, insbesondere der Verarbeitung sensibler Daten, ab.

l) Frage: Der Vermittler bekommt Daten und leitet diese an Partner (Versicherung, WPF) zur Abwicklung weiter. Oder er erfasst diese Daten direkt im System des Versicherer oder WPF. Wer haftet für die Daten? Wer muss Auskunft (dem Kunden etc.) geben?
Antwort: Insbesondere im Bereich der Versicherungswirtschaft, aber auch im Bereich der Finanzdienstleistungsunternehmen, werden Kundendaten vom Vermittler erfasst und in der Folge an das Versicherungs- oder Wertpapierdienstleistungsunternehmen weitergegeben oder in dessen System eingespielt.

Hier haften Makler (vertraglich und deliktisch) und Agent (deliktisch) dem Kunden gegenüber für die weitere Verwendung der Kundendaten bei den Versicherungsunternehmen. Der Versicherungsmakler wird daher in seine Verträge mit den Versicherungsunternehmen ebenso wie die Versicherungsagenten in ihre Agenturverträge entsprechende Vertragsbestimmungen zur Absicherung, Übernahme der Haftung, Schad- und Klagloshaltung mit den Versicherungsunternehmen aufzunehmen haben.

Ansprechpartner für die Kunden betreffend Auskunft- und Löschwünschen ist der Vermittler.

m) Frage: Wie erfülle ich meine **Informationspflichten** aufgrund der DSGVO?
Eigene Datenschutz-, Cookie-Erklärung, Kontakte zu Dritten..

Dieser Punkt sprengt den Rahmen der FAQs und wird wahrscheinlich im nächsten BAV-Newsletter im Detail beantwortet werden (denn die DSGVO hört mit dem 25.5.2018 nicht auf…).

Ein paar Punkte zum Gegenchecken:

- **Eigene Datenschutzerklärung** (wie erfüllt das Unternehmen die DSGVO, was wird gespeichert, wie lange etc.) ist online zu stellen.
  Tipp: Leicht auffindbar auf der Homepage, in leicht verständlicher Sprache
- **Cookie-Strategie** ist online bekannt zu geben und vor dem Einstieg des Nutzers ein Ja oder Nein („keine Cookies") einzuholen. Technische Cookies werden wohl erlaubt bleiben, Tracking-Cookies sind bedenklich.
- **Auskunftsbegehren:** Binnen einem Monat zu beantworten! Welche Daten wurden gefunden, aufgrund welchen Rechtsgrunds sind sie gespeichert, wann wird gelöscht etc. Und am Ende ist eine Belehrung über die Rechte (Auskunft, Berichtigung etc.) und Beschwerdemöglichkeit anzugeben.
  Tipps: Keine Auskünfte an Unberechtigte geben (Identitätsnachweis einholen).
  Auch Leermeldungen sind abzugeben („keine Daten gefunden"), um zu verhindern, dass der Anfrager sich ignoriert fühlt und sich bei der Behörde beschwert (was diese als Grund für eine Vorortkontrolle nutzen könnte).
- **Löschbegehren:** Hier gilt Analoges wie beim Auskunftsbegehren. Allerdings müssen Sie noch ergänzen, ob und was Sie löschen. Bzw. was Sie nicht löschen dürfen (weil etwa eine steuerliche Aufbewahrungsfrist dagegen spricht).
  Tipp: Auch Ihr Recht, Daten aufzubewahren, um sich gegen eventuelle Schadenersatzansprüche freibeweisen zu können, ist hier zu dokumentieren.
- **Data Breach-Auskünfte:** Wenn etwa durch einen **Hacker-Angriff oder Verlust** von Laptop etc. die Möglichkeit besteht, dass personenbezogene Daten in fremde Hände fallen könnten, dann sind davon die Datenschutzbehörde und die Betroffenen zu informieren. Mit Hinweisen, was passiert ist und welche Gefahr drohen könnte (etwa gleiche Kombination aus Benutzernamen und Passwort wird woanders auch verwendet).

n) Frage: Sind USB-Sticks künftig noch erlaubt? Bekanntlich kann man auf diesem Wege ganz einfach Viren verteilen und damit Systeme zum Absturz bringen. Auch verliert man sie leicht. Was, wenn darauf personenbezogene Daten gespeichert sind?

Antwort: Jedes Unternehmen muss selbst entscheiden, ob die Nutzung von USB-Sticks erlaubt bleibt. Sie sind praktisch, weil man damit leicht Daten verteilen kann. Aber auch riskant. Den Verlust von Daten kann man vermeiden, indem man den USB-Stick – z.B. mit dem Windows-eigenen Bitlocker-Programm – verschlüsselt. Die Gefahr, durch das Anstecken eines USB-Sticks einen Virus oder Trojaner ins System einzuschleusen, kann man dadurch nicht ausschalten.
Sollte ein unverschlüsselter USB-Stick verloren gegangen sein, ist das Data Breach-Prozedere abzuarbeiten, das wir unter „Data Breach" bei den „Informationspflichten" beschrieben haben.

o) Frage: Gilt die DSGVO nur für elektronische Datenverarbeitung oder auch für Papier-Akten?

Antwort: Wenn die Papier-Akten **nach einem System aufbewahrt** werden, fallen sie auch unter die DSGVO. Kann ich etwa in einem Aktenschrank nach dem Namen suchen und die Akte finden, dann gilt die DSGVO. Mache ich mir Notizen auf einem Zettel und lege diesen in einer Schachtel unsystematisch ab, gilt hierfür die DSGVO nicht.

Recherche-Quellen: Mag. Günter Wagner, B2B-Projekte, Mag. Georg Markus Kainz, Quintessenz und RA Mag. Stephan Novotny (Spezialgebiet Versicherungen & Datenschutz-Grundverordnung), diverse Homepage-Seiten der WKO zum Thema Datenschutz, Praxishandbuch „Das österreichische Versicherungsvermittlerrecht" (wurde gerade auf Stand 2018 aktualisiert, Details dazu hier…)