MITTWALD
Webhosting. Einfach intelligent.

DSGVO-Webinar

Mit Johannes Schrader, Stefan Wolfarth, Reidar Janssen & Jan Meyer

www.mittwald.de

Ziele des Webinars

- Grundlegender Überblick über die Herausforderungen der DSGVO
- Fokus auf Bedürfnisse von Agenturen und Freelancern
- Akzente bei AV-Verträgen und TOM
- Detaillierte Informationen in unserem *Wissenspaket für Agenturen*
- Webinar stellt keine Rechtsberatung dar

DSGVO Themen

Grundbegriffe:

1. Personenbezogene Daten

- Der Ausdruck „personenbezogene Daten“ (pbDaten) bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Vor- und Nachname
Geburtsdatum / Alter
Postanschrift
E-Mail-Adresse
Telefonnummer
Personalausweisnummer
Reisepassnummer
Sozialversicherungsnummer
KFZ-Kennzeichen
Bankverbindung
Kreditkarteninformationen
Zeugnisse
Foto (z. B. Profilfotos)
Unterschrift
Zugangsdaten (Benutzername inkl. dazugehörigem Dienst)
IP-Adresse

Grundbegriffe:

2. Verarbeitung personenbezogener Daten

- Als „Verarbeitung“ sind lt. DSGVO unter anderem Verfahren zu verstehen, die Daten erfassen, speichern, verwenden, verändern, sortieren, übermitteln, verbreiten, löschen oder veröffentlichen.
- Beispiele: Nutzung von Zahlungsdienstleistern, Durchführung von Datensicherungen, Newsletter-Versand…

Grundbegriffe:

3. Verantwortlicher

- Der Ausdruck „Verantwortlicher“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von pbDaten entscheidet.

- Kurz: Derjenige, der die Verarbeitung von pbDaten veranlasst.

Grundbegriffe:

4. Auftragsverarbeiter

- Der Ausdruck „Auftragsverarbeiter“ bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die pbDaten im Auftrag des Verantwortlichen verarbeitet.
- Kurz: Auftragsverarbeiter ist, wer sich für einen anderen um dessen pbDaten kümmert.
- Beispiele aus dem Agenturbereich: Druckereien, Webhoster, Anbieter von Buchhaltungssoftware…

Datenschutzprinzipien

- Rechtmäßigkeit → Verarbeitung mit Rechtsgrundlage
- Verarbeitung nach Treu und Glauben → Verarbeitung ohne Täuschung
- Transparenz → Verarbeitung muss für betroffene Person nachvollziehbar sein
- Zweckbindung → Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke
- Datensparsamkeit → Verarbeitung beschränkt auf das zweckgebundene, notwendige Maß
- Richtigkeit → Daten sind sachlich korrekt und auf dem aktuellen Stand
- Speicherbegrenzung → Daten sind frühestmöglich zu löschen
- Integrität und Vertraulichkeit → Datensicherheit durch technisch organisierte Maßnahmen
- Rechenschaftspflicht → Oben genannte Punkte nachgewiesen und dokumentiert

- Privacy by Design → Sicherstellung des Datenschutzes durch technische Maßnahmen
- Privacy by Default → Sicherstellung des Datenschutzes durch datenschutzfreundliche Voreinstellung

Voraussetzungen für Datenverarbeitung

- Grundsätzlich ist Datenverarbeitung verboten, es sei denn:
- → Rechtliche Verpflichtung (z.B. Aufbewahrungspflicht gem. HGB oder AO) *oder*
- → Erfüllung eines Vertrags bzw. vorvertraglicher Maßnahmen (z.B. für Onlineshop Lieferadresse) *oder*
- → Berechtigtes Interesse (z.B. für Online Marketing) *oder*
- → Einwilligung

Zusätzlich: Die Datenschutzprinzipien werden eingehalten

Einwilligung

- Muss freiwillig erfolgen
- Auf einen bestimmten Fall beschränkt
- UND unmissverständlich sein
- Information des Einwilligenden über Widerrufsrecht, Nennung des Verantwortlichen und des Zwecks der Datenverarbeitung
- Nachweisbarkeit der Einwilligung durch Protokollierung und *Double Opt-In*
- Kann widerrufen werden
- Mindestalter des Einwilligenden in DE ist 16 Jahre
- Kopplungsverbot

Betroffenenrechte

- Auskunft
- Berichtigung
- Löschung
- Datenübertragbarkeit
- Widerspruch
- Einschränkung der Verarbeitung

Informations- und Meldepflichten

- Datenschutzerklärung
- Impressum
- Meldepflichten bei „Datenpannen“

Datensicherheit

- Vertraulichkeit → z.B. Zugriff nur durch Berechtigung
- Integrität → z.B. Schutz vor ungewollten Veränderungen und Manipulationen
- Verfügbarkeit und Belastbarkeit → z.B. Erstellen von Backups
- Transparenz → z.B. Trennbarkeit von Daten

Dokumentationspflichten

1. Verzeichnis der Verarbeitungstätigkeiten (VV)

- Wer ist für die Verarbeitung der pDaten intern zuständig?
- In welchem Ausmaß und warum werden die pDaten (Umfang, Art, Zweck) verarbeitet?
- Welche Kategorien von pDaten werden verarbeitet?
- Welche Kategorien von Personen sind betroffen?
- Wem werden die pDaten zur Verarbeitung bereitgestellt?
- Warum ist die Verarbeitung der pDaten gerechtfertigt?
- Bleiben die pDaten innerhalb der EU?
- Wann werden die pDaten wieder gelöscht?
- Wie werden die pDaten geschützt?

Dokumentationspflichten

2. Technische & organisatorische Maßnahmen (TOM)

- Welche Maßnahmen werden ergriffen, um die Daten zu schützen?
- Beispiele: Pseudonymisierung von Daten, Unterweisung der Mitarbeiter in Datenschutz, Zugriffskontrollen und -beschränkungen für Daten, Firewalls, Virenscanner, USV
- Dokumentation aller Maßnahmen in dem Dokument

Dokumentationspflichten

3. Auftragsverarbeitungs-Verträge (AV-Verträge)

- Regeln den sicheren Umgang mit den Daten, die der Auftragnehmer zur Verarbeitung nach Weisung erhalten hat
- Auch elektronisch abschließbar
- Agentur schließt AV-Verträge mit Dienstleistern und Kunden

- Beispiel AV-Vertragskette:

Mittwald <-> Agentur, Agentur <-> Auftraggeber

→ Agentur ist je nach Verhältnis Auftragnehmer oder Auftraggeber

Dokumentationspflichten

4. Überprüfung vorliegender Erlaubnistatbestände

Alte vorliegende Einwilligungen dürfen weiter eingesetzt werden, wenn sie den Anforderungen der DSGVO entsprechen:

- Freiwilligkeit
- Hinweis auf Widerrufsrecht
- Kein Verstoß gegen Kopplungsverbot
- Nicht mit vorangekreuzten Checkboxen entstanden

Datenschutzbeauftragter

- Erforderlichkeit: Mindestens 10 Personen sind ständig mit Verarbeitung pbDaten beschäftigt
- Intern oder Extern: Interner Mitarbeiter kein Mitglied der Geschäftsführung oder leitender MA für EDV oder Personal
- Besonderer Kündigungsschutz des internen Datenschutzbeauftragten
- Nennung des Datenschutzbeauftragten in der Datenschutzerklärung mit Name und Kontaktdaten

Fazit

- Es gibt selten schwarz und weiß im Datenschutz und oft keine klaren Antworten: Gesunder Menschenverstand und vernünftiges Abwägen ist angesagt.
- Zuerst den „Außenputz“ (Datenschutzerklärung, Impressum, Cookie-Hinweise), dann die internen Prozesse angehen.
- *„Ich schaff‘ das nicht mehr rechtzeitig bis zum 25.05.18!“* Doch! Es ist nicht zu spät, die wesentlichen Herausforderungen der DSGVO zu meistern.
- *„Ab dem 25.05.18 hat sich das Thema Gott sei Dank erstmal erledigt!“* Nein! Nach dem 25.05.18 hört das Thema nicht auf, sondern setzt sich als kontinuierlicher Prozess fort.

Vielen Dank für Ihre Aufmerksamkeit!