Themenübersicht

Geldwäschegesetz (GWG)

- Grundsätze
- Bareinzahlungen
- Risikofaktoren
- Umgang mit Ausweiskopien

DSGVO Datenschutzgrundverordnung

- Grundsätze
- Konkrete Umsetzung in der Agentur
- Integrität und Vertraulichkeit
- Rechtsfolgen und Risiken
- Umgang mit Betroffenenrechte

Fragen der Teilnehmer

Geldwäschegesetz (GWG) - Definition

Geldwäsche

Unter Geldwäsche versteht man das **Einschleusen illegaler Vermögenswerte in den Wirtschaftsreislauf**. Dadurch sollen sie dem Zugriff der Ermittlungsbehörden entzogen werden. Bei strafbarer Geldwäsche stammen die Gelder u. a. aus schweren Straftaten der organisierten Kriminalität (z. B. Drogenhandel, Menschenhandel, Prostitution, Einschleusung von Ausländer, Raub, Diebstahl, Betrug). Geldwäsche betrifft dabei aber nicht nur Bargeschäfte oder Geld aus Drogenhandel, sondern auch die Anlage von Geld aus gewerbs- oder bandenmäßiger Steuerhinterziehung und organisierter Schwarzarbeit. Geldwäsche kann nicht nur durch Bank-, sondern auch mittels Versicherungs- und Hypothekengeschäften (Lebens-, Renten-, UBR- Versicherungen, Darlehen) betrieben werden.

Terrorismusfinanzierung

Im Geldwäschegesetz ist seit dem Jahr 2002 auch die **Prävention von Terrorismusfinanzierung** reguliert. Dabei geht es um die Geldbeschaffung für Personen und Vereinigungen, die in Verbindung zum Terrorismus stehen. Im Gegensatz zum Tatbestand der Geldwäsche können bei der Terrorismusfinanzierung die finanziellen Mittel auch aus legalen Quellen stammen, die dann durch Einbeziehung von Finanz- und Versicherungsprodukten zur Verschleierung der eigentlichen Herkunft letztendlich den Mitgliedern von terroristischen Organisationen zur Verfügung gestellt werden.

Geldwäschegesetz (GWG)

Strafbarkeit

Strafbar wäre eine Beteiligung an der Geldwäschehandlung des Kunden. Die Meldung eines Geldwäsche- oder Terrorismusverdachts befreit den Meldepflichtigen vom Sanktionierungsrisiko. **Die Identifizierung nach dem Geldwäschegesetz allein schützen nicht vor leichtfertiger Geldwäsche.** Diese formalen Pflichten sollen zunächst sicherstellen, dass ein Finanzinstitut seine Kunden und die Personen kennt („Know your customer (KYC)-Prinzip), denen ein Geschäft wirtschaftlich zugerechnet wird und dies entsprechend dokumentiert.

Im Geldwäschegesetz wurden die Bußgeldtatbestände drastisch ausgeweitet und erhöht.

Verpflichtete bis 5 Mio
Sonst bis 100.000,- €

Geldwäschegesetz (GWG) – wer wird identifiziert?

Wer und wann ist zu identifizieren

Die Identifizierung zählt zu den allgemeinen Sorgfaltspflichten. Die Identifizierung besteht aus:
- Feststellung der Identität durch Erheben der Angaben und
- Überprüfung der Identität anhand entsprechender Unterlagen

Wer ist zu identifizieren
- Vertragspartner
- die ggf. für den Vertragspartner auftretenden Personen
- wirtschaftlich Berechtigte
- **Identifizierung des Bezugsberechtigten**

Vom Vertragspartner abweichende Bezugsberechtigte oder Zahlungsempfänger von Kapitalleistungen (z. B. für Rückkaufswerte oder Erlebensfallleistungen) müssen i. S. des GwG ebenfalls identifiziert werden.

Zeitpunkt der Identifizierung

Die Identifizierung muss spätestens vor Auszahlung erfolgen. Wird der Bezugsberechtigte zunächst nur pauschal bezeichnet, sind zunächst keine weiteren Angaben erforderlich. Eine weitergehende Prüfung erfolgt bei Eintritt des Versicherungsfalls vor Auszahlung. Die erforderlichen Unterlagen werden von den vertragsführenden Stellen angefordert.

Geldwäschegesetz (GWG) – wie wird identifiziert?

Persönliche Anwesenheit
Der Vertragspartner (zu Identifizierende) muss anwesend sein. Mit Ihrer Unterschrift oder in der Angebotssoftware bestätigen Sie, dass der Vertragspartner persönlich anwesend war und mit dem Identifizierungsdokument übereinstimmt.

Erforderliche Angaben

- Name und Vorname(n)
- Geburtsdatum, Geburtsort, Staatsangehörigkeit, soweit jeweils im Ausweis enthalten
- Wohnanschrift (keine Postanschrift, c/o-Anschrift, kein Postfach)
- Ausweisdaten: Art, Nummer, ausstellende Behörde und das Ablaufdatum (gültig bis)

Dokumentenart Als Ausweispapiere können anerkannt werden:

- Personalausweis
- Reisepass
- vorläufiger Personalausweis oder Reisepass (nicht Ersatz-Personalausweis!)
- eAufenthaltstitel (elektronischer Aufenthaltstitel)
- Diplomatenausweis
- durch deutsche Behörden ausgestellte Reisedokumente für Personen, die nicht deutsche Staatsangehörige sind

Geldwäschegesetz (GWG) – wie wird identifiziert?

Einbeziehung Dritter, Unterrichtungspflicht

Die Identifizierung des Vertragspartners und des wirtschaftlich Berechtigten müssen durch den Vertreter, das Agenturpersonal oder Außendienstangestellte wahrgenommen werden. Eine Verlagerung auf Dritte ist nicht zulässig. Vertreter **haften** für ihre Angestellten unmittelbar.

Keine „indirekte Identifizierung“ durch Angehörige !

Geldwäschegesetz (GWG) – Identifizierung von Firmen

Identifizierung juristischer Personen oder Personengesellschaften

Handels-, Genossenschafts-und Partnerschaftsregister sowie zum Teil auch Vereinsregister können über die Servicestelle des gemeinsamen Registerportals der Länder (www.handelsregister.de) online eingesehen werden.

Erforderliche Angaben

- Name oder Bezeichnung (Firma)
- Rechtsform
- Registernummer(insbesondere Handelsregisternummer), falls vorhanden
- Anschrift des Sitzes oder der Hauptniederlassung
- Namen der Mitglieder des Vertretungsorgans bzw. der gesetzlichen Vertreter (Angabe von fünf Vertretern ausreichend). Sofern eines der Mitglieder eine juristische Person oder Personengesellschaft ist, sind von diesem ebenso die o. g. Angaben zu erheben

Dokumentenart

Die Überprüfung der Identifizierung ist anhand folgender Dokumente möglich:

- Auszug aus dem Handels-, Genossenschafts- und Partnerschaftsregister oder aus einem vergleichbaren amtlichen Register oder Verzeichnis
- Gründungsdokumente oder gleichwertige beweiskräftige Dokumente
- Wirtschaftsauskunft

Geldwäschegesetz (GWG) – BAV

Pensionskassen, Pensionsfonds und Unterstützungskassen

Es besteht **kein Identifizierungserfordernis** (weder Versicherungsnehmer noch wirtschaftlich Berechtigter) bei Abschluss einer Versorgung über **Pensionskassen, Pensionsfonds** und **Unterstützungskassen** für:

- die Versorgungsempfänger sowie
- den Arbeitgeber, der die Versorgung durch diese veranlasst.

Das Geldwäschegesetz ist für diese Fälle selbst dann nicht anwendbar, wenn Pensionskassen, Pensionsfonds und Unterstützungskassen Tochtergesellschaften des Versicherers sind bzw. von dieser verwaltet werden, weil die Versorgungsleistungen dieser Einrichtungen von der Anwendung der EU-Lebensversicherungsrichtlinie und damit des Geldwäschegesetzes ausdrücklich ausgenommen sind.

Geldwäschegesetz (GWG) – BAV

Firmendirektversicherung

Bei Abschluss einer Firmendirektversicherung bei Standardvereinbarung („Sämtliche Bezugsrechte sind nicht übertragbar oder beleihbar“) können vereinfachte Sorgfaltspflichten angewendet werden und somit besteht **kein Identifizierungserfordernis für den wirtschaftlich Berechtigten,** da die versicherte Person der wirtschaftlich Berechtigte ist und zu dieser die erforderlichen Daten stets vorhanden sind.

Für den **Vertragspartner** kann eine **Erleichterung** bei der **Überprüfung** der für die Identifizierung erforderlichen Unterlagen angewendet werden. D.h. eine Übersendung aussagekräftiger Kopien/Fotos von Unterlagen der Firma (z. B. Handelsregisterauszug) ohne Angabe zu den Gesellschafterverhältnissen ist ausreichend. Es muss jedoch sichergestellt sein, dass die Angaben auf den Kopien zu den Angaben des Vertragspartners passen und plausibel sind.

Geldwäschegesetz (GWG) – Bareinzahlungen

Darf Bargeld in den Agenturen entgegengenommen werden?

Sofern Inkassovollmacht besteht dürfen für Sachversicherungsverträge (Ausnahme UBR) bis zu maximal 2.500,- € bar kassiert werden. Die Abwicklung sollte nicht über das Agenturkonto erfolgen.

Beiträge zu UBR-, Lebens- oder Krankenversicherungen , wie zu sonstigen Kapitalanlageprodukten dürfen auf keinen Fall bar oder unbar entgegen genommen werden!

Das Nutzen des eigenen Kontos für Geldtransfers Dritter verstößt gegen Bestimmungen der **Abgabenordnung** und neben dem Risiko der **strafbaren Geldwäsche** besteht zusätzlich auch das Risiko der **strafbaren Beihilfe zur Steuerhinterziehung.**

Geldwäschegesetz (GWG) – Sorgfaltspflichten

Erhöhte Sorgfaltspflicht gilt bei:

- PEP´s - politisch exponierte Persönlichkeiten
- Einmalanlagen ab 100.000,- €
- Unplausibler Mittelherkunft
- Auffällige Rahmenbedingungen

Bei vorliegen diese Umstände sollte der Agenturinhaber informiert werden, der sich ggf mit dem Produktgeber abstimmt.

Geldwäschegesetz (GWG) – Auffällige Konstellationen

Geldwäschegesetz (GWG) – Auffällige Konstellationen

Zweifel bei Angaben des Vertragspartners, unplausibles Verhalten:

- Kunde erteilt falsche, vage, schwer verifizierbare oder allgemein widersprüchliche Angaben z. B. zu Tätigkeit, Wohnort, Firmensitz oder in Bezug auf seine Person.
- Ungewöhnliche Angaben, die auf einen nicht dauerhaften Wohnsitz hindeuten (Hotel, c/o), der sich nicht plausibel und nachvollziehbar erklären lässt.
- Die Höhe von Versicherungsbeiträgen oder Anlagevermögen passt nicht zur Stellung des Vertragspartners.
- Ausweisdokumente zur Identifizierung sind zweifelhaften Ursprungs.
- Vertragspartner verweigert (weitergehende) Auskünfte zur Herkunft der Mittel.
- Wirtschaftlich nicht nachvollziehbare Kundenentscheidung, insbesondere kein Interesse an z. B. günstigeren Konditionen, Anlagenrendite, Abwicklungsmodalitäten, Versicherungsschutz, steuerlichen Vorteilen. Stattdessen nur Interesse an Möglichkeit der Kündigung vor Vertragsablauf und Höhe des Rückkaufwertes.
- Fortführung wirtschaftlich angeschlagener Unternehmen (insbesondere nach Eigentümerwechsel).
- Abschluss verschiedener Versicherungsverträge ohne ersichtlichen Grund.
- Nicht plausible Wahl des Vermittlers.
- Kein Zusammenhang mit Wohnort, Arbeitsort, Kundensitz.
- Erbringen von Dienstleistungen (z. B. Beratungen) ohne erkennbaren Grund.
- Verfügungsberechtigung über Depot.
- Ankündigung aus dem Rahmen fallender Geschäfte, die vom eigentlichen Geschäftszweck ablenken sollen.
- Unbekannter Kunde erkundigt sich nach hoher Risiko-Lebensversicherung.
- Unklarer Bedarf bzw. unklare wirtschaftliche Verhältnisse; eventuell auch mit Bezug zu Risikoland.
- Erkundigung nach Meldepflichten der Produktgeber an Behörden (z. B. Steuerbehörden).
- VN-Wechsel kurz nach Vertragsschluss ohne erkennbaren Grund, insbes. mehrere Wechsel kurz hintereinander.
- Versuch des Vertragspartners, den angestrebten persönlichen Kontakt zu vermeiden.

Geldwäschegesetz (GWG) – Auffällige Konstellationen

Einschalten Dritter:

- Zweifel an den Angaben des Vertragspartners zur wirtschaftlichen Berechtigung an den Vermögenswerten(Strohmann).
- Benennung eines Verfügungsberechtigten, der in keiner erkennbaren Beziehung zum Vertragspartner steht.
- Auftreten von Bevollmächtigten für Interessenten im Ausland, bei denen kein erkennbarer Bezug zu Deutschland besteht, insbesondere von Ausländern, die aus einem Land stammen, das ein erhöhtes Geldwäscherisiko aufweist. Das sind zum einen Embargoländer wie beispielsweise Iran und Syrien, zum anderen sind das Länder, die von der internationalen Geldwäschebekämpfungsgruppe FATF auf die sog. Beobachtungsliste gesetzt wurden (aktuell insb. Myanmar, Nigeria, Nordkorea).
- Kunden treten ohne nachvollziehbare Gründe Rechte an Fondsanteilscheinen/Lebensversicherungen/Bausparverträgen an Unternehmen ab, welche dann die Verträge/Depots vorzeitig auflösen.

Ungewöhnliche Geschäftsabwicklung:

- Vertragspartner möchte Versicherungsbeitrag bar zahlen (auch Barscheck).
- Wunsch nach Beitragszahlung weit vor Vertragsschluss (Vertragspartner hat nicht die Absicht, den Vertrag zu schließen, sondern strebt Rückzahlung von Versicherung als „guter Adresse“ an).
- Erkundigung nach Zahlungs-und Auszahlungsmöglichkeiten (z. B. Barzahlung, Konto im Ausland), die sich nicht durch Lebensumstände erklären lassen (z. B. Wohnsitzwechsel ins Ausland).
- Im Inland ansässiger Antragsteller bietet Beitragszahlung in Devisen an.
- Wunsch, Kredite durch Hinterlegung von Bargeld zu erhalten oder mit Bargeld zurückzuführen.
- Stellung von Sicherheiten durch unbekannte Dritte (kein erkennbarer Bezug zum Vertragspartner) oder Auszahlungswunsch von Krediten an unbekannte Dritte.
- Wertpapierdepoteröffnung und Anfrage nach physischer Aus- bzw. Einlieferung (Tafelgeschäfte).

Geldwäschegesetz (GWG) – Speicherung des Ausweises

Das Personalausweisgesetz verbietet prinzipiell das Speichern von Personalausweisen
Die Speicherung ist nur zulässig wenn es dafür eine gesetzliche Grundlage gibt. Wir unterscheiden zwischen

Gebunde Vermittler

Unterliegen dem GWG nicht direkt und dürfen Ausweise generell nicht als Kopie speichern. Sie geben nur Kopien und Angaben an den Versicherer weiter, die dann wieder zu löschen sind.

Vermittler mit eigener Erlaubnis

Unterliegen dem GWG direkt und müssen / dürfen den Ausweis zur Identifizierung zum Nachweis fünf Jahre speichern.

Nach fünf Jahren ist die Ausweiskopie zu löschen.

Themenübersicht

Geldwäschegesetz (GWG)

- Grundsätze
- Bareinzahlungen
- Risikofaktoren
- Umgang mit Ausweiskopien

DSGVO Datenschutzgrundverordnung

- Grundsätze
- Konkrete Umsetzung in der Agentur
- Integrität und Vertraulichkeit
- Rechtsfolgen und Risiken
- Umgang mit Betroffenenrechte

Fragen der Teilnehmer

Datenschutz – Allgemeine Informationen

- Die Verordnung gilt ab dem **25. Mai 2018** unmittelbar
- Ziel ist die **Vereinheitlichung** des Datenschutzre
- DSGVO **ersetzt** das bisherige BDSG und **wird präzisiert** durch das BDSG-neu
- **Stärkung der Betroffenenrechte** bei Transparenz, Zweckbindung und Datenminimierung
- **Höhere Rechenschafts- und Nachweispflichten** für Unternehmen
- Integration der Anforderungen in die Unternehmens-IT erforderlich
- **Drastisch erhöhte Bußgelder** je nach Schwere bis zu 10 Mio oder 20 Mio je nach Kategorie oder von bis zu 2 % oder 4% des Konzernumsatzes

Das meiste galt schon vorher nach BDSG !

Datenschutz – Grundsätze

Art1 Gegenstand und Ziele

- Diese Verordnung enthält Vorschriften zum **Schutz natürlicher Personen** bei der **Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten**.
- Diese Verordnung schützt die Grundrechte und Grundfreiheiten **natürlicher Personen** und insbesondere **deren Recht auf Schutz personenbezogener Daten**.
- Der **freie Verkehr personenbezogener Daten** in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder **eingeschränkt noch verboten** werden.

Datenschutz – Grundsätze

Art2 Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

> im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,
> durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,
> durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,
> durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.

(3) Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union gilt die Verordnung (EG) Nr. 45/2001. [2]Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, werden im Einklang mit Artikel 98 an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst.

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1.„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden **„betroffene Person**“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1.Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

6. Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Datenschutz – Erste Prüfungen

Datenschutzgrundverordnung

Landesdatenschutzbeauftragte überprüfen die Einhaltung

In der jüngsten Zeit haben die Landesdatenschutzbehörden von Bayern und auch von Niedersachsen damit begonnen, Prüfungen bei Unternehmen, davon auch kleine und mittlere Unternehmen (KMU), vorzunehmen. Das geschieht durch Übersendung eines umfangreichen Fragenkatalogs, der darauf abzielt, festzustellen, welche Maßnahmen zur Umsetzung der Vorschriften der Datenschutzgrundverordnung (DSGVO) im Unternehmen durchgeführt wurden.

usheva · 123RF.com

Datenschutz – Bußgelder

Das Unternehmen Kolibri Image ersuchte den Hamburger Landesbeauftragten im Mai 2018 um Rat. Die kleine Firma bat einen ihrer Dienstleister mehrfach um einen Vertrag zur Auftragsverarbeitung, bekam diesen aber nicht. Sie war ratlos und fragte nach, wie sie nun vorgehen solle. Der Landesbeauftragte antwortete, dass beide Seiten zu solch einem Vertragsschluss verpflichtet seien. Kolibri Image müsse den Vertrag deshalb selbst absenden und dürfe den Dienstleister erst nach Vertragsschluss beauftragen. Der Landesbeauftragte versendete am 17.12.2018 einen Bußgeldbescheid in Höhe von 5.000 Euro zuzüglich 250 Euro Gebühren. Er begründete den Bescheid gegenüber dem Unternehmen mit einem Verstoß gegen Art. 83 Absatz 4 DSGVO. Der Grundsatz „Fragen kostet nichts“, traf hier nicht zu.

Datenschutz – Bußgelder

Auch Start-Ups sind von Datenschutzverstößen damit von Bußgeldern betroffen. Im Fall des jungen Online-Bank N26 hatte die Berliner Datenschutzbeauftragte die Speicherung von Namen ehemaliger Kunden zum Zwecke der Geldwäscheprävention mit einem Bußgeld von 50.000 Euro sanktioniert.

Datenschutz – Bußgelder

Gegen das **Krankenhaus** hat der Landesbeauftrage für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz ein Bußgeld verhängt. Dieses beruht auf mehreren Verstößen gegen die Datenschutzgrundverordnung im Zusammenhang mit einer **Patientenverwechslung bei der Patientenaufnahme. Auf diese Weise sollen sich strukturelle technische und organisatorische Defizite beim Patientenmanagement offenbart haben**, so der Landesdaten-schutzbeauftragte. Die Festsetzung des Bußgelds erfolgte unter individueller Bewertung von insgesamt drei Verstößen. Die Klinik hat das Bußgeld akzeptiert.

Datenschutz – Bußgelder

Gegen den **Telekommunikationsdienstleister** verhängte der Bundesdatenschutzbeauftragte ein Bußgeld. Das Unternehmen hatte keine hinreichenden technisch-organisatorischen Maßnahmen ergriffen, um zu verhindern, dass Unberechtigte bei der telefonischen Kundenbetreuung Auskünfte zu Kundendaten erhalten können. **Um an umfassende personenbezogene Kundendaten zu gelangen, hat die Angabe von Name und Geburtsdatum gereicht.** Weil dadurch personenbezogene Daten nicht systematisch geschützt würden, hat die Aufsichtsbehörde einen Verstoß gegen Artikel 32 DSGVO angenommen. Ein Bußgeld war nach Aussage des BfDI geboten, da der Verstoß nicht nur auf einen geringen Teil der Kunden begrenzt gewesen sei, sondern ein Risiko für den gesamten Kundenbestand darstellte.

Datenschutz – Bußgelder

Das höchste Bußgeld hierzulande in Höhe von 14,5 Millionen Euro wurde von der Berliner Datenschutzbeauftragten gegen die Immobilienfirma Deutsche Wohnen erlassen.

Der Grund: Das Unternehmen hat laut der Behörde personenbezogene Daten von Mietern in einem Archivsystem gespeichert, bei dem nicht mehr erforderliche Daten nicht gelöscht werden konnten.

Datenschutz – Bußgelder

Bußgeld in Höhe von 265 Mio. Euro gegen die Meta Platforms Ireland Ltd. (Irland) wegen der Veröffentlichung von Nutzer:innendaten

Die irische Datenschutzbehörde hat am 28.11.2022 ein Bußgeld in Höhe 265 Mio. € gegen Meta Platforms Ireland Ltd. verhängt. Ausgangspunkt für die Verhängung war die Veröffentlichung von personenbezogenen Daten, wie z.B. Namen, Telefonnummern und E-Mail-Adressen, von bis zu 533 Mio. Nutzer:innen aus über 100 Ländern in einem Hacker-Forum im vergangenen Jahr. Die Hacker machten sich dabei die Funktionen Facebook Search, Facebook Messenger Contact Importer und Instagram Contact Importer zunutze.

Die irische Behörde leitete daraufhin ein Verfahren ein, in dem sie mit den Aufsichtsbehörden der anderen europäischen Staaten zusammenarbeitete. Sie kamen nun zum Ergebnis, dass Facebook in Bezug auf die oben genannten Funktionen gegen Art. 25 Abs. 1 und Abs. 2 DSGVO verstoßen habe. Gemäß diesen datenschutzrechtlichen Vorgaben sind Unternehmen dazu verpflichtet, sowohl bereits bei der Gestaltung als auch bei der Konfiguration von Technik, technische und organisatorische Maßnahmen zu implementieren, welche die Einhaltung datenschutzrechtlicher Grundsätze gewährleisten (=data protection by design and by default).

Geldwäschegesetz - Datenschutz

Bußgelder

15.08.2014	64.000 €	Mr. Wash	DE	Unerlaubte Videoüberwachung und fehlende Bestellung eines Datenschutzbeauftragten. »Details
03.12.2019	105.000 €	Universitätsmedizin der Johannes Gutenberg-Universität Mainz	DE	Patientenverwechselung bei der Aufnahme eines Patienten. »Details
11.03.2020	2.000 €	Restaurant	DE	Unerlaubte Kameraüberwachung des Gastraumes eines Restaurants. »Details
14.03.2020	229 €	LKW-Fahrer	DE	Betrieb einer Dashcam im Straßenverkehr und Veröffentlichung von Aufnahmen über Youtube. »Details
24.03.2020	12.000 €	Betreiber eines Schwimmbades	DE	Unerlaubte Videoüberwachung in Schwimmbad, fehlender AV-Vertrag und keine Benennung eines DSB. »Details
24.03.2020	50.000 €	Unternehmen	DE	Fehlender AV-Vertrag und Verstoß gegen Transparenz- und Verständlichkeitsgebot. »Details
03.04.2020	6.000 €	Berliner Landesverband der NPD	DE	Veröffentlichung der Kontaktdaten von Flüchtlingshelfern über Google Maps. »Details
08.01.2021	10.400.000 €	notebooksbilliger.de AG	DE	Unrechtmäßige Videoüberwachung von Mitarbeitern und Kunden über einen Zeitraum von mindestens zwei Jahren. »Details

Datenschutz – Grundsätze

Verbot mit Erlaubnisvorbehalt

Da die Verarbeitung personenbezogener Daten in das verfassungsrechtlich geschützte Persönlichkeitsrecht eingreift, ist **eine Datenverarbeitung grundsätzlich verboten.**

Nur, wenn sie z. B. **gesetzlich erlaubt** oder auf der **Einwilligung** der betroffenen Person beruht, ist sie erlaubt.

Rechtmäßigkeit

Die Verarbeitung ist dann rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht **(Rechtsgrundlage, Einwilligung** usw.) und der Zwecke der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.

Datenschutz – Grundsätze

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

[1]Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.

- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

Datenschutz – Grundsätze

Transparenz

Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. **Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht**)

Zweckbindung

Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck eng zusammenhängen.

Datenschutz – Grundsätze

Datenminimierung

Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für die **Zweckerreichung notwendig** sind.

Richtigkeit

Die Daten **müssen richtig sein**, anderenfalls müssen sie berichtigt oder gelöscht werden.

Speicherbegrenzung

Die Datensparsamkeit ist hierbei zu beachten, also die Frage, wann Daten nicht mehr benötigt und daher gelöscht werden können. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

Datenschutz – Grundsätze

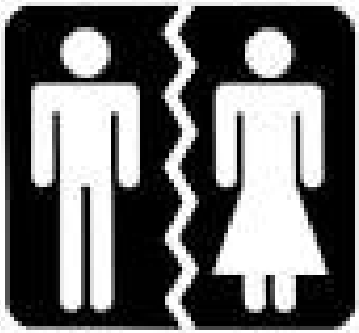
Integrität und Vertraulichkeit

Die DS-GVO verknüpft sehr stark den **Datenschutz mit der Technik**. Die IT-Verfahren müssen somit schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (**privacy by design**).

Rechenschaftspflicht

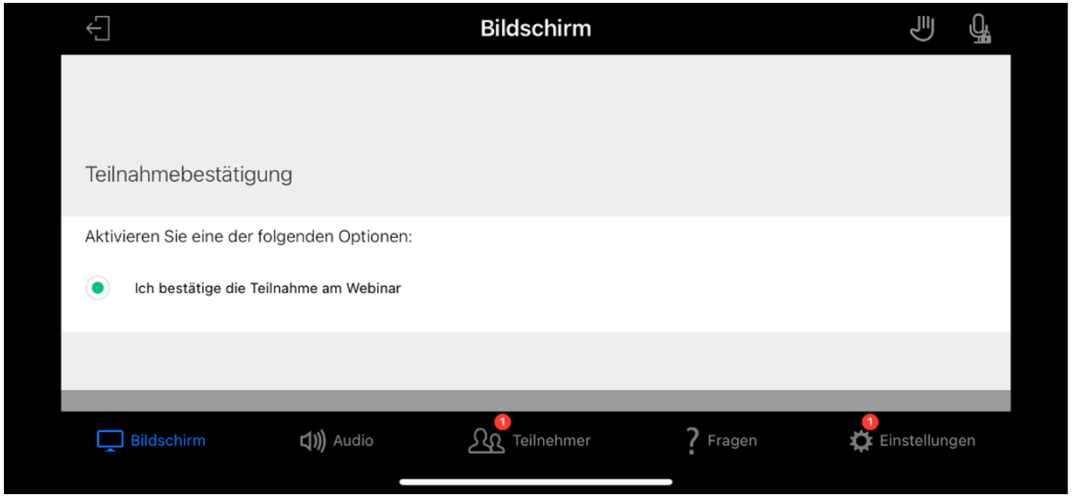
Das ist der wichtigste Aspekt der Grundsätze! Die verantwortliche Stelle, also das Unternehmen oder die Institution sind verantwortlich für den Datenschutz und seine Beachtung. **Dazu ist ein Datenschutzmanagement notwendig** – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden und der Menge und der Qualität der Daten. Zumindest muss aber **auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können**. Denn die Verletzung der Datenschutzpflichten zieht empfindliche Bußgelder nach sich.

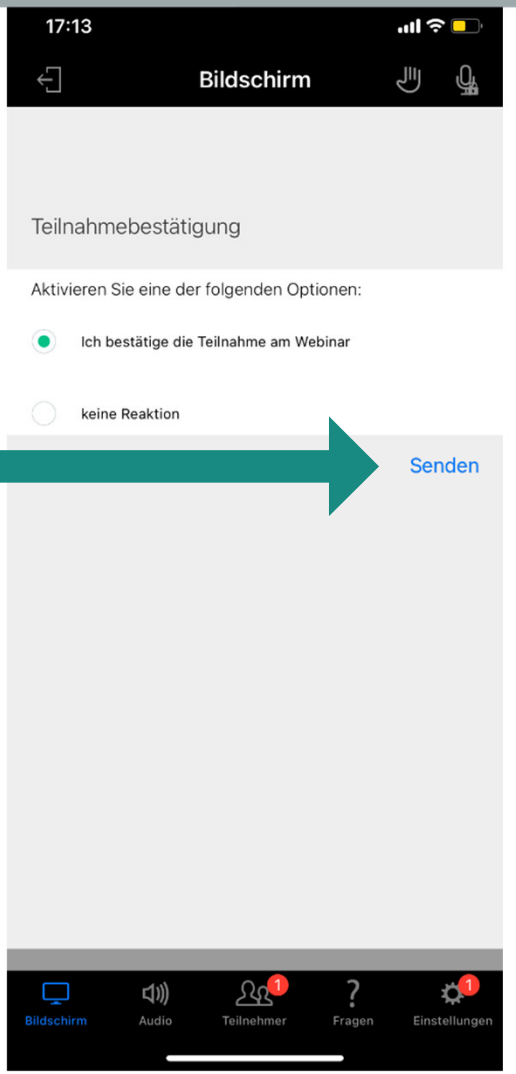
Datenschutz – Risiken



Teilnahmebestätigung

Achtung ! Wenn Sie ein Smartphone nutzen, halten Sie das Gerät hochkant oder scrollen Sie um den „Senden“-Button bedienen zu können.





Datenschutz - Risiken

DSGVO - die Bußgelder:

2%-4% des Konzernumsatzes

bis 10 – 20 Mio

- ⇨ Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind erhebt und verarbeitet
- ⇨ Wer die organisatorischen Maßnahmen nicht implementiert
- ⇨ entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt (notwendig ab 20 Angestellten)

Der Vermittler trägt die Verantwortung für den Datenschutz !

Datenschutz - Risiken

BDSG § 7 Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen **zum Schadensersatz verpflichtet**. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Strafe bis zu 1 Jahr Gefängnis

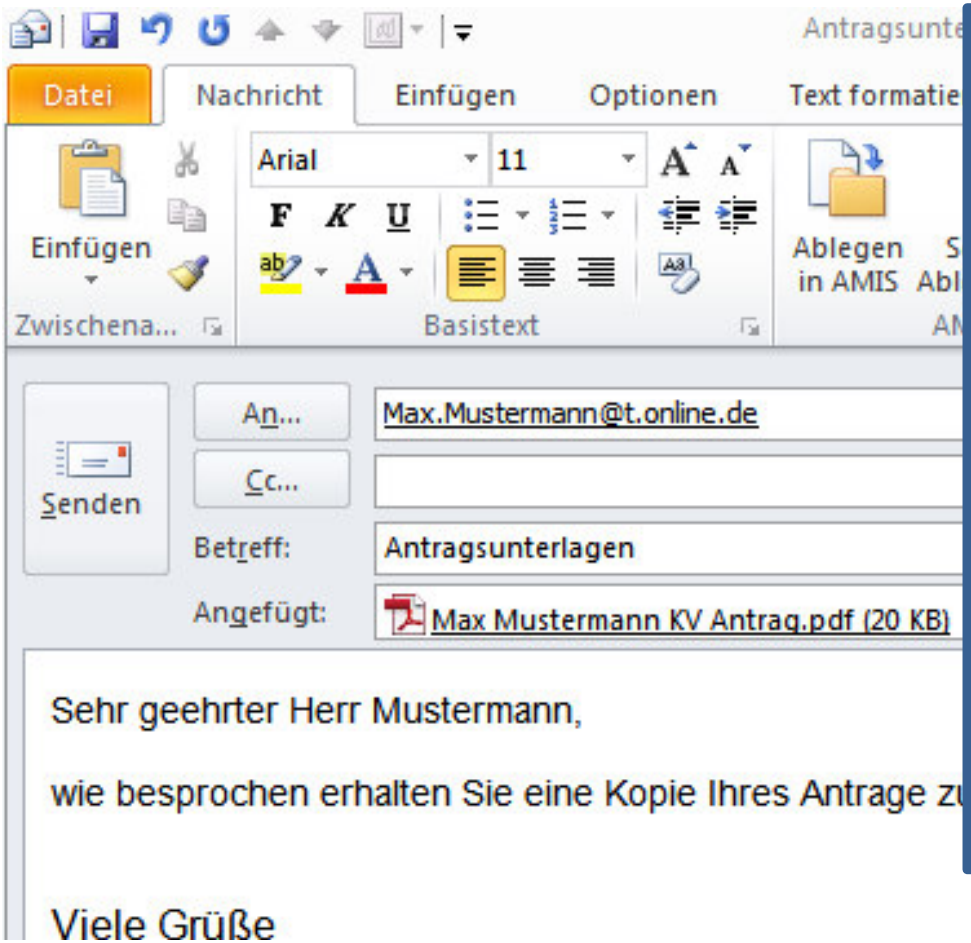
§ 203 StGB Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als:

Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit

Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

Geldwäschegesetz - Datenschutz



Das Gesetz stellt die unbefugte Offenbarung von entsprechenden Geheimnissen unter Strafe (§ 203 StGB).

Offenbart wird der jeweilige Nachrichteninhalt in jedem Fall, da zumindest Mitarbeiter des jeweilige TK-Dienstleisters in der Lage sind, Einsicht in unverschlüsselte Kommunikationsinhalte zu nehmen. Daran ändert auch ein ggf. gem. §§ 88 TKG, 206 StGB bestehendes Verbot am Ende nichts.

Ohne das Vorliegen einer wirksamen Einwilligung sollten solche Berufsträger daher trotz aller Vorteile auf eine Kommunikation per E-Mail mit ihren Mandanten verzichten.

Geldwäschegesetz - Datenschutz

Die Techniker Krankenkasse führt für ihre Mitglieder einen neuen digitalen Service ein: Wer beim Arzt seine Krankenkassenkartevergessen hat, kann auf die TK-App zurückgreifen. Wer allerdings erwartet, dass man mittels der App eine digitale Version der Krankenkassenkarte vorzeigen kann, dürfte enttäuscht sein.

Die TK hat sich etwas anderes ausgedacht: Die App sorgt dafür, dass die Bescheinigung per Fax an die Arztpraxis übermittelt wird. Mit der TK-App könne man, so die Krankenkasse in einem Schreiben an ihre Mitglieder, *"blitzschnell eine Bescheinigung über Ihre Mitgliedschaft bei uns anfordern"*.
Dabei betont die Krankenkasse: *"Die Sicherheit Ihrer Daten ist uns wichtig. Deshalb faxen wir nur an Nummern von Arztpraxen, die uns bekannt sind."*

Datenschutz gegenüber dem Arbeitnehmer

Wie lange darf man Bewerbungen speichern?

Bis zu 6 Monaten

Wie kann ich die daten von potentiellen Bewerbern für später sichern?

Sie informieren den Bewerber ausführlich, in welcher Form und warum Sie seine personenbezogenen Daten weiterhin speichern und der Bewerber gibt dafür seine schriftliche Zustimmung.

Datenschutz gegenüber dem Arbeitnehmer

Darf der/die Angestellte seine Personalakte einsehen?

Ja, jederzeit. Gleichzeitig besteht das Recht, dass veraltetet oder unrichtige Angaben berichtigt werden. Das gilt auch für aufgelöste Beschäftigungsverhältnisse.

Wie lange wird die Personalakte bei Ausgeschiedenen aufbewahrt?

Sie darf frühestens 3 Jahre nach dem Ausscheiden vernichtet werden. Enthält die Personalakte auch steuerrelevante Informationen, so müssen diese mindestens 6, im Zweifelsfall 10 Jahre aufbewahrt werden, Unterlagen zu einer betrieblichen Altersversorgung, die erst später in Anspruch genommen wird, müssen bis zum Versorgungstermin aufbewahrt werden. Die verlängerte Aufbewahrungsfrist kann bis zu 30 Jahre betragen.

Datenschutz gegenüber dem Arbeitnehmer

Was steht in der Personalakte

Personenbezogene und Vertragsunterlagen

- Bewerbung
- Arbeits- und Schulzeugnisse
- Lebenslauf ggf. Passbild
- Vermerke über die Einsichtnahme ins amtliche Führungszeugnis
- Arbeitsvertrag und Stellenbeschreibung
- Erklärung zu Nebenbeschäftigungen
- Verschwiegenheitserklärung
- Datenschutzverpflichtung

Aufbewahrungsfrist ergibt sich aus der Verjährungsfrist von Ansprüchen aus dem Arbeitsvertrag

Datenschutz gegenüber dem Arbeitnehmer

Was steht in der Personalakte

Sonstige Vertragsrelevante Unterlagen

- Personalbogen
- Urlaubsliste und Fehlzeitenübersicht
- Beurteilungen
- Abmahnungen - Ermahnungen
- Personalentwicklungsplan
- Protokolle von Mitarbeitergesprächen
- Bescheinigungen über Belehrungen, Untersuchungen beim Arbeitsschutz
- Weiterbildungsnachweise

Datenschutz gegenüber dem Arbeitnehmer

Was steht in der Personalakte

Sozialversicherungs- und Steuerunterlagen

- Anmeldungen zur Krankenkasse
- Beitragsnachweis Krankenkassenbeiträge
- Lohnabrechnung
- Sozialversicherungsausweis
- Ggf VWL Unterlagen
- Nachweis für Kinderlose/Kinder wegen Beitrag Pflegeversicherung
- Unterlagen zur Lohnsteuer
- Ggf. Unterlagen zur betrieblichen Altersversorgung

Aufbewahrungsfrist Sozialversicherungsunterlagen 1 Jahr nach der letzten Betriebsprüfung
Steuerunterlagen 6 Jahre
BAV bis zum Leistungszeitpunkt

Datenschutz gegenüber dem Arbeitnehmer

Gibt es besondere Anforderung an die Aufbewahrung der Akte?

Ja, es muss sicher gestellt sein, dass Dritte, die nicht mit der Personalführung betraut sind, keinen Zugang zur Akte haben. Nach dem Ausscheiden aus dem Unternehmen kommt die Akte „unter Verschluss“

Dürfen Daten zu Gesundheit, Sexualität oder Religion gespeichert werden?

Nur mit ausdrücklicher Zustimmung der Betroffenen oder wenn die Daten öffentlich zugänglich sind.

Darf der Arbeitgeber nach sensiblen Daten (Krankheit) fragen?

Nein, der Arbeitnehmer hat, wenn er gefragt wird sogar das recht zu lügen. Das gilt bei Bewerbungen wie im laufenden Arbeitsverhältnis.

Datenschutz gegenüber dem Arbeitnehmer

Sollte die Nutzung des betrieblichen Mailaccount für private Zwecke erlaubt werden?

Nein, ist die private Nutzung erlaubt dürfen Dritte das Postfach nicht mehr einsehen. Das Nutzungsverbot ermöglicht den Zugang bei Krankheit oder Ausscheiden

Was ist bei der Nutzung von Abwesenheitsassistenten zu beachten?

Der Schutz der Persönlichen Daten verbietet persönliche Gründe für die Abwesenheit zu nennen. Als NICHT

- Bin bis… im Urlaub
- Bin Krankheitsbedingt erst …. erreichbar

Tipps für die Umsetzung – Rechte der Betroffenen

Integrität und Vertraulichkeit

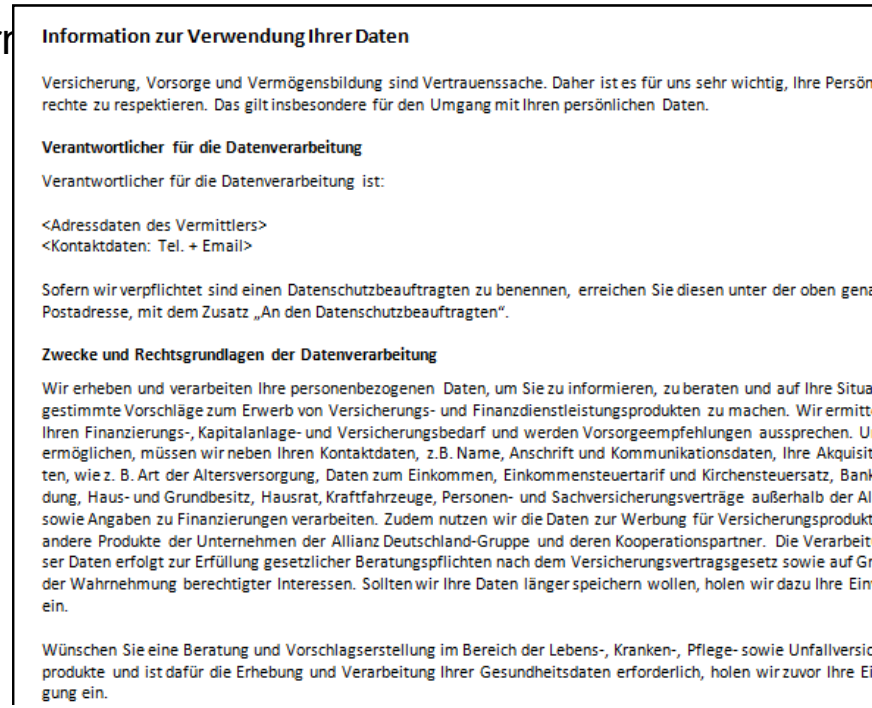
- Sicheres Passwort - Passwort sicher aufbewahren
- Keine Kunden- und Interessentendaten überspielen
- Keine Daten auf´s Handy (WhatsApp)
- Haben Kunden Einsicht oder Zugang zu PC?
- Hygiene beim Umgang mit Kundenakten
- Offenes Fenster – PC bei Abwesenheit sperren - Bildschirm weg vom Fenster – keine Akten offen rumliegen lassen – alte Akten schreddern
- Identifizierung von Kunden am Telefon
- Weitergabe von Informationen an Dritte nur mit Zustimmung !!
- BCC statt CC bei mehreren Mail-Empfängern
- Keine Info zu Dritte über Abwesenheitsgrund, kein offener Urlaubskalender

Tipps für die Umsetzung – Rechte der Betroffenen

Proaktive Benachrichtigung der Betroffenen über

- Kontaktdaten des Verantwortlichen,
- die Verarbeitungszwecke sowie die Rechtsgrundlage,
- gegebenenfalls die Empfänger oder Kategorien von Empfängern
- Absicht der Übermittlung in ein Drittland, aber auch die
- Dauer der Speicherung, beziehungsweise die
- Kriterien für die Festlegung dieser Dauer.

Infoblatt aushändigen am besten in Verbindung mit Daten- und Werbe-Einwilligung
Dewe + Wewe



Information zur Verwendung Ihrer Daten

Versicherung, Vorsorge und Vermögensbildung sind Vertrauenssache. Daher ist es für uns sehr wichtig, Ihre Persön
rechte zu respektieren. Das gilt insbesondere für den Umgang mit Ihren persönlichen Daten.

Verantwortlicher für die Datenverarbeitung

Verantwortlicher für die Datenverarbeitung ist:

<Adressdaten des Vermittlers>
<Kontaktdaten: Tel. + Email>

Sofern wir verpflichtet sind einen Datenschutzbeauftragten zu benennen, erreichen Sie diesen unter der oben gena
Postadresse, mit dem Zusatz „An den Datenschutzbeauftragten".

Zwecke und Rechtsgrundlagen der Datenverarbeitung

Wir erheben und verarbeiten Ihre personenbezogenen Daten, um Sie zu informieren, zu beraten und auf Ihre Situa
gestimmte Vorschläge zum Erwerb von Versicherungs- und Finanzdienstleistungsprodukten zu machen. Wir ermitt
Ihren Finanzierungs-, Kapitalanlage- und Versicherungsbedarf und werden Vorsorgeempfehlungen aussprechen. U
ermöglichen, müssen wir neben Ihren Kontaktdaten, z.B. Name, Anschrift und Kommunikationsdaten, Ihre Akquisit
ten, wie z. B. Art der Altersversorgung, Daten zum Einkommen, Einkommensteuertarif und Kirchensteuersatz, Bank
dung, Haus- und Grundbesitz, Hausrat, Kraftfahrzeuge, Personen- und Sachversicherungsverträge außerhalb der Al
sowie Angaben zu Finanzierungen verarbeiten. Zudem nutzen wir die Daten zur Werbung für Versicherungsprodukt
andere Produkte der Unternehmen der Allianz Deutschland-Gruppe und deren Kooperationspartner. Die Verarbeit
ser Daten erfolgt zur Erfüllung gesetzlicher Beratungspflichten nach dem Versicherungsvertragsgesetz sowie auf Gr
der Wahrnehmung berechtigter Interessen. Sollten wir Ihre Daten länger speichern wollen, holen wir dazu Ihre Ein
ein.

Wünschen Sie eine Beratung und Vorschlagserstellung im Bereich der Lebens-, Kranken-, Pflege- sowie Unfallversic
produkte und ist dafür die Erhebung und Verarbeitung Ihrer Gesundheitsdaten erforderlich, holen wir zuvor Ihre Ei
gung ein.

Tipps für die Umsetzung – Rechte der Betroffenen

Recht auf Berichtigung und die Vervollständigung sie betreffender unzutreffender personenbezogener Daten (Art. 16 DSGVO).

Wenig Relevanz für Agentur

Recht auf Löschung wenn diese zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind oder die dazu erteilte Einwilligung widerrufen wurde.

1. **Interne Maßnahmen – Löschroutinen**
2. **Verhalten bei Löschanfragen**

Weitergabe der Anfrage an Versicherer (Daten Versicherer)
Weitergabe an Agenturinhaber bei Nachfrage nach internen Daten

Tipps für die Umsetzung – Rechte der Betroffenen

Recht auf Vergessenwerden“ (Art. 17 Abs. 2 DSGVO), wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat. Diese Vorschrift ist von besonderer Bedeutung für den Betrieb von Internet-Suchmaschinen.

Einschränkung der Verarbeitung (Art. 18 DSGVO) – zum Beispiel, wenn der die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen. Die Einschränkung der Verarbeitung entspricht damit begrifflich im Wesentlichen der Sperrung im Sinne von §§ 20 Abs. 3, 35 Abs. 3

Wenig Relevanz für Agentur

Tipps für die Umsetzung – Rechte der Betroffenen

Recht auf Datenübertragbarkeit (Art. 20 DSGVO). Mit seiner Einführung wird die Datensouveränität der betroffenen Person gestärkt. Das Recht auf Datenübertragung gibt betroffenen Personen daher unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten.

Weiterleitung der Anfrage an Versicherer

Bei Anfrage nach Daten in der Agentur Weitergabe der Anfrage an den Verantwortlichen / Agenturinhaber

Datenschutz – Vorsicht bei Datenpannen!

Artikel 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen **72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsicht[illegible]e, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu ei[illegible]nd Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbeh[illegible] Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezoge[illegible] diese d[illegible] Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Date[illegible] Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Ka[illegible] betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstig[illegible]nlaufstelle für weitere Informationen

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

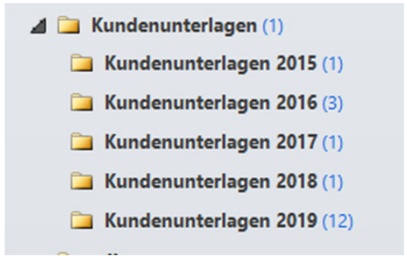
d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

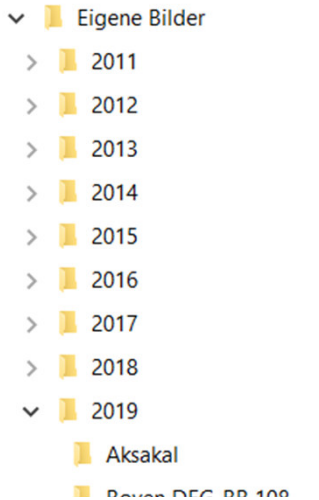
Handeln Sie nur abgestimmt!

Haben Sie ein Datenschutzkonzept?

Tipps für die Umsetzung – Praxisbeispiele

- **Überlegen Sie welche Daten Sie wirklich dauerhaft brauchen**
- **Speichern Sie Leistungs- und Schadendaten nicht in den Agentursystemen**
- **nutzen Sie Postausgangsordner in Outlook, die regelmäßig gelöscht werden.**
- Werden Daten Dritter verarbeitet?
- Werden diese über die Verarbeitung informiert?
- Wie sensibel gehen alle Funktionäre mit Daten Dritter um
- Sind Löschroutinen vorhanden?





Gibt es ein Handbuch oder Arbeitsanweisungen?

Datenschutz – was darf ich speichern ?

	auf Basis gesetzlicher Grundlage	Speicherfristen	mit Einwilligung
Steuerliche Unterlagen	ja	10 Jahre	ja
Handelsbriefe	ja	6 Jahre	ja
Ausweise (GWG) eigenregistriert	ja	5 Jahre	5 Jahre
Interessentendaten	nein		ja
Beratungsdokumentation	ja	30 Jahre	ja
Vertragsunterlagen	ja	Vertragsdauer	ja
Anträge	nein	während Bearbeitung	ja
persönliche Unterlagen	nein	nein	ja
Gesundheitsdaten	nein	während Bearbeitung	nein?

Datenschutz – Wer haftet?

Für die ordnungsgemäße Datenverarbeitung haftet der „Verantwortliche“

- Der Betriebsinhaber
- Der Agenturinhaber
- Der Vereinsvorstand
- Die Firmenleitung

Der Verantwortliche haftet für den richtigen Umgang mit Daten und die Einhaltung der technischen und Organisatorischen Maßnahmen:

- Systemsicherheit
- Schulung und Weiterbildung der Mitarbeiter sowie deren Dokumentation
- Erstellung eines Datenschutzkonzeptes im Betrieb

Datenschutz – Unterweisung und Haftung der Mitarbeiter

Und was gilt nun bei Bußgeldern aufgrund von Datenschutzverstößen für das Arbeitsverhältnis?
Nach Abs. 83 DSGVO können Aufsichtsbehörden zwar Bußgelder verhängen, die auch bis 20.000.000 € betragen können, der Adressat eines solchen Bußgeldes ist aber immer der (für die Datenverarbeitung) Verantwortliche – und das ist der Arbeitgeber.

Ein Arbeitnehmer haftet daher in Bezug auf ein Bußgeld nach Art. 83 DSGVO nur im Innenverhältnis. Das liegt daran, dass die Einhaltung der datenschutzrechtlichen Vorgaben, zu den Pflichten des Arbeitsverhältnisses gehören, die bei der täglichen Arbeit zu beachten sind.

Folgen für den Arbeitnehmer

Leichteste-/ leichte Fahrlässigkeit
Handelt der Arbeitnehmer nur leicht fahrlässig haftet er nicht.

Normale-/ mittlere Fahrlässigkeit
Handelt der Arbeitnehmer „normal“ fahrlässig wird der Schaden geteilt. Allerdings wird die Haftung des Arbeitnehmers bei sehr hohen Schäden häufig auf ein Monatsgehalt begrenzt.

Grobe-/ gröbste Fahrlässigkeit
Handelt der Arbeitnehmer grob fahrlässig, haftet er grundsätzlich in vollem Umfang.

- Ausnahme 1 Gericht beschränkt die Haftung bei sehr hohen Forderungen auf 3 Gehälter
- Ausnahme 2 Das Handeln war grob fahrlässig oder vorsätzlich, der Schadeneintritt wurde aber nur fahrlässig herbei geführt

Vorsatz
Nur wenn der Arbeitnehmer vorsätzlich handelt und auch den Schaden vorsätzlich verursacht, haftet er voll.

Datenschutz – Tipps für den Agenturalltag

1. Erstellen Sie ein Datenschutzkonzept (Vorlage)
2. Überprüfen Sie dabei die Arbeitsabläufe
   - Welche Daten werden gespeichert – welche nicht
   - Wo werden die Daten gespeicherte
   - Wie ist die Löschung sichergestellt
   - Datenabfluss aus dem Agentursystem (Handy)
3. Speichern Sie nur „erlaubte Daten“
4. (Oder) nutzen Sie die Einwilligung
5. Speichern Sie die Einwilligung verlässlich
6. Unterweisen Sie Ihre Mitarbeiter
7. Verpflichten Sie Ihre Mitarbeiter
8. Dokumentieren Sie die Unterweisung

Datenschutzgrundverordnung DSGVO

Mit diesen kleinen Vortrag können Sie sich über die Grundzüge der DSGVO informieren. Sie erfahren dabei wie konkret Sie in Ihrer Agenturarbeit davon betroffen sind.

Die nachstehenden Downloads können Sie zur Unterstützung Ihrer Datenschutzkonzeption nutzen. Die Unterlagen sind Stand April 2018 und sind nur ein Vorschlag für Ihre eigene Umsetzung.

Muster Datenschutzkonzept in der Agentur

Nachweis Mitarbeiterunterweisung

Arbeitnehmervereinbarung zur Nutzung des Internet

Vereinbarung für Bürogemeinschaften

Verpflichtung von Mitarbeitern zur Wahrung des Datenschutz und von Geschäftsgeheimnissen

Die Vorlagen der Einwilligungserklärungen wurden mit Unterstützung eines Fachanwaltes optimiert. Wir empfehlen künftig die aktuelle Version zu verwenden, die unter anderem auch die Datenspeicherung für Kinder unserer Kunden und die Zusammenarbeit in Bürogemeinschaften regelt. In der Vorgängerversion eingeholte Erklärungen brauchen natürlich nicht ausgetauscht werden.

Muster Einwilligungserklärung zur Datenspeicherung

Muster Einwilligungserklärung zur Datenspeicherung kombiniert mit Werbeeinwilligung und Auskunftsvollmacht

Ergänzung der Einwilligungserklärung für Bürogemeinschaften

Datenschutz – Checkliste

1. Ist ein Datenschutzbeauftragter bestellt und wann wurde dieser gemeldet? Wenn nein, warum wurde dieser nicht bestellt?

2. Existiert bei Ihnen ein Verzeichnis der Verarbeitungstätigkeiten?

Neu – erst ab 20 Personen mit Datenzugang

3. Werden geeignete Sicherheitsmaßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DSGVO getroffen?

4. Sind Beschäftigte zur weisungsgebundenen Verarbeitung personenbezogener Daten sensibilisiert?

5. Ist ein Verfahren vorhanden, mit denen auf Datenschutzverletzungen innerhalb von 72 Stunden reagiert werden kann?

Datenschutz – Checkliste

6. Wie wird die Einhaltung von Betroffenenrechten (Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sichergestellt?

7. Haben Sie Verträge mit Auftragsdatenverarbeitern erfasst?

8. Wie stellen Sie die Schulung/Sensibilisierung von Mitarbeitern sicher?

9. Gibt es Datenverarbeitungen, die auf einer Einwilligung beruhen und haben Sie hierzu entsprechende Einwilligungserklärungen?

10. Wie haben Sie sich als Unternehmen auf die DSGVO vorbereitet? Gibt es ein Konzept zur Umsetzung?

Verhalten bei unerwarteten Situationen

Verhalten bei unerwarteten Situationen

Durchsuchungsbeschluss der Staatsanwaltschaft

- Machen Sie keine Angaben außer die zur Person (Schweigen)
- Lassen Sie sich den Durchsuchungsbeschluss aushändigen
- Informieren Sie umgehend den Inhaber
- Keine Unterlagen bei Seite räumen
- Signalisieren Sie Kooperationsbereitschaft
- Händigen Sie nur Unterlagen aus, die im Durchsuchungsbeschluss genannt sind
- Lassen Sie sich Kopien der Daten und Unterlagen gaben.
- Lassen Sie sich die Unterlagen quittieren und stellen Sie klar, dass die Herausgabe nicht freiwillig, sondern aufgrund Beschluss erfolgte

Verhalten bei unerwarteten Situationen

Kontrolle Zoll

- Machen Sie keine Angaben außer die zur Person (Schweigen)
- Informieren Sie umgehend den Inhaber
- Notieren Sie den Namen der Beamten
- Nur die Einsicht in Lohn- und Meldeunterlagen muss geduldet werden
- Keine eigenmächtige Entnahme von Unterlagen ohne Durchsuchungsbeschluss
- Sind die Unterlagen beim Steuerberater können die Beamten dorthin verwiesen werden
- Privaträume sind ohne Durchsuchungsbeschluss tabu

Verhalten bei unerwarteten Situationen

Revision – Mitarbeiter des Versicherers

- Machen Sie keine Angaben außer die zur Person (Schweigen)
- Informieren Sie umgehend den Inhaber
- Nur der Inhaber tritt in Verhandlungen oder Gespräche
- Es besteht kein unmittelbares Herausgaberecht von Unterlagen oder Geräten
- Machen Sie vom Hausrecht Gebrauch wenn der Inhaber nicht anwesend ist

Vielen Dank für Ihre Teilnahme!

- Unterlagen sind ab morgen 10 Tage auf www.isv-treffpunkt.de abrufbar.
- Alle **Erstteilnehmer** schicken uns bitte Ihre Einwilligungserklärung zur Datenspeicherung per Dialog aus unserer Seminar-Seite
- Bitte geben Sie uns Ihr Feedback. Der Link kommt in Kürze per Mail
- Alle Info´s finden Sie auf unserer Homepage