Datenschutz für die Praxis-

Was jeder Unternehmer für die DSGVO umsetzen muss

WORUM GEHT ES ÜBERHAUPT?

Im Datenschutzrecht geht es um personenbezogene Daten von privaten Nutzern

Einer bestimmten Person zuordnungsfähig:

- Name
- Anschrift
- E-Mail-Adresse,
- Telefonnummern
- Einkommen, Beruf
- Hobbys
- Personalausweisnummer
- Sozialversicherungsnummer
- Ausbildung
- Familienstand
- Geburtsdatum
- KFZ-Kennzeichen
- Kaufhistorie
- Klickhistorie einzelner Nutzer
- IP-Adresse von Nutzern

Sensible Daten

- Zahlungskonten,
- Kontodaten
- Benutzerkennungen,
- Passworte

Die Verarbeitung folgender Daten ist untersagt:

- Rasse und ethnische Herkunft
- politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse und weltanschauliche Überzeugungen
- Genetische und biometrische Daten einer Person
- Gesundheitsdaten
- Daten über die sexuelle Orientierung

DIE BASIS:

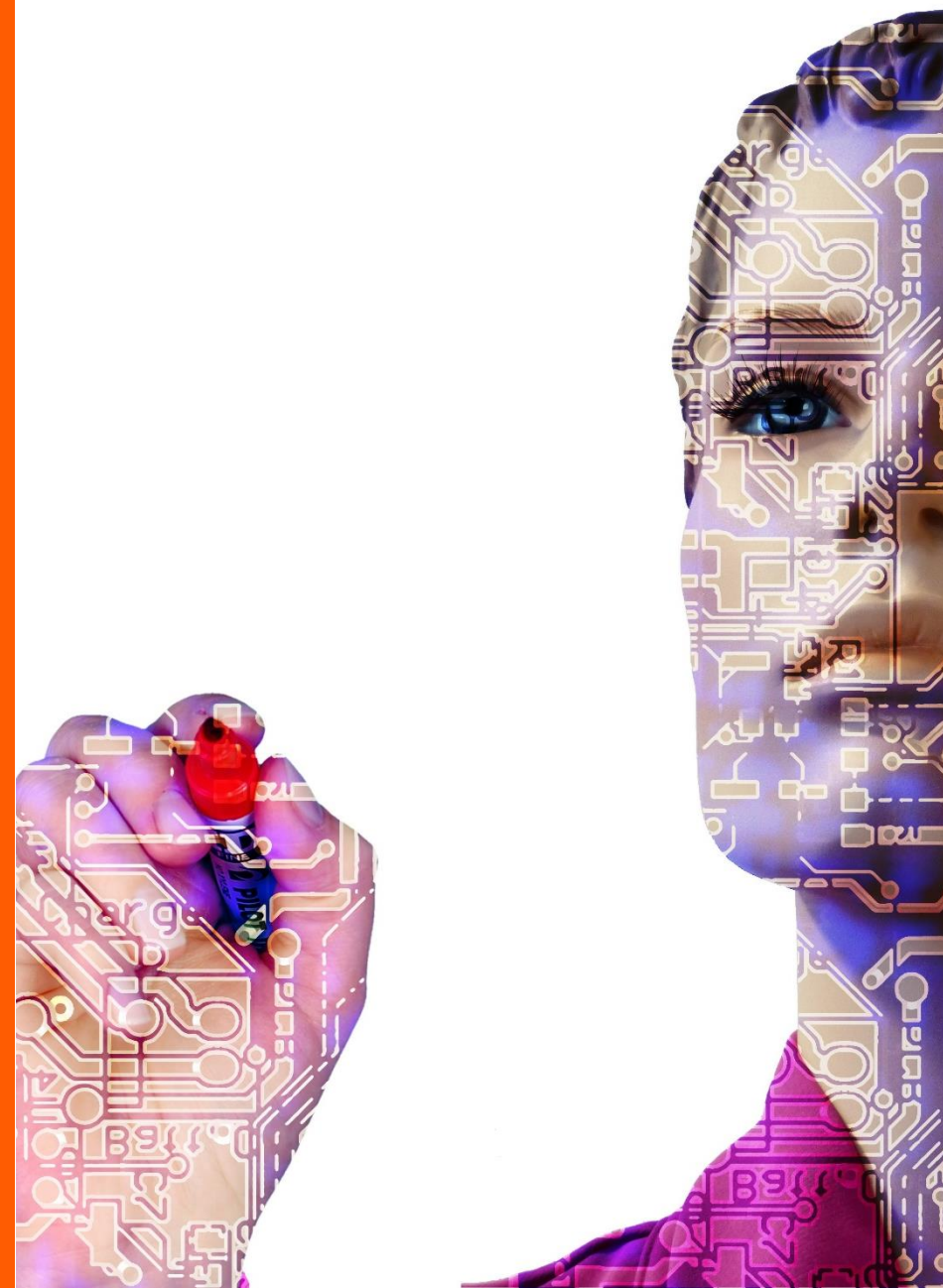
Die Verarbeitung personenbezogener Daten ist laut DSGVO verboten

Grundsätzlich gilt, dass Datenverarbeitung verboten ist, sofern sie nicht gesetzlich erlaubt oder von einer Einwilligung des Betroffenen gedeckt ist *(sog. Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG: „nur“ zulässig …),* sie bedarf also immer einer Rechtsgrundlage oder Einwilligung.

§53 BDSG

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

= Vereinbarungen zum Datengeheimnis

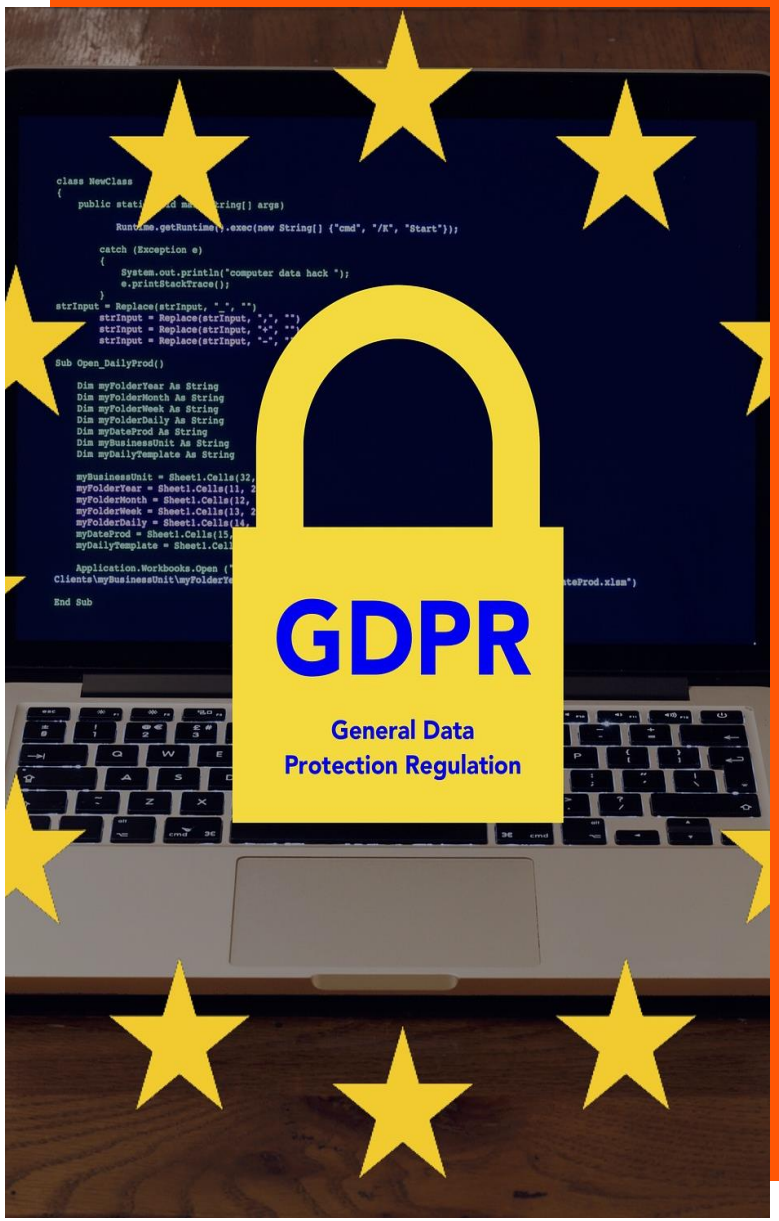


DIE ROLLEN

BETROFFENE	VERANTWORTLICHE	VERARBEITER
natürliche Personen, deren Daten zu schützen ist	Personen, Unternehmen oder Organisationen, die personenbezogene Daten erheben, speichern, verarbeiten oder nutzen	Personen, Unternehmen oder Organisationen, die im Auftrag personenbezogene Daten erheben, speichern, verarbeiten oder nutzen
Ihr Gast / Kunde Sie selbst Ihr Kollege oder Mitarbeiter	Unternehmen, die personenbezogene Daten nutzen und/ oder im Internet tätig sind	Software-Dienstleister, die im Auftrag von Unternehmen die Daten speichern und verarbeiten: Shop-Software, Tracking-Software, Kundendatenbank, Finanzbuchhaltungs-Software, Lohnsoftware, Bewertungsassistent, UCC-Software, Hosting-Dienstleister u.a.

NEU MIT DER DSGVO

- Pflicht zur Führung eines Verzeichnisses aller Datenverarbeitungstätigkeiten
- Dokumentationspflichten und Datenschutzfolgenabschätzung
- Neue Vorgaben für Einwilligungserklärungen online und offline
- Erweitere Vorgaben für Datenschutzerklärungen auf Webseiten
- Pflicht zur Datenportabilität (Gemeint ist das Recht einer Person, ihre personenbezogenen Daten bei einem Anbieterwechsel mitzunehmen)
- “Recht auf Vergessen werden” von Nutzerdaten
- „Recht auf Auskunft“
- Neuregelungen bei der Auftragsdatenverarbeitung



NEU MIT DER DSGVO

- Neuregelungen bei Mitarbeiterdaten
- Privacy by design und privacy by default
- Personenbezogene Daten von Kindern bis 13 Jahren
- Prinzip des "One-Stopp-Shop”
- Stellung des Datenschutzbeauftragten
- Meldepflicht von "Datenpannen”
- Neue Haftungsregeln und höhere Bußgelder

BUßGELDER BEI VERSTÖßEN

Es soll weh tun!

Bußgelder nach Artikel

83 und 84 der DSGVO:

WAS IST ZU TUN?

ANALYSE DER DATEN UND DATENSCHUTZPROZESSE

- Datenbestand, welche personenbezogenen Daten liegen vor?
- Welche Daten nutzen Sie tatsächlich?
- Welche Daten dürfen Sie rechtmäßig nutzen?
- Welche Daten dürfen Sie rechtmäßig weitergeben?
- Was sind die Datenquellen?
- Welche Daten erheben Sie rechtmäßig?
- Welche Daten dürfen Sie zu welchen Zwecken nutzen?
- Welche Daten dürfen verbundenen Unternehmen rechtmäßig zur Verfügung gestellt werden?

UMSETZUNG DER DSGVO VORGABEN

- Bereinigung nicht genutzter Daten
- Bereinigung unrechtmäßig erhobener Daten
- Prüfen Sie Vertragsarten mit Auftrags-Datenverarbeitern
- Erstellen Sie einen Maßnahmenplan, der folgendes festlegt:
  - welche Daten werden künftig gespeichert
  - wie lange
  - wie werden Einwilligungen eingeholt?
  - wie werden Mitarbeiter geschult und informiert?

AUFBAU GEEIGNETER DATENSCHUTZ MANAGEMENT PROZESSE

- Erfüllung gesetzlicher Vorgaben
- Bestimmung Datenschutzbeauftragter, IT-Sicherheitsbeauftragter
- Erstellung einer betrieblichen Datenschutzrichtlinie
- Inkl. Beschreibung der Schritte und Fristen in Notfällen (unrechtmäßige Datenweitergabe durch Fehlversendung, Diebstahl, Hacking)
- Beschreibung aller Maßnahmen zur Umsetzung des BDSG und der DSGVO und Festlegung der Verantwortlichen

PFLICHT FÜR ALLE VERANTWORTLICHEN: VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Liste aller Fachverfahren und Software-Anwendungen aufzustellen,
die personenbezogene Daten verarbeiten

DGSVO VERZEICHNIS VERARBEITUNGSTATIGKEITEN

Betrieb:	
Name des Verantwortlichen	
Kontaktdaten Verantwortlicher:	

Bezeichnung der Verarbeitungstätigkeit (z.B. Reservierung, Check In, Kontaktanfrage, Angebotsanfrage, Tischreservierung, Gutscheinverkauf, Newsletter-Abo etc.)	Zweck der Verarbeitung (z.B. Vertragserfüllung, Pfichten aus Steuer/ Meldegesetz, Marketing, Versand Angebot…)	Betroffenen-kreise	Datenkategorien (z.B. Adressdaten, Kontaktdaten, Zugriffsdaten, Bewerberdaten, Mitaberbeitervertragsdaten, Aufenthaltsdaten etc.)	Sensible Daten	Speicherdauer der Datenkategorie (Löschzeiten)	Empfängerkreise (z.B. Bewertungsassistent, Hotelsoftware CRS des Franchise Gebers, Zahlungsdienstleister etc.)	Wer hat Zugang? (Mitarbeiter, Mitarbeiter des Dienstleisters, Berater etc.)	Transfer in Länder außerhalb EU (z.B. Google oder Franchisegeber)	Beschreibung der Datensicherungsmaßnahmen um Hacking (Verlust), Veränderung, unautorisierten Zugang zu verhinden. (Organisatorische und technische Maßnahmen, z.B. Verschlüsselung, Datenschutzvereinbarung mit Mitarbeitern/ Dienstleistern etc.)

LISTE AUFTRAGSVERARBEITER

Datenkategorien	Art der Speicherung (Analog/ digital)	Ort der Speicherung (Server im Betrieb, Rechenzentrum des Softwarepartners, Ordner im Reservierungs- oder Personalbüro etc.)	Name Software der Speicherung (Property Management, Bewertungsassistent, Newslettertool, Booking Engine, Channel Manager, Hosting Webseite, Telefonanlage, Zeiterfassung, CRM, Lohnbuchhaltung etc.) oder des Dienstleisters	Kontaktdaten für Datenschutz beim Softwarepartner oder Dienstleister	Liegt Datenschutz-vereinbarung vor? Ist sie angefordert?	Liegt Auftrags-datenverar-beitungs-erklärung vor (Technische und organisatorische Schutzmaßnahmen)	Automatisierte Löschvorgänge, wie?	Ist der Dienstleister in der Daten-schutzerklärung aufzuführen? Erledigt?
Adress- und Kontaktdaten digitaler Buchender, Aufenthaltsdaten, Webtracking	digital	Rechenzentrum Webseiten Hoster und Rechenzentrum	Marketingbetreuung, Web-Redakteur	Gabriele Schulze, Ulmenallee 26, 14050 Berlin gs@marketing4results.de	übersendet	übersendet	Webanalyse 14 Monate, Bucherdaten bis 7 Tage nach Abreise	nein

AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

- Bildschirmschutz nach 5 min
- Eingegangene Post oder sonstige Dokumente mit personenbezogenen Informationen in verschließbaren Schränken lagern
- Prozesse für Einwilligungen definieren, damit personenbezogene Daten über den Aufenthalt hinaus gespeichert werden dürfen
- Einwilligungen dokumentieren (und aufbewahren)
- Aufnahme von Kundenwünschen (Allergien, Konfektionsgrößen etc.) in der Kundendatenbank bedarf der ausdrücklichen Zustimmung des Kunden
- Weisung an Mitarbeiter: Auskünfte über Kunden dürfen nicht gegeben werden (es sei denn der Kunde stimmt zu)

AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

Bestellannahme / Onlineshop

- Daten dürfen im Rahmen der vorvertraglichen Geschäftsverhältnisse verarbeitet werden, sind aber z.B. bei kostenfreier Stornierung wieder zu löschen.
- Online-Shop sendet die Daten verschlüsselt (https)
- Informationspflicht über Datenschutzerklärung auf Webseite und in allen Buchungsprozessen.
- Dienstleister muss auch in Datenschutzerklärung der Webseite aufgeführt sein.
- Passwortmanagement im Angebot/ Vertrag über die Datenverarbeitung informieren.
- Kundenakten unter Verschluss halten (oder gar nicht mehr anlegen/ ausdrucken)
- Nie Kreditkartendaten per E-Mail versenden (feste Vorgaben zum Umgang mit Kreditkarten)

Kreditkartendaten:

- Nach **Kaufprozess** löschen oder verschlüsseln
- **Optimal:** Tokenisation durch Zahlungsdienstleister
- Benutzerrechte auf Kreditkartendaten stark einschränken
- Ausgedruckte Kreditkartendaten unter Verschluss aufbewahren

Besondere Meldepflicht gegenüber Datenschutzbehörde, wenn es zum Missbrauch oder Diebstahl von Kreditkartendaten gekommen ist.

AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

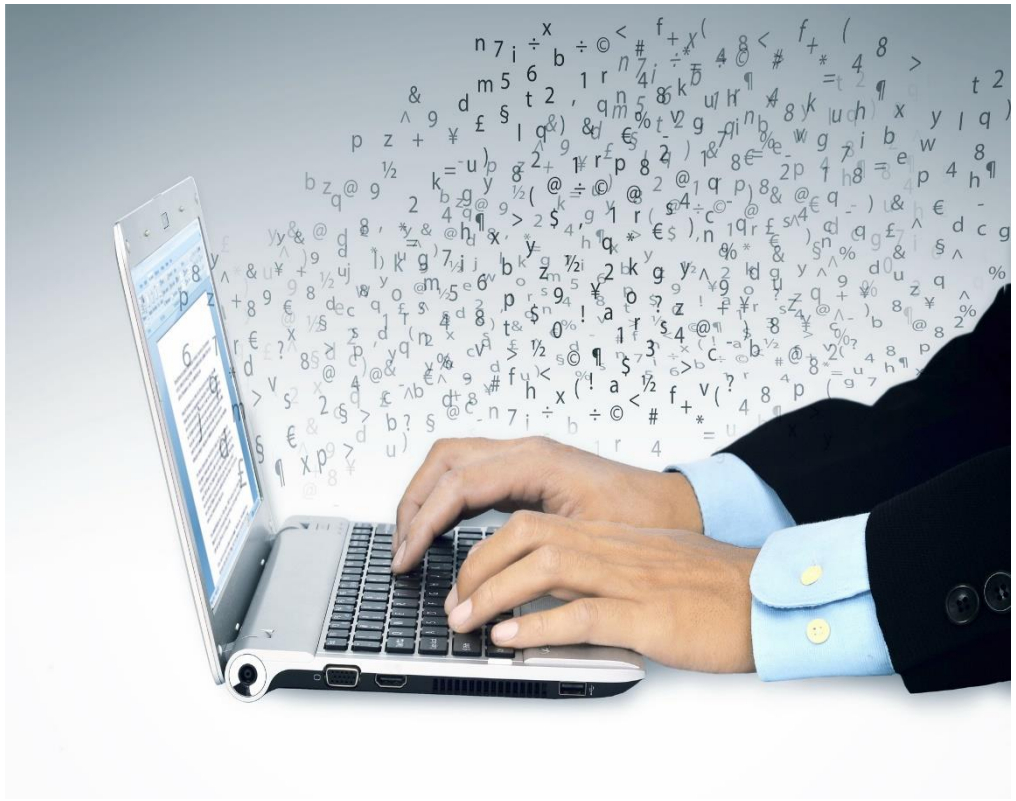
Webmaster/ E-Commerce/ Marketing

- Webseitencheck (Cookie-Warnung, Datenschutzerklärung, keine unnötigen Daten verarbeiten, Kommentare und Formulare mit Einverständnis versehen etc.)
- Datenschutzerklärung
- Prozesse Newsletter – Kommunikation – Erlaubnis nachweisen, Widerspruch umsetzen
- Altdaten bereinigen
- Social Media Marketing datenschutzkonform gestalten
- Bewertungsmanagement datenschutzkonform gestalten
- Kundenbindungsprogramme prüfen
- Gewinnaktionen und Verlosungen prüfen
- Trackingsysteme datenschutzkonform einsetzen

AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

EDV - IT

- Sicherung (physisch und digital) der Standorte von Servern auf denen personenbezogene Daten gelagert werden. Zugangs- und Zutrittskontrolle Serverraum. (TOM umsetzen und dokumentieren)
- Abschluss von Datenschutzvereinbarungen und Auftragsdatenverarbeitungserklärungen mit allen Dienstleistern, die Zugang zu den Daten haben (auch Fernwartung).
- Prozesse zur Löschung, wenn Zeck entfällt und keine Einwilligung vorliegt.
- Genaue Steuerung welche Mitarbeiter auf welche Daten Zugriff haben.
- Implementierung eines sicheren Passwortmanagements und Benutzerrechten
- Sicherstellung, dass alle Aktivitäten der Benutzer protokolliert werden
- Belehrung der Benutzer (IT-Richtlinie), dass sie sich abmelden, wenn sie ihren Arbeitsplatz verlassen und Passwörter nicht weiter geben dürfen.



AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

Personal

Gemäß § 26 BDSG-neu darf der Arbeitgeber alle Daten der Beschäftigten erheben, die für die Entscheidung

- über die Begründung eines Beschäftigtenverhältnisses oder nach Begründung
- des Beschäftigungsverhältnisses
- für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.
- Dies umfasst insbesondere alle Informationen zu Qualifizierung inklusive Arbeitszeugnisse, Daten zur Identifizierung (z.B. Personalausweisnummer, Geburtsdatum), und Personenstand
- Vorsicht bei Bewerbern unter 16 (Schülerpraktika) – Verarbeitung nur bei Einwilligung der Eltern

- ✓ Unterlagen abgelehnter Bewerber nach 6 Monaten löschen (Löschkonzept)
- ✓ Zugriffskontrolle und Zugangskontrolle Personalakten (wie?)
- ✓ Arbeitsrechtliche Unterlagen ehemaliger Mitarbeiter nach 10 Jahren vernichten
- ✓ Verschwiegenheitserklärungen für alle Mitarbeiter, die personenbezogene Daten verarbeiten
- ✓ Datenschutzbestimmungen zum Umgang mit Bewerberdaten erstellen und aus Jobbereich der Webseite verlinken
- ✓ Vereinbarung zur privaten Nutzung von Telefon und Internet abgeschlossen? Falls nein, nachholen (Empfehlung: private Nutzung verbieten)
- ✓ Verschlüsselte Übertragung der Bewerbungsunterlagen ermöglichen (Formular mit Upload Möglichkeit)

AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

Buchhaltung

In der Personalabteilung und Buchhaltung werden die sensibelsten Daten verarbeitet. Entsprechend sind die Räumlichkeiten und digitalen (und analogen) Speicherorte zu sichern.

- Aktenschränke abschließbar, Schlüssel nur berechtigten Personen aushändigen
- abschließbare Büros, abgeschlossen, wenn kein autorisierter Mitarbeiter im Büro ist
- Keine frei zugänglichen Postfächer für personenbezogene Daten oder Gehaltsabrechnungen nutzen
- Räumlich getrennte Drucker

AUFGABEN UND MAßNAHMEN NACH BETRIEBSBEREICHEN

Einkauf

- Falls Lieferanten personenbezogene Daten erhalten (u.a. Lettershop) lassen Sie sich schriftlich im Vertrag oder als Zusatzvereinbarung zusichern, dass der Lieferant keine Daten an Dritte weitergibt und verlangen Sie eine ADV (Auftragsdatenverarbeitungs-Vereinbarung).

REVISION ALLER VERTRÄGE MIT AUFTRAGSDATENVERARBEITERN

Führen Sie eine Revision aller Verträge mit Dienstleistern durch, die von Ihnen personenbezogene Daten bekommen:

- Auftragsverarbeiter dürfen nur Personen bei der Verarbeitung einzusetzen, die zur Verschwiegenheit vertraglich oder gesetzlich verpflichtet sind.
- Der Auftragsverarbeiter hat alle sich jetzt aus Art. 32 DSGVO ergebenden erforderlichen technisch-organisatorischen Maßnahmen zu ergreifen.
- Festlegung, was mit den Daten bei Vertragsende passiert (Rückgabe, Vernichtung).
- Auftraggeber muss Kontrollen durchführen können. Verstöße gegen das Datenschutzrecht müssen der Datenschutzaufsichtsbehörde des Bundeslandes, in dem das Unternehmen sich befindet, unverzüglich nach dem Bekanntwerden gemeldet werden.

WICHTIG ZU WISSEN

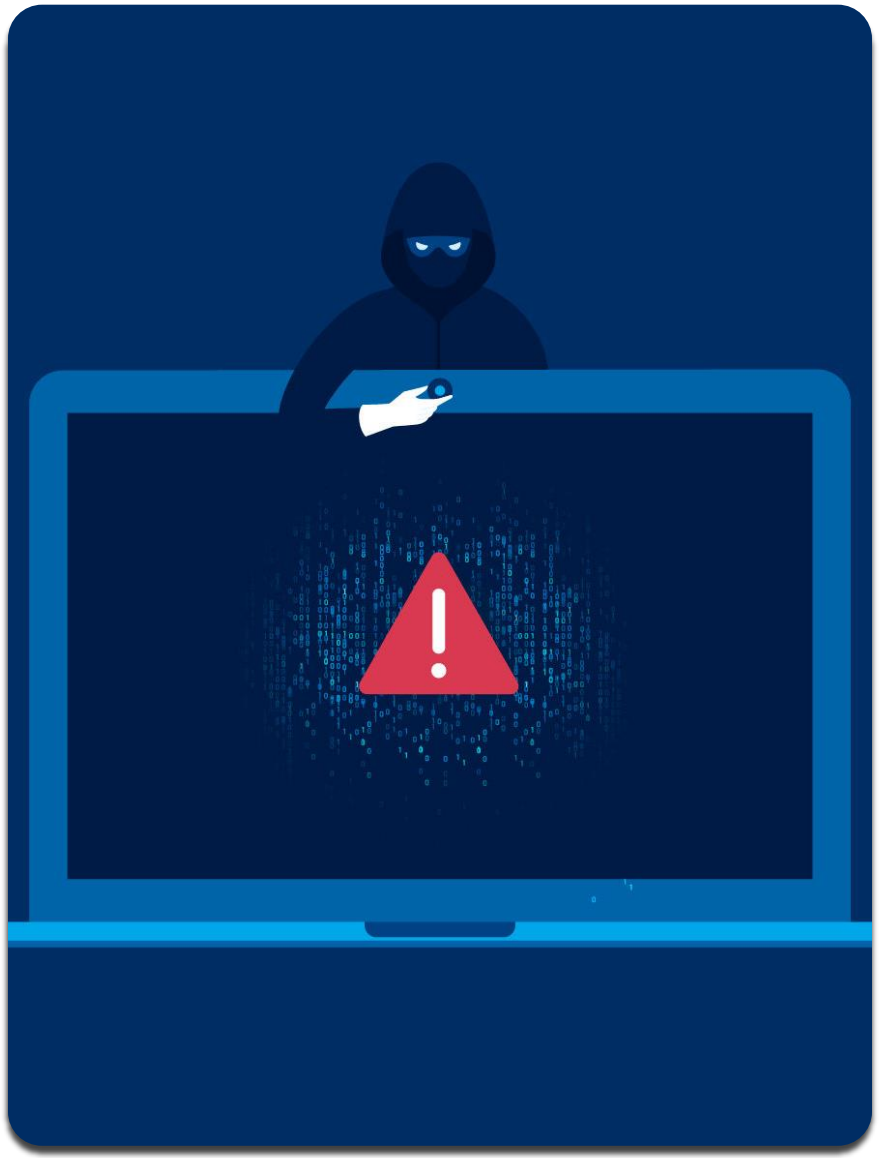
- Laut UWG §7 (Gesetz gegen den unlauteren Wettbewerb) dürfen Sie personenbezogene Daten von Kunden (nicht Interessenten) speichern, die zum Vertragsabschluss nötig waren (Name, Adresse, Tel, Aufenthalt, gebuchtes Zimmer). z.B. : auch die E-Mailadresse **(wenn Sie sie durch den Vertragsabschluss erhalten haben)**. Dann dürfen Sie diese Daten auch für E-Mailings nutzen.
  - das gilt auch für alle Personen, die schon Kunde sind. Aufbewahrung, maximal 10 Jahre nach letztem Vertragsabschluss

- Post-Sales, z.B. Bewertungseinladung: Eigentlich gibt es dafür keine Rechtsgrundlage. Aber: es gibt eine aktuelle Kammergerichtsentscheidung Berlin: Innerhalb von zwei Wochen nach dem Aufenthalt darf eine Bewertungseinladung (die ansonsten werbefrei ist) versendet werden
  - Pre-Stay: jederzeit erlaubt, da es zur vorvertraglichen Kommunikation gehört

WICHTIG ZU WISSEN

Dürfen Sie einen Zechpreller in der CRM-Software als solchen markieren?

ja, aber verwenden Sie ein Symbol oder einen Code, dessen Bedeutung nur dem Kundenmanager und der Geschäftsleitung bekannt ist



WICHTIG ZU WISSEN

Was ist, wenn Sie erfahren, dass personenbezogene Daten gestohlen und aus Versehen oder durch einen Hack angegriffen werden?

- Sofortige Schutzmaßnahmen
- Sofortige Information an die Landesdatenschutzbehörde: https://www.datenschutz-berlin.de/wirtschaft-und-verwaltung/meldung-einer-datenpanne/datenpannenformular
- ggf. Sofortige Informationen der Betroffenen, falls dadurch Schaden abgewendet oder minimiert werden kann

Nicht öffentliche Stellen:

Darüber hinaus besteht nach § 38 BDSG (neu) eine Bestellpflicht, soweit der Verantwortliche oder der Auftragsverarbeiter mit ***mindestens 20 Personen*** *ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.*

WORÜBER MÜSSEN SIE IHREN DATENSCHUTZBEAUFTRAGTEN INFORMIEREN?

- Sie planen die Einführung einer neuen Software oder einen Vertrag mit einem neuen Dienstleister (z.B. Outsourcing Buchhaltung), durch den personenbezogene Daten verarbeitet werden
  - ✓ Auftragsdatenverarbeitungserklärung anfordern und an DBA senden
- Wenn Sie neue personenbezogene Daten erstmalig verarbeiten wollen, z.B. Mitarbeiterbilder auf der Webseite veröffentlichen, Ihren Parkplatz mit einer Videoüberwachung ausstatten möchten o.ä.
- Geplante Änderung von Datenverarbeitungsverfahren
- Beschwerden/ Anfragen von Gästen, Behörden oder Verbraucherschutzvereinen
- Verlorene, zerstörte, gestohlene Daten (umgehend)

Meldung von Datenpannen in Berlin:
https://www.datenschutz-berlin.de/wirtschaft-und-verwaltung/meldung-einer-datenpanne/datenpannenformular

VORSICHT BITTE

- Eine Person oder eine Behörde (oder eine Verbraucherschutzorganisation) verlangt Auskunft über Datenschutzangelegenheiten oder zu personenbezogenen Daten von Gästen oder Mitarbeitern. Bestehen Sie auf ein schriftliches Auskunftsersuchen mit Angabe der Rechtsgrundlage für die Auskunft. Und informieren Sie sofort den Datenschutzbeauftragten.
- Geben Sie telefonisch keine Auskunft über Gäste oder Kunden
- **Lassen Sie NIEMALS Listen mit personenbezogenen Daten öffentlich einsehbar liegen** *(Teilnehmer Kundenevent, Besteller zum Abholen etc.)*
- Gäste haben ein Auskunftsrecht (nur über sich selbst!!) – Sie müssen sichere Verfahren nutzen, um sicherzustellen, dass der Anfragende der Betroffene ist.

VORSICHT BITTE

Das Öffnen von Mailanlagen, insbesondere das Aktivieren von Dokumenten ist gefährlich

- Nur aus sehr verlässlichen Quellen
- Ansonsten um Inhalte in Outlook bitten

Hacker sind kreativ:

Gefakte Bewerbungen

Gefakte Aufträge

UNTER STRAFE STEHEN

Jede Person hat die Möglichkeit z.B. bei Verbraucherschutz-Verbänden oder seinen Anwalt einen Verstoß zu melden:


IHRE FRAGEN

Danke fürs Zuhören

… und vielleicht für eine Bewertung bei Google oder Facebook?

Gabriele Schulze
gs@marketing4results.de
Tel. +49 (0)30 23 13 73 64