DS-GVO für Unternehmen
und Vereine

schmid
datensicherheit

Datenschutz / EU-DS-GVO

1 Jahr DS-GVO:

..... **Wie ist die Lage?**

Bild: pixabay.com (Geralt, IO-Images)

NEW Landkreis Neustadt an der Waldnaab

26.06.2019, Neustadt/WN
02.07.2019, Vohenstrauß
10.07.2019, Grafenwöhr

Inhaltsübersicht

schmid datensicherheit

Datenschutz für Unternehmen und Vereine

- Überblick zu den Datenschutzgrundlagen
- Fragerunden
- Sanktionen
- Überwachungstätigkeit der bayerischen Aufsichtsbehörde
- Datenschutzbeauftragter und Auftragsverarbeitung
- Betroffenenrechte
- Datenschutzverletzungen
- Datenschutz im Internet
- Technischer Datenschutz und Informationssicherheit
- Werbung
- Bilder
- Kopieren von Personalausweisen
- Internationaler Datenverkehr
- Beschäftigtendatenschutz
- Vereine

schmid datensicherheit

Europäische Datenschutz-Grundverordnung

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016

EU-weit verpflichtend wirksam seit **25. Mai 2018**

Tätigkeitsbericht 2017/18 - Bayerisches Landesamt für Datenschutzaufsicht

Im Jahr 2018 in Bayern:

- 3643 Beschwerden
- 9212 Beratungen
- 2471 Datenschutzverletzungen
- (7293 DS-GVO-Meldungen beim. BundesDSB)

Datenschutz – Woher kommt das?

schmid datensicherheit

Ursprung der Rechtsprechung zum Datenschutz:

- **Informationelle Selbstbestimmung**
  Das Recht auf informationelle Selbstbestimmung ist im Recht Deutschlands das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (Rechtsprechung des Bundesverfassungsgerichts).
- **Europäische Menschenrechtskonvention**
  „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz."
  – EMRK Art. 8 Abs. 1
- **Persönlichkeitsrecht**
  Das allgemeine Persönlichkeitsrecht (APR) wird mit einem umfassenden Persönlichkeitsschutz aus Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) in Verbindung mit Art. 1 Abs. 1 GG (Menschenwürde) abgeleitet.
- **Unverletzlichkeit der privaten Wohnung**
  Das Grundrecht der Unverletzlichkeit der Wohnung dient als Freiheitsrecht vorrangig der Abwehr hoheitlicher Eingriffe in die Privatsphäre, welche die Wohnung bietet. Daneben gibt es dem Gesetzgeber den Auftrag, die Wohnung vor Privatpersonen zu schützen. Dieser Aufgabe kommt der Statt beispielsweise durch den Schutz der Wohnung im Rahmen des Straf- und Zivilrechts nach.
  – Deutsches Grundgesetz (GG) Art. 13 Abs. 1
- **Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**
  Dieses Recht wird im Grundgesetz nicht eigens genannt, sondern wurde als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts 2008 durch das Bundesverfassungsgericht derart formuliert bzw. aus vorhandenen Grundrechtsbestimmungen abgeleitet.

(Bilerd: pixabay.com; Texte sind teilweise Auszüge aus https://de.wikipedia.org/)

schmid datensicherheit

Ziele der EU-DS-GVO:

- EU-weiter einheitlicher wirksamer Schutz personenbezogener Daten (Stärkung und Präzisierung der Rechte der betroffenen Personen);
- Verschärfung der Auflagen für diejenigen, die personenbezogenen Daten verarbeiten und darüber entscheiden;
- EU-weite einheitliche Befugnisse der Mitgliedsstaaten (Vorschriften, Überwachung, Sanktionen);

Worauf bezieht sich "Daten"? [1]

schmid datensicherheit

Personenbezogenen Daten sind:

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Im Detail:

- **Name und Adresse**
- **Personalausweisnummer**
- **Kundennummer**
- **Mitgliedsnummer**
- **Online-Nutzername**
- **E-Mail-Adresse**
- **Telefonnummer**
- **IP-Adresse (!)**
- **Sprachaufzeichnung**
- **Geburtsdatum, Geburtsort**
- **Porträtfoto, Videoaufzeichnung einer Person**
- **...**

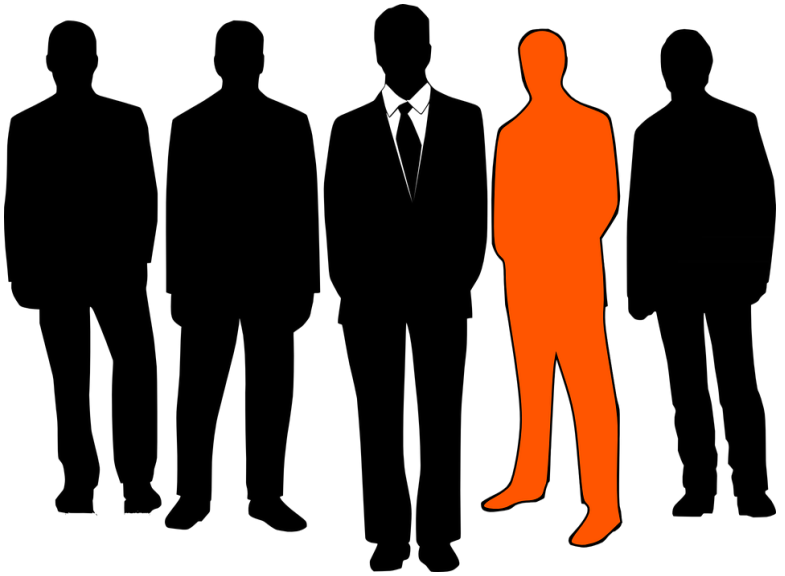


Bild: pixabay.com, OpenClipart-Vectors

Worauf bezieht sich "Daten"? [2]

schmid datensicherheit

Personenbezogenen Daten sind auch:

Daten, über die ein Personenbezug auf eine identifizierbare natürliche Person hergestellt werden kann. Im Detail:

- **Standortdaten**
- **Kontonummer**
- **Kennnummer**
- **Rentenversicherungsnummer**
- **Sozialversicherungsnummer**
- **Kfz-Kennzeichen**
- **...**

Deutsche Rentenversicherung

Bilder: geoportal.bayern.de/bayernatlas/, www.deutsche-rentenversicherung.de

Worauf bezieht sich "Daten"? [3]

schmid datensicherheit

Besondere Arten personenbezogener Daten, die in höherem Maße sensibel sind, unterliegen einem verschärften Schutz. Die Kategorien sind:

- **Rassische und ethnische Herkunft**
- **Politische Meinungen**
- **Religiöse oder weltanschauliche Überzeugungen**
- **Gewerkschaftszugehörigkeit**
- **Gesundheit und Sexualität**
- **Genetische und biometrische Daten zur eindeutigen Identifizierung einer Person**
- **Vermögens- und Finanzverhältnisse**

Erlaubte Verarbeitung

schmid datensicherheit

Voraussetzungen für eine erlaubte Datenverarbeitung:

- **Einwilligung der betroffenen Person**
- **Es gibt ein berechtigtes Interesse an der Datenverarbeitung und schutzwürdige Interessen des Betroffenen stehen dem nicht entgegen**
- **Die Datenverarbeitung ist erforderlich**
  - zur Erfüllung eines Vertrages
  - für vorvertragliche Maßnahmen auf eine Anfrage hin (z.B. für Versicherung)
  - zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen
  - zum Schutz lebenswichtiger Interessen der betroffenen oder einen anderen natürlich Person
  - im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt

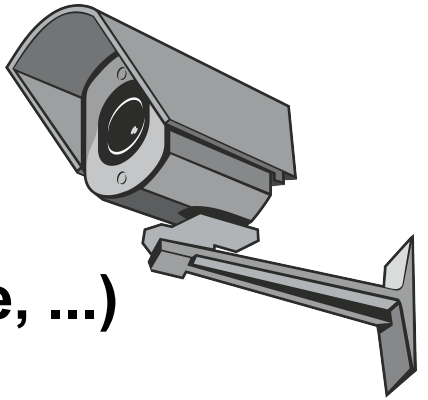
Datenschutz = Verbot mit Erlaubnisvorbehalt

Überblick zu Datenarten

schmid datensicherheit

Arten von personenbezogenen Daten:

- **Beschäftigtendaten**
- **Kundendaten**
- **Lieferantendaten (Ansprechpartner)**
- **Kommunikationsdaten (soz. Netzwerke)**
- **Gesundheitsdaten (Krankentage, Sportgruppen)**
- **Bewegungsprofile (Fahrzeugflotten)**
- **Überwachungsdaten (Videoaufzeichnungen)**
- **Daten über gekaufte Produkte (Händler)**
- **Mitgliederprofile (Stiftungen, Parteien, Vereine, ...)**
- **...**



Bilder: pixabay.com, OpenClipart-Vectors, 3dman_eu

Fragerunde 1

schmid datensicherheit

Verantwortlichkeit für die Verarbeitung, Art. 24 DS-GVO:

Wer innerhalb des Unternehmens ist für den Datenschutz verantwortlich und stellt nachweislich sicher, dass die Verarbeitung gemäß der DS-GVO erfolgt**?**

A) Der/die Datenschutzbeauftragte;

B) Die Unternehmensleitung;

C) Der/die Verantwortliche für die IT (IT-Leitung);

Fragerunde 1 (Antwort)

schmid datensicherheit

Verantwortlichkeit für die Verarbeitung, Art. 24 DS-GVO:

Wer innerhalb des Unternehmens ist für den Datenschutz verantwortlich und stellt nachweislich sicher, dass die Verarbeitung gemäß der DS-GVO erfolgt**?**

A) ~~Der/die Datenschutzbeauftragte~~;

B) Die Unternehmensleitung;

C) ~~Der/die Verantwortliche für die IT (IT-Leitung)~~;

Sanktionen

schmid datensicherheit

Artikel 83, Abs. 4 (bis 10 Mio. € oder 2% des weltweiten Vorjahresumsatzes), **Abs. 5 und 6** (bis 20 Mio. € oder 4% des weltweiten Vorjahresumsatzes)

Bilder: pixabay.com, JCamargo, L.J.Schmid

Abmahnungen und Verwarnungen

schmid datensicherheit

Abmahnungen:

- **die Sintflut von DS-GVO-Abmahnungen ist ausgeblieben;**
- **es besteht nach wie vor Unsicherheit, ob das UWG (unlauterer Wettbewerb) auf Belange des Datenschutzes anwendbar ist;**
- **die bisherigen Urteile dazu ergeben kein eindeutiges Ergebnis;**
- **Datenschutzbehörden werden verstärkte Kontrollen durchführen;**
- **Berufshaftpflicht kann nach DS-GVO-Verstößen bei Abmahnungen schützen** (nicht bei Bußgeldern)**;**

Im Jahr 2018 in Bayern:

- **keine Warnungen, Verwarnungen, Geldbußen oder Widerruf von Zertifizierungen (**auf Basis der DS-GVO**);**
- **Erlass von Anweisungen und Anordnungen;**

Verwarnungen und Bußgelder

schmid datensicherheit

Aufsichtsbehörden in anderen Bundesländern:

- **Versandunternehmen aus Hamburg soll 5.000 Euro Bußgeld wegen eines fehlenden Auftragsverarbeitungsvertrags zahlen (Art. 83 Abs. 4 DSGVO);**
- **Chat-Netzwerk hat personenbezogene Daten seiner Nutzer nicht ausreichend gesichert und wurde gehacked; Bußgeld in Höhe von 20.000 Euro, weil E-Mail-Adressen, Pseudonyme und Passwörter von circa 330.000 Nutzern im Netz veröffentlicht wurden;**
- **Privatperson verschickt vielfach E-Mails an Vertreter der Wirtschaft, Presse und Politik; Geldbuße von über 2.600 Euro wegen öffentlich sichtbaren Empfängerlisten (Adressaten in "An" und "CC", richtig: "BCC");**
- **Versehentliche Veröffentlichung von Gesundheitsdaten führt zu einer Geldbuße von 80.000.- + 4.000.- (Verfahrensgebühr) Euro;**
- **Telekomfiliale in Schleswig-Holstein übergibt einer Kundin einen USB-Stick, auf dem hunderte Urlaubsbilder, Nachrichten und Anrufprotokolle von anderen Telekom-Kunden gespeichert waren; das Verfahren läuft;**
- **Bisher wurden ca. 40 mal Bußgelder verhängt, (>50 Verwarnungen);**
- **Geldstrafen liegen in der Regel im 4- und 5-stelligen Bereich.**

Checkliste für Bußgelder

schmid datensicherheit

Schlussfolgerungen aus den bisher verhängten Bußgeldern:

- **Wenn Sie eine Datenpanne oder einen Datenschutzverstoß bemerken, holen Sie sofort fachlichen Rat ein und melden sie diesen ggf. bei der zuständigen Aufsichtsbehörde (72 Std. Meldefrist);**
- **Arbeiten Sie eng und transparent mit der Datenschutzbehörde zusammen und tun Sie alles, um den Schaden so gering wie möglich zu halten – das wirkt sich strafmildernd aus;**
- **Vergessen Sie nie, mit Dienstleistern einen Vertrag zur Auftragsverarbeitung abzuschließen und denken Sie daran:**
  Sie können die Verantwortung nicht abgeben,
  Sie bleiben Hauptverantwortlicher für den Datenschutz;
- **Achten Sie auch bei alltäglichem Schriftverkehr per E-Mail auf den Datenschutz und prüfen Sie besser mehrmals, dass keine Mail-Adressen öffentlich sichtbar sind (zusätzliche Adressaten immer "BCC" setzen);**

Fragerunde 2

schmid datensicherheit

Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO:

Innerhalb welches Zeitraums werden Sie bei der Ausübung des Rechts auf Auskunft den betroffenen Personen die vollständigen Informationen mitteilen**?**

A) Spätestens nach einem Monat – in begründeten Fällen könnten wir jedoch auch mehr Zeit benötigen;

B) Wie allgemein bekannt muss eine solche Auskunft innerhalb von zwölf Wochen erteilt werden – diese Frist halten wir ein;

C) Wenn der Aufwand für uns zu hoch ist, müssen gar keine Auskünfte erteilt werden – wie lange wir grundsätzlich brauchen, kann derzeit noch nicht abgeschätzt werden;

Fragerunde 2 (Antwort)

schmid datensicherheit

Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO:

Innerhalb welches Zeitraums werden Sie bei der Ausübung des Rechts auf Auskunft den betroffenen Personen die vollständigen Informationen mitteilen**?**

A) Spätestens nach einem Monat – in begründeten Fällen könnten wir jedoch auch mehr Zeit benötigen (die Begründung muss plausibel sein);

B) ~~Wie allgemein bekannt muss eine solche Auskunft innerhalb von zwölf Wochen erteilt werden – diese Frist halten wir wohl ein~~;

C) ~~Wenn der Aufwand für uns zu hoch ist, müssen gar keine Auskünfte erteilt werden – wie lange wir grundsätzlich brauchen, kann derzeit noch nicht abgeschätzt werden~~;

Datenschutzaufsicht

schmid datensicherheit

Bild: Bayerisches Landesamt für Datenschutzaufsicht, Ansbach

8. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für die Jahre 2017 und 2018

schmid datensicherheit

Einzelne Prüfaspekte (Details am Ende des Dokuments):

- **Videoüberwachung in Gastronomie und Kinos**
- **Kfz-Werkstätten-Kontrolle**
- **Patch Management bei WordPress-Websites**
- **WordPress GDPR Compliance Plugin**
- **Patch Management bei Magento-Websites**
- **Informationspflichten bei Bewerbungen**
- **Ransomware bei Arztpraxen**

DS-GVO-Prüfung bei kleinen und mittleren Unternehmen

schmid datensicherheit

Die DS-GVO verlangt von einem Verantwortlichen, dass die Einhaltung der DS-GVO nachgewiesen wird (Art. 5 Abs. 2 DS-GVO). Die Behörde kontrolliert daher, ob kleine und mittlere Unternehmen die wesentlichen Anforderungen der DS-GVO umsetzen.

Prüffragen:

(Kontrolle durch schriftliches Verfahren mit 20 Fragen, hier nur Auszug)

- **Ist ein Datenschutzbeauftragter bestellt und der Aufsichtsbehörde gemeldet?**
- **Gibt es ein Konzept im Unternehmen, wer bezogen auf den Datenschutz für was zuständig ist?**
- **Ist ein vollständiges Verarbeitungsverzeichnis vorhanden?**
- **Existiert ein Löschkonzept?**

Der betriebliche Datenschutzbeauftragte

schmid datensicherheit

Benennung eines betrieblichen Datenschutzbeauftragten:

- Allgemeine Vorschriften für die Benennung eines Datenschutzbeauftragten in Art. 37 Abs. 1 DS-GVO;
- § 38 Abs. 1 Satz 1 BDSG schreibt vor, dass bei mindestens zehn Personen, die mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, ebenfalls ein Datenschutzbeauftragter zu benennen ist.
- Dabei kommt es nach dem Gesetzeswortlaut darauf an, dass diese zehn Personen zum einen in der Regel sowie zum anderen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Zentrale Frage: Wann ist in einem Unternehmen oder bei einer anderen Stelle jemand „in der Regel“ sowie „ständig“ mit der automatisierten Verarbeitung personenbezogener Daten „beschäftigt“?

Funktion des DSB:

- **Der Datenschutzbeauftragte hat eine Beratungsfunktion und insoweit auch eine Überwachungsfunktion** (Art. 39 Abs. 1 Buchstabe b DS-GVO)**.**

Auftragsverarbeiter

schmid datensicherheit

Auftragsverarbeiter, Artikel 28 DS-GVO:

- Bei der Beauftragung eines Dienstleisters zur Auftragsverarbeitung ist grundsätzlich ein Vertrag mit datenschutzrechtlichen Regelungen vorgeschrieben.
- Auftragsverarbeitung im datenschutzrechtlichen Sinne liegt nach unserer Auffassung nur in Fällen vor, in denen eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird.
- Die Beauftragung mit fachlichen Dienstleistungen anderer Art, d. h. mit Dienstleistungen, bei denen nicht die Datenverarbeitung im Vordergrund steht bzw. bei denen die Datenverarbeitung nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt in der Regel keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.
- Die Verantwortlichkeit liegt beim Auftraggeber, der für die datenschutzrechtliche Verarbeitung beim Auftragsverarbeiter haftet.
- Wenn sich die verantwortliche Stelle und der Auftragsverarbeiter nicht auf einen Vertrag zur Auftragsverarbeitung einigen können, muss jegliche Verarbeitung von Daten durch den Auftragsverarbeiter unterbunden werden.

Fragerunde 3

schmid datensicherheit

Risiko für die Rechte und Freiheiten natürlicher Personen, insbesondere Art. 24 u. 32 DS-GVO:

Wie geht Ihr Unternehmen mit dem zentralen Datenschutz-Begriff des "Risikos" um, der sich wie ein roter Faden durch die gesamte DS-GVO zieht**?**

A) Wir meinen, das Datenschutzrisiko ermöglicht uns bei geplanten Verarbeitungen, die an sich keine Rechtsgrundlage haben, einen eigenen Ermessensspielraum, um die Verarbeitungen womöglich doch durchzuführen, wenn das Risiko nicht allzu hoch ist;

B) Wir werden künftig bei unseren Verarbeitungen unter Bezug der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung die jeweilige Eintrittswahrscheinlichkeit und die Schwere berücksichtigen, um Datenschutz-Risiken für Rechte und Freiheiten natürlicher Personen zu ermitteln;

C) Unser Unternehmen kennt den Begriff des Risikos bereits aus dem Bereich der IT-Sicherheit, so dass wir das Datenschutz-Risiko als mathematisches Produkt von Eintrittswahrscheinlichkeit und finanziellem Schaden ermitteln werden;

Fragerunde 3 (Antwort)

schmid datensicherheit

Risiko für die Rechte und Freiheiten natürlicher Personen, insbesondere Art. 24 u. 32 DS-GVO:

Wie geht Ihr Unternehmen mit dem zentralen Datenschutz-Begriff des "Risikos" um, der sich wie ein roter Faden durch die gesamte DS-GVO zieht**?**

A) ~~Wir meinen, das Datenschutzrisiko ermöglicht uns bei geplanten Verarbeitungen, die an sich keine Rechtsgrundlage haben, einen eigenen Ermessensspielraum, um die Verarbeitungen womöglich doch durchzuführen, wenn das Risiko nicht allzu hoch ist~~;

B) Wir werden künftig bei unseren Verarbeitungen unter Bezug der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung die jeweilige Eintrittswahrscheinlichkeit und die Schwere berücksichtigen, um Datenschutz-Risiken für Rechte und Freiheiten natürlicher Personen zu ermitteln;

C) ~~Unser Unternehmen kennt den Begriff des Risikos bereits aus dem Bereich der IT-Sicherheit, so dass wir das Datenschutz-Risiko als mathematisches Produkt von Eintrittswahrscheinlichkeit und finanziellem Schaden ermitteln werden~~;

Betroffenenrechte [1]

schmid datensicherheit

Informationspflichten:

- Eine praxistaugliche und angemessene Balance zwischen den Informationspflichten nach Art. 13 und 14 DS-GVO und der Gefahr einer Informationsermüdung bzw. Informationsüberhäufung bei den betroffenen Personen ist zu finden.
- Regelung aus Art. 12 Abs. 1 DS-GVO: Es sind geeignete Maßnahmen zu treffen sind, um die (Datenschutz-) Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.
- Es müssen immer die Informationen zur Identität des Verantwortlichen und zu den Zwecken der Verarbeitung gegeben werden, soweit diese Informationen nicht ohnehin schon wegen der Art des Kontakts mit der betroffenen Person offenkundig sind (z. B. bei deren Anruf zu einer Terminvereinbarung mit dem Friseur oder Steuerberater).
- Je nach Art des Kontakts mit der betroffenen Person ist ergänzend noch auf das Bestehen der Betroffenenrechte hinzuweisen. Dabei müssen alle Informationen nach Art. 13 bzw. 14 DS-GVO für die betroffene Person erhältlich sein bzw. gegeben werden (Link zu einer entsprechenden Website, Bereithalten eines entsprechenden Informationsblattes).

Betroffenenrechte [2]

schmid datensicherheit

Informationspflichten bei Karten-Zahlungen:

- Bei Zahlungsvorgängen mit EC- oder Kreditkarte sind Informationen an die bezahlenden Kunden situationsgerecht auszugeben.
- Empfohlen werden Hinweisaufkleber, Aufsteller oder kleinere Aushänge im Kassenbereich bzw. am Ladeneingang mit Informationen zu den Verantwortlichen sowie mit einem Internet-Link zu den weiteren Informationen. Ergänzend muss für Interessierte ein vollständiges Info-Blatt an der Kasse bzw. im Laden etc. erhältlich sein.

Informationspflichten bei Traueranzeigen:

- Bei der Aufgabe von gedruckten Traueranzeigen oder für Online-Medien muss der Veranlasser der Traueranzeige die übrigen darin genannten Personen (z. B. Angehörige) hierzu informieren, nicht etwa die Zeitung oder den Dienst selbst.

Informationspflichten am Telefon

- Bei Telefongesprächen können die Informationspflichten situations- und bedarfsgerecht in abgeschichteter Form ausreichend erfüllt werden.
- Entscheidend ist, wer den Anruf initiiert hat; (Zusendung eines Informationsblattes).

Betroffenenrechte [3]

schmid datensicherheit

Informationspflichten zur Gesprächsaufzeichnung in Callcentern:

- Eine Aufzeichnung von Telefongesprächen in Callcentern bedarf der informierten Einwilligung der externen Gesprächspartner.
- Eine datenschutzrechtlich wirksame Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO ist notwendig.
- Der datenschutzrechtlich Verantwortliche muss nachweisen können, dass die betroffene Person eine wirksame Einwilligung erteilt hat (Art. 7 Abs. 1 DS-GVO), er muss auch nachweisen können, dass die betroffene Person die Einwilligung „in informierter Weise“ abgegeben hat (vgl. Art. 4 Nr. 11 DS-GVO).

Informationspflichten bei Ärzten:

- Patienten müssen nicht unterschreiben, dass sie Datenschutzinformationen in der Arztpraxis zur Kenntnis genommen haben.
- Informationen können in der Praxis, bspw. im Wartebereich oder bei der Anmeldung, als Flyer oder Handout bereitliegen.
- Nachweispflichten sind erfüllt, wenn das Aushändigen der Information vermerkt wird oder ein konkreter Verfahrensablauf betreffend der Umsetzung der Informationspflicht dokumentiert ist, aus dem hervorgeht, wie die Patientin oder der Patient die Informationen im Regelfall erhält.
- Eine Verweigerung der Behandlung wegen einer bloßen Verweigerung der ohnehin nicht erforderlichen Unterschrift durch den Patienten ist nicht mit der DS-GVO vereinbar.

Betroffenenrechte [4]

schmid datensicherheit

Auskunftsrecht bei Ärzten:

- Patienten, die ihr Recht auf Auskunft gelten machen, ist eine vollständige Übersicht der Daten in verständlicher Form von den Arztpraxen zu geben, ohne dass dabei medizinische Fachbegriffe erläutert werden müssen.

Kopien von Unterlagen bei Auskunft:

- Das Auskunftsrecht über gespeicherte personenbezogene Daten begründet keinen allgemeinen Anspruch auf Kopien von Dokumenten oder Akten.
- Nach Art. 15 Abs. 3 DS-GVO ist nur eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind“, zur Verfügung zu stellen.
- Manche bereichsspezifische Vorschriften gehen über den datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DS-GVO hinaus, wie z. B. § 630g BGB mit einem Recht von Patienten auf elektronische Abschriften der Patientenakte, allerdings gegen Kostenerstattung.

Betroffenenrechte [5]

schmid datensicherheit

Informationspflicht gegenüber nicht-deutschen Betroffenen:

- Betroffene müssen so informiert werden, dass sie eine geplante Verarbeitung verstehen.
- Dazu müssen auch fremdsprachige Informationen zur Verfügung stehen.
- Auch Kindergärten mit verschiedenen Nationalitäten müssen die Sprache der Kinder und deren Eltern berücksichtigen.

Bilder: pixabay.com, geralt, MonikaP

Betroffenenrechte [6]

schmid datensicherheit

Grundsatz der Datensparsamkeit:

- Verarbeitende Stellen dürfen nur die für die Zwecke der Verarbeitung notwendigen Daten erheben und speichern. Der Betroffene muss nur notwendige Daten an die verarbeitende Stelle aushändigen.

Allgemeines zum Recht auf Berichtigung:

- Das Recht auf Berichtigung ist ein zentrales Datenschutzrecht für betroffene Personen.

Berichtigung eines Werturteils in Versicherungs- oder Arztakten:

- Gespeicherte Werturteile sind einem Berichtigungs- bzw. Löschanspruch zugänglich.
- Gespeicherte Werturteile über eine Person wie „unverschämt“, „zahlungsunwillig“, „schleppende Zahlungsweise“ müssen im Falle eines Bestreitens durch die beurteilte Person von dem Verantwortlichen entweder hinreichend belegt werden können oder je nach Sachverhalt berichtigt bzw. sogar gelöscht werden.

Betroffenenrechte [7]

schmid datensicherheit

Löschung bei Werbung:

- Die Löschung der Postadresse bei einem Werbeversender verhindert nicht automatisch die spätere Zusendung von Postwerbung.
- Möchte die betroffene Person vorrangig von einer werblichen Ansprache durch ein Unternehmen verschont bleiben, ist dafür die Aufnahme ihrer Kontaktdaten in eine Werbesperrdatei bei diesem Unternehmen das richtige Mittel zur Berücksichtigung ihres Willens.
- Wünscht eine betroffene Person ausdrücklich und allein eine Löschung aller Daten, sollte sie darauf hingewiesen werden, dass sie bei einem künftigen – rechtlich zulässigen – Einsatz von Fremddaten eventuell wieder Werbung erhalten kann.

Betroffenenrechte [8]

schmid datensicherheit

Löschung bei Patientendaten:

- Patientendaten sind nicht in jedem Fall auf Wunsch der betroffenen Person zu löschen.
- Personenbezogene Daten sind zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 Buchstabe a DS-GVO). Eine Löschpflicht besteht hier auch ohne Aufforderung durch den Betroffenen.
- Gemäß Art. 17 Abs. 3 DS-GVO dürfen Daten nicht gelöscht werden, wenn für diese eine gesetzliche Pflicht zur Aufbewahrung besteht.
- Für Schadensersatzansprüche wegen Körper- oder Gesundheitsverletzungen beträgt die objektive Verjährungsfrist gemäß § 199 Abs. 2 BGB dreißig Jahre (siehe Art. 17 Abs. 3 Buchstabe e DS-GVO, Rechtsansprüche).

Fragerunde 4

schmid datensicherheit

Recht auf Datenübertragbarkeit, Art. 20 DS-GVO:

Können Sie die Daten einer betroffenen Person bei Bedarf in einem strukturierten, gängigen und maschinenlesbaren Format zurückgegeben**?**

A) Wir werden prozessuale und technische Vorkehrungen treffen, um Daten übertragbar vorzuhalten – bei Bedarf könnte der Betroffene dann einen entsprechenden Output seiner Daten erhalten;

B) Eine betroffene Person kann standardmäßig die in unserem Unternehmen hinterlegten Stammdaten als Text-Datei erhalten – sollten weitere Daten gewünscht sein, muss dies explizit angegeben werden;

C) Eine Datenübertragbarkeit können wir nicht gewährleisten, da unsere Organisation und Systeme nicht ausreichend dafür ausgelegt sind - eine Aktualisierung wäre unwirtschaftlich;

Fragerunde 4 (Antwort)

schmid datensicherheit

Recht auf Datenübertragbarkeit, Art. 20 DS-GVO:

Können Sie die Daten einer betroffenen Person bei Bedarf in einem strukturierten, gängigen und maschinenlesbaren Format zurückgegeben**?**

A) Wir werden prozessuale und technische Vorkehrungen treffen, um Daten übertragbar vorzuhalten – bei Bedarf könnte der Betroffene dann einen entsprechenden Output seiner Daten erhalten;

B) ~~Eine betroffene Person kann standardmäßig die in unserem Unternehmen hinterlegten Stammdaten als Text-Datei erhalten – sollten weitere Daten gewünscht sein, muss dies explizit angegeben werden~~;

C) ~~Eine Datenübertragbarkeit können wir nicht gewährleisten, da unsere Organisation und Systeme nicht ausreichend dafür ausgelegt sind - eine Aktualisierung wäre unwirtschaftlich~~;

Betroffenenrechte [9]

schmid datensicherheit

Allgemeines zum Recht auf Datenübertragbarkeit:

- Das Recht auf Datenübertragbarkeit ist eines der neuen Instrumente der DS-GVO und soll den betroffenen Personen bessere Kontrolle über ihre Daten bieten.
- Das in Art. 20 DS-GVO verankerte Recht auf Datenübertragbarkeit, das meist auch unter Recht auf Datenportabilität bekannt ist, stärkt die Rechte der betroffenen Personen gerade im Bereich digitaler Dienste, wie z. B. bei sozialen Netzwerken.
- Zweck der Vorschrift ist es primär, den Wettbewerb um datenschutzfreundliche Produkte und Dienstleistungen zu fördern.
- Das Recht auf Datenübertragbarkeit bezieht sich dem Wortlaut nach nur auf diejenigen personenbezogenen Daten, die die betroffene Person einem Verantwortlichen bereitgestellt hat.

Datenübertragbarkeit bei Ärzten:

- In der Regel besteht kein Anspruch auf Datenportabilität für Patienten gegenüber Ärzten oder medizinischen Laboren.

Datenschutzverletzungen [1]

schmid datensicherheit

Meldung an die Aufsichtsbehörde und Betroffene (Art. 33, 34):

- Bei hohem Risiko Aufsichtsbehörde und betroffene Personen benachrichtigen.
- Bei (normalen) Risiko nur die Aufsichtsbehörde benachrichtigen.
- Datenschutzverletzungen immer dokumentieren, evtl. keine Meldung notwendig.

Prüfung der Aufsichtsbehörde nach grobem Grundschema:

- Wurde die Risikoeinschätzung vom Verantwortlichen richtig durchgeführt?
- Wurden bei hohem Risiko die betroffenen Personen informiert?
- Sind die eingeleiteten Abhilfemaßnahmen zur Schadenseindämmung ausreichend?
- Wurde die Ursache der Datenschutzverletzung, sofern strukturell bedingt, durch geeignete technische und organisatorische Maßnahmen zur Minderung der Wahrscheinlichkeit zukünftiger Vorfälle erkannt und beseitigt?

Datenschutzverletzungen [2]

schmid datensicherheit

Bedrohungen für Verantwortliche aus dem Cybersicherheitsumfeld:

- Sicherheitslücke bei Hotelbuchungssoftware:
  Cyberkriminelle stehlen Kreditkartendaten über Ausnutzung einer Lücke.
- Kryptomining auf Webservern:
  Über unzureichend geschützte Serverressourcen wird Kryptowährung geschürft.
- Erpressung nach Cyberangriff:
  Nach Datendiebstahl verlangen Kriminelle Lösegeld, sonst Veröffentlichung.
- Kundendaten aus Shop-System online einsehbar:
  Kundendaten öffentlich einsehbar durch mangelnde Sorgfalt bei Konfigurations- und Wartungsarbeiten am Server.
- Hacking von eBay-Accounts:
  Online-Zugänge nicht nur mit Passwort schützen, sondern mit zweitem Faktor.
- Angriffe auf den Login bei Online-Shops:
  Online-Shops werden permanent angegriffen – nur aktuell gehaltene Systeme können effektiv standhalten und Kundenlogins angemessen schützen.

Fragerunde 5

schmid datensicherheit

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Art. 33 DS-GVO:

Wann meldet Ihr Unternehmen künftig eine Datenschutzverletzung bei der zuständigen Aufsichtsbehörde, z. B. bei einem Hacking-Vorfall, Diebstahl oder Fehlversendung**?**

A) Eine Meldung an die Aufsichtsbehörde planen wir durchzuführen, wenn es sich mit unseren eigenen Interessen deckt – sollte dies der Fall sein, wird innerhalb von 7 Tagen gemeldet;

B) Wir beabsichtigen grundsätzlich keine Meldungen dieser Art zu praktizieren, da wir keine Notwendigkeit darin erkennen;

C) Wir versuchen, möglichst binnen 72 Stunden ab Kenntniserlangung jeden relevanten Vorfall an die Aufsichtsbehörde zu melden;

Fragerunde 5 (Antwort)

schmid datensicherheit

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Art. 33 DS-GVO:

Wann meldet Ihr Unternehmen künftig eine Datenschutzverletzung bei der zuständigen Aufsichtsbehörde, z. B. bei einem Hacking-Vorfall, Diebstahl oder Fehlversendung**?**

A) ~~Eine Meldung an die Aufsichtsbehörde planen wir durchzuführen, wenn es sich mit unseren eigenen Interessen deckt – sollte dies der Fall sein, wird innerhalb von 7 Tagen gemeldet~~;

B) ~~Wir beabsichtigen grundsätzlich keine Meldungen dieser Art zu praktizieren, da wir keine Notwendigkeit darin erkennen~~;

C) Wir versuchen, möglichst binnen 72 Stunden ab Kenntniserlangung jeden relevanten Vorfall an die Aufsichtsbehörde zu melden;

Datenschutz im Internet [1]

schmid datensicherheit

Datenschutzbestimmungen auf Websites:

- Eine DS-GVO gesetzeskonforme Datenschutzerklärung für einen Internetauftritt obliegt dem Verantwortlichen der Website.
- Websitebetreiber haben nach DS-GVO zahlreiche, zum Teil auch neue Informationspflichten.
- Die Datenschutzerklärung muss vollständig und inhaltlich richtig sein und den Informationspflichten (Art. 13) nachkommen.
- Durch umfassende, konkrete Überprüfung des jeweiligen internen Umgangs mit den personenbezogenen Daten der Nutzer beim Verantwortlichen ergibt sich ein Teil der Erklärung.
- Durch eine technische Überprüfung des Internetauftritts und Verhaltens der Webseiten ergibt sich ein weiterer Teil der DS-Erklärung.
- Bei der Nutzung von im Internet frei abrufbaren Textgeneratoren für Datenschutzerklärungen ist darauf zu achten, dass die damit erstellte Datenschutzerklärung auf den individuellen Internetauftritt abgestimmt ist.

Datenschutz im Internet [2]

schmid datensicherheit

Einbindung von Cookies auf Websites und „Cookie-Banner“:

- Mit einem sog. „Cookie-Banner“ soll eine Einwilligung des Nutzers eingeholt und über die Datenverarbeitung informiert werden.
- Eine Vielzahl dieser Cookie-Banner erfüllt die datenschutzrechtlichen Anforderungen **nicht**. Folgendes ist zu beachten:
  - Beim erstmaligen Öffnen einer Website, erscheint das Banner.
  - Das Banner blockiert zunächst alle Skripte einer Website.
  - Erst wenn der Nutzer seine Einwilligung durch eine aktive Handlung abgegeben hat, darf die Datenverarbeitung stattfinden.
  - Diese Aktion des Nutzers, die Abgabe der Einwilligung, wird vom Verantwortlichen gespeichert.
  - Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zum Widerruf implementiert werden.
  - Die Einwilligung umfasst nicht nur das Setzen von Cookies, sondern alle einwilligungsbedürftigen Verarbeitungstätigkeiten, wie z.B. Tracking im Browser oder Verfahren zur Verfolgung der Nutzer durch Zählpixel oder Canvas Fingerprinting.

Datenschutz im Internet [3]

schmid datensicherheit

Kontaktaufnahme, WhatsApp, Facebook:

- Kontaktformulare:
  Kontaktformulare können unter Berücksichtigung weniger Anforderungen mühelos auf Websites zur Verfügung gestellt werden. Prüfung: HTTPS, Rechtsgrundlage, besondere Kategorien von pers. Daten, Pflichtfelder.
- WhatsApp:
  Hinsichtlich des Einsatzes von WhatsApp im beruflichen Umfeld bestehen große Datenschutzbedenken.
- Facebook Custom Audience über die Kundenliste:
  Der Bayerische Verwaltungsgerichtshof bestätigt die Anordnung der Aufsichtsbehörde hinsichtlich Facebook Custom Audience (Werbekampagne unzulässig).
- Facebook-Fanpages:
  Fanpage-Betreiber haben auf Facebook eine datenschutzrechtliche Verantwortung gegenüber den Fanpage-Nutzern (Verarbeitung unklar).

Technischer Datenschutz und Informationssicherheit [1]

schmid datensicherheit

Risiko, Cybersicherheit, Technikgestaltung, DSFA:

- Risikoorientierter Ansatz unter der DS-GVO:
  Der zentrale **Risiko**-Begriff ist das wesentliche Element für die Auswahl geeigneter Schutzmaßnahmen – Standardchecklisten für technische und organisatorische Maßnahmen haben ausgedient.
- Cybersicherheit als gesetzliche Datenschutzkomponente:
  Cyberkriminelle abzuwehren dient nicht nur den eigenen wirtschaftlichen Interessen, sondern ist auch **gesetzliche Datenschutzanforderung** für Verantwortliche zum Schutz personenbezogener Daten.
- Datenschutz durch Technikgestaltung:
  Der technische Datenschutz durchdringt als wichtiges Datenschutzelement fast alle Verarbeitungsbereiche, die Umsetzung ist ein **kontinuierlicher Prozess**.
- Datenschutz-Folgenabschätzung (DSFA):
  Die Datenschutz-Folgenabschätzung ist eine besondere Herangehensweise bei Verarbeitungen von personenbezogenen Daten mit hohem Risiko.

Technischer Datenschutz und Informationssicherheit [2]

schmid datensicherheit

TOMs, HTTPS, Mail-Verschlüsselung, Löschkonzepte:

- Wirksamkeitsprüfung im Rahmen der Rechenschaftspflicht:
  Technische und organisatorische Maßnahmen müssen auch auditiert und fortwährend angepasst werden.
- HTTPS-Verschlüsselung und HTTPS-Prüfung:
  Viele Verantwortliche haben immer noch Probleme damit, eine wirksame **Transportverschlüsselung** auf ihrer Website einzusetzen.
  Verantwortliche müssen beim Betrieb von Websites sicherstellen, dass personenbezogene Daten angemessen geschützt und damit auch sicher übertragen werden. Implementierung eines HTTPS-Zertifikats und Konfiguration der Kommunikationsparameter muss nach den gesetzlichen Anforderungen erfolgen (Stand der Technik).
- E-Mail-Verschlüsselung:
  Die DS-GVO erfordert den Schutz personenbezogener Daten auch bei E-Mails. Eine Transportverschlüsselung zwischen E-Mail-Client und Provider wird vorausgesetzt. Die Verschlüsselung des Inhalts muss im Einzelfall in Erwägung gezogen werden (Stand der Technik).
- Löschen unter der DS-GVO:
  Mit der DS-GVO endet die Zeit des unter dem BDSG-alt bekannten Sperrens von Daten – **Löschkonzepte** werden dagegen wichtiges Datenschutzelement.

Fragerunde 6

schmid datensicherheit

Sicherheit der Verarbeitung, Art. 32 DS-GVO:

Sind in Ihrem Unternehmen alle Systeme, Prozesse und Menschen bezüglich der Angriffsmöglichkeiten durch Cyberkriminelle ausreichend sensibilisiert und geschützt**?**

A) Durch Sicherheitsprodukte ist ein entsprechender Schutz in unserem Unternehmen gewährleistet;

B) Cybersicherheit ist uns ein wichtiges Anliegen, um die Vorgaben der DS-GVO einhalten zu können - entsprechend widmen wir diesem Bereich besonders viel Aufmerksamkeit;

C) Da wir nicht im Visier von Cyberkriminellen stehen, stellen diese für uns kein echtes Datenschutzproblem dar;

Fragerunde 6 (Antwort)

schmid datensicherheit

Sicherheit der Verarbeitung, Art. 32 DS-GVO:

Sind in Ihrem Unternehmen alle Systeme, Prozesse und Menschen bezüglich der Angriffsmöglichkeiten durch Cyberkriminelle ausreichend sensibilisiert und geschützt**?**

A) ~~Durch Sicherheitsprodukte ist ein entsprechender Schutz in unserem Unternehmen gewährleistet~~;

B) Cybersicherheit ist uns ein wichtiges Anliegen, um die Vorgaben der DS-GVO einhalten zu können - entsprechend widmen wir diesem Bereich besonders viel Aufmerksamkeit;

C) ~~Da wir nicht im Visier von Cyberkriminellen stehen, stellen diese für uns kein echtes Datenschutzproblem dar~~;

Intermission

schmid datensicherheit

PAUSE

Informationssicherheit [1]

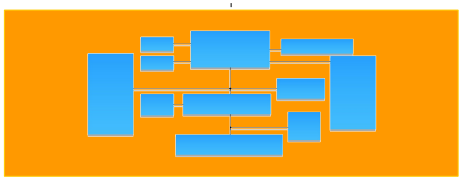
schmid datensicherheit

Nutzung von Schwachstellen

Bilder: pixabay.com

Technische Mängel

Menschliches Fehlverhalten



Organisatorische Mängel

Informationssicherheit [2]

schmid datensicherheit

Risiken der Informations- und Kommunikationtechnik

Potentielle Angreifer

- Cyberkriminelle
- Wettbewerber
- Hacker
- Nachrichtendienste und staatliche Stellen
- Beschäftigte
- Script-Kiddies

Motivation

- Kontrolle über Systeme
- Löse- und Schweigegeld
- Kreditkartendaten
- Identitätsdiebstahl
- Kundendaten
- Soziale Gründe (Rache, Frust)
- Unternehmenspläne (neue Aufträge, neue Entwicklungen, Patentvorbereitungen)
- Ausschreibungen

Folgen

- Verlust geschäftsrelevanter, kritischer Daten
- Umsatzverluste bis hin zur Insolvenz
- Stillstand des Geschäftsbetriebs
- Vertrauensverlust / Reputationsschäden
- Kosten für die Benachrichtigung Betroffener (Kunde/ Lieferanten/Partner)
- Sanktionen durch Aufsichtsbehörden

Informationssicherheit [3]

schmid datensicherheit

Einbruchdiebstahl

Schadenskosten:

- Direkte Kosten des Einbruchs (Schäden + Ermittlungen, Stillstand)
- Arbeitsausfall durch fehlendes Werkzeug
- Umsatzausfall durch nicht vorhandene Ware
- Kosten für Nachkauf der gestohlenen Güter
- Versicherungskosten steigen
- Reputationsverlust

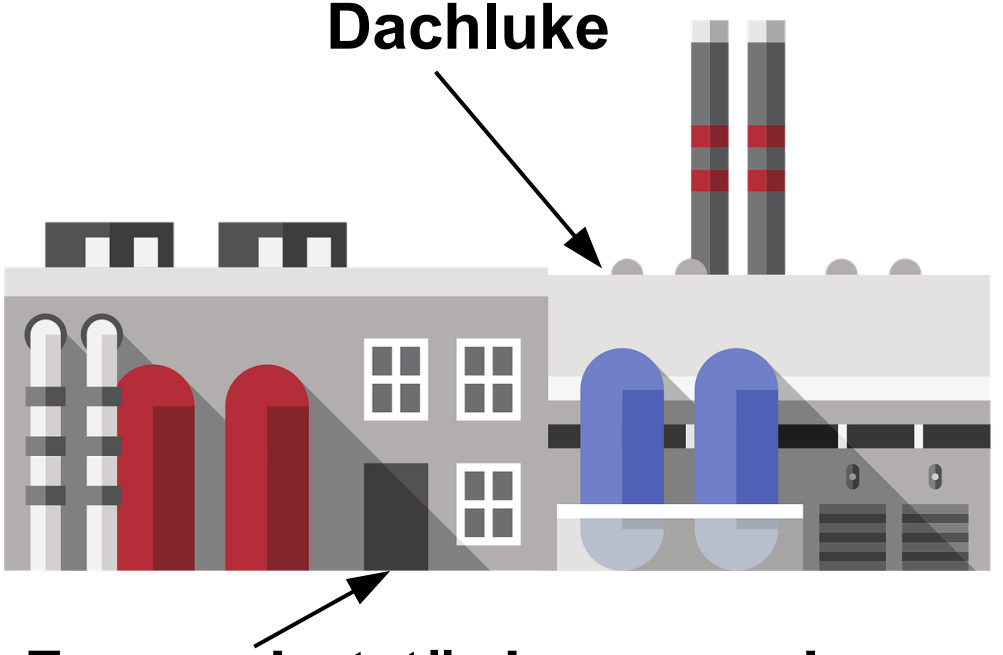


Bild: pixabay.com

Informationssicherheit [4]

schmid datensicherheit

Angriffe auf Webseiten

Beispiel: WordPress-Plugin Wordfence

Top 10 Countries Blocked

Country	Total IPs Blocked	Block Count
United Kingdom	17	216
United States	110	153
Russian Federation	5	90
France	32	80
Vietnam	39	54
Singapore	24	38
Germany	31	36
India	25	28
Netherlands	15	18
Canada	12	18

Top 10 Failed Logins

Username	Login Attempts	Existing User
admin	199	No
admin1	1	No

Screenshots: Wordfence

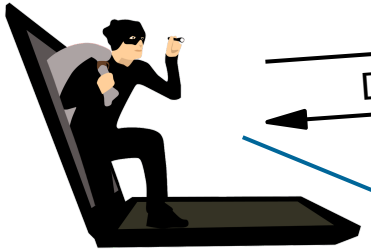
Informationssicherheit [5]

schmid datensicherheit

E-Mail-Betrug

1. Angreifer holt sich Informationen über den Dienstleister

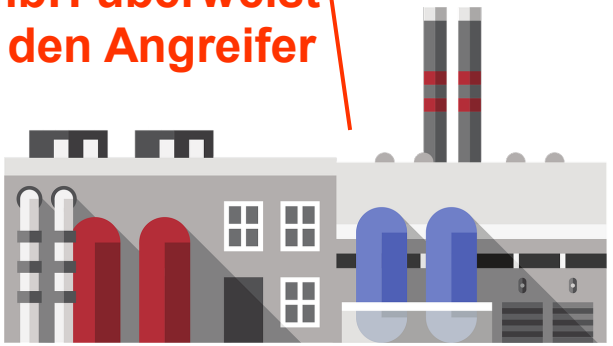
Die Mustermann GmbH ist Kunde des Dienstleisters



Dienstleister

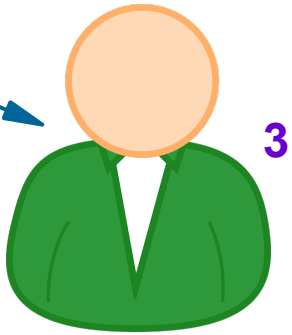
2. Angreifer sendet gefälschte E-Mail an Mitarbeiter der Mustermann GmbH

5. Die Mustermann GmbH überweist an den Angreifer



Mustermann GmbH

4. Änderung der Kontonummer für die Bezahlung des Dienstleisters



3. Mitarbeiter hält E-Mail für echt

Mitarbeiter der Mustermann GmbH

Bild: pixabay.com

Informationssicherheit [6]

schmid datensicherheit

Emotet – Multifunktionstrojaner

- Cyber-Kriminelle haben die Methoden hochprofessioneller Angriffe adaptiert und automatisiert (Advanced Persistent Threat Attacks)
- Opfer soll Dateianhang öffnen (z.B. Telekom-Rechnungsmail, Bewerbungsdaten in Excel-Tabelle)
- Kontaktbeziehungen und E-Mail-Inhalte werden aus den Postfächern infizierter Systeme ausgelesen
- Emotet verschickt authentisch aussehende Spam-Mails, die automatisiert erzeugt werden („Outlook-Harvesting“)
- Empfänger erhält fingierte Mails von Absendern, mit denen sie kürzlich in Kontakt standen

---

- Emotet ist äußerst gefährlich und perfide, weil vielseitig einsetzbar
- Lädt Banking-Trojaner Trickbot oder Krypto-Mining-Trojaner auf infizierten Computer
- Kopiert Passwörter aus Browsern und Mail-Clients
- Verbreitet sich wurmartig in Netzwerken u. versteckt sich effektiv vor Schutzsoftware
- Angreifer erhalten vollständigen Remote-Zugriff auf das infizierte System
- Emotet modifiziert sich ständig und wird selten von Virenschutzprogrammen erkannt

Fragerunde 7

schmid datensicherheit

Sicherheit der Verarbeitung, Art. 32 DS-GVO:

Wie gewährleisten Sie die Sicherheit der Verarbeitung personenbezogener Daten in Ihrem Unternehmen und können diese notfalls auch der Aufsichtsbehörde nachweisen**?**

A) Wir planen ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit unserer technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung;

B) Wir schützen unsere Server und PCs mit Firewalls und Virenscanner - es findet dabei ein umfassendes Monitoring durch unsere IT-Abteilung statt, so dass wir dies der Aufsichtsbehörde mitteilen können;

C) Wir werden eine IT-Zertifizierung (z. B. ISO/IEC 27001) anstreben und so einen ausreichenden Nachweis erhalten;

Fragerunde 7 (Antwort)

schmid datensicherheit

Sicherheit der Verarbeitung, Art. 32 DS-GVO:

Wie gewährleisten Sie die Sicherheit der Verarbeitung personenbezogener Daten in Ihrem Unternehmen und können diese notfalls auch der Aufsichtsbehörde nachweisen**?**

A) Wir planen ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit unserer technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung;

B) ~~Wir schützen unsere Server und PCs mit Firewalls und Virenscanner - es findet dabei ein umfassendes Monitoring durch unsere IT-Abteilung statt, so dass wir dies der Aufsichtsbehörde mitteilen können~~;

C) Wir werden eine IT-Zertifizierung (z. B. ISO/IEC 27001) anstreben und so einen ausreichenden Nachweis erhalten; (möglich, aber DS berücksichtigen);

Wichtig: Cybersicherheit ist eine gesetzliche Datenschutzkomponente !

Informationssicherheit [7]

schmid datensicherheit

Maßnahmen

- Schulung und Sensibilisierung der Mitarbeiter
- Organisatorische Maßnahmen
- Präzise Regelungen und Verpflichtungen
- Dokumentation der Prozesse und Verarbeitungen
- Prüfung der verarbeiteten Daten und des Umgangs mit diesen Daten
- Technische Maßnahmen, Identifikation, Verschlüsselung

- Zeitnahe Installation von den Herstellern bereitgestellter Sicherheitsupdates
- Einsatz zentral administrierter AV-Software
- Regelmäßige Durchführung von mehrstufigen Datensicherungen (Backups)
- Regelmäßiges manuelles Monitoring von Logdaten
- Netzwerk-Segmentierung (Trennung von Client-/Server-/Domain-Controller-Netzen sowie Produktionsnetzen)
- Nur die zur Aufgabenerfüllung notwendigen Berechtigungen für Nutzer vergeben
- Deaktivierung von Makros und OLE-Objekten in Microsoft Office, Verwendung von signierten Makros (= eine von verschiedenen Maßnahmen gegen Emotet)

Technik und Medienrecht

schmid datensicherheit

Datenschutz durch Technikgestaltung

- Für einen zu erzielenden Zweck muss jeweils die Lösung gewählt werden, die am wenigsten in die Grundrechte der betroffenen Person eingreift.
- In der DS-GVO findet sich der Verweis auf den „Stand der Technik“.
- „Stand der Technik“ soll sicherstellen, dass die in der Praxis beste verfügbare Technik zum Einsatz kommt.

Telemediengesetz (TMG)

- Der Gesetzgeber hat das Telemediengesetz (TMG) bisher nicht an die DS-GVO angepasst.
- Die DS-GVO kommt für sämtliche automatisierte Verarbeitungen personenbezogener Daten vorrangig zur Anwendung (Ausnahmen beachten).
- Rechtsgrundlage für die Verarbeitung ist nur Artikel 6 Absatz 1, insbesondere Buchstaben a), b) und f) DS-GVO (Interessenabwägung im Einzelfall).
- Allgemeine Grundsätze aus Artikel 5 Absatz 1 DS-GVO, sowie die besonderen Vorgaben z. B. aus Artikel 25 Absatz 2 DS-GVO einhalten.

Fragerunde 8

schmid datensicherheit

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5 Abs. 1 lit. f (angemessene Sicherheit) DS-GVO:

Warum ist es wichtig, mit kritischen Internetdiensten mittels HTTPS oder TLS (SSL) verbunden zu sein**?**

A) HTTPS verhindert die Vorratsdatenspeicherung der Liste der von Ihnen besuchten Webseiten;

B) HTTPS schützt Sie vor CEO Fraud und anderen Phishing-Angriffen;

C) Sichere Verbindungen garantieren die Richtigkeit einer Internetadresse bzw. eines Links;

D) HTTPS-geschützte Verbindungen garantieren die Verschlüsselung von übertragenen Daten sowie die Identität des Server-Besitzers;

Fragerunde 8 (Antwort)

schmid datensicherheit

Grundsätze für die Verarbeitung personenbezogener Daten, Art. 5 Abs. 1 lit. f (angemessene Sicherheit) DS-GVO:

Warum ist es wichtig, mit kritischen Internetdiensten mittels HTTPS oder TLS (SSL) verbunden zu sein**?**

A) ~~HTTPS verhindert die Vorratsdatenspeicherung der Liste der von Ihnen besuchten Webseiten~~;

B) ~~HTTPS schützt Sie vor CEO Fraud und anderen Phishing-Angriffen~~;

C) ~~Sichere Verbindungen garantieren die Richtigkeit einer Internetadresse bzw. eines Links~~;

D) HTTPS-geschützte Verbindungen garantieren die Verschlüsselung von übertragenen Daten (Integrität, Vertraulichkeit) sowie die Identität des Server-Besitzers;

Werbung [1]

schmid datensicherheit

Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung:

- Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO
- Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO
  - Erwägungsgrund (ErwGr.) 47 DS-GVO, berechtigtes Interesse des Verantwortlichen

Versand von Grüßen und Glückwünschen:

- Die Versendung von Weihnachts-, Neujahrs- und sonstigen Glückwunschkarten wird durch die DS-GVO nicht verhindert.
- Widerspruchseingaben von Betroffenen gegen Werbung beachten.
- Wenn bei bestehenden Geschäfts- oder Kundenbeziehungen die gesetzlich vorgesehenen Informationen nach Art. 13 und Art. 21 Abs. 4 DS-GVO schon im Laufe des Jahres erfolgt sind, können diese Informationen bei den Weihnachts- oder Neujahrsgrüßen unterbleiben
  (wo sie ohnehin nur störend wirken würden).

Werbung [2]

schmid datensicherheit

Zustimmung zur Werbung und Koppelungsverbot:

- **Kostenlose E-Mail-Accounts (**Beispiel für einen Dienst**) mit einer dazu vereinbarten Werbe-Newsletter-Zusendung sind weiterhin möglich.**
- **In der Praxis gibt es vielfach kostenlose Dienstleistungsangebote, die die Nutzer mit der Zustimmung für eine werbliche Nutzung ihrer Daten „bezahlen“, z. B. ein kostenloser E-Mail-Account gegen die Zustimmung für Werbe-Newsletter-Zusendung als „Gegenfinanzierung“ (= Koppelung).**
- **Die Aufsichtsbehörde gehen bei solchen Geschäftsmodellen von einer vertraglichen Grundlage für die Verarbeitung der personenbezogenen Daten gemäß Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO aus.**
  - Die Gegenleistung des Nutzers, d. h. die Zustimmung zur Verarbeitung seiner Daten für die Zusendung eines Werbe-Newsletters, muss bei Vertragsabschluss über die vereinbarte kostenlose Dienstleistung klar und verständlich dargestellt werden, damit ein Nutzer eine sachgerechte Entscheidungsgrundlage hat (Transparenz).
- **Direkte Verknüpfungen von Einwilligungen mit Verträgen ist Kopplung.**

Marketing

schmid datensicherheit

Zustimmung zur Kontaktaufnahme und zur Analyse:

- **Die Nutzung von personenbezogenen Daten muss auf einer Rechtsgrundlage basieren (insbesondere Marketing-Maßnahmen).**
- **E-Mail-Werbung erfordert eine Einwilligung.**
- **Newsletter und ähnliches erfordert Double Opt-in-Zustimmung.**
- **Kontakte zu Bestandskunden können in begrenztem Umfang über Art. 6 Abs. 1 lit. f mittels einer Interessenabwägung erfolgen (berechtigte Interessen des Verantwortlichen).**
- **Google-Analytics erfordert eine Einwilligung auf der Webseite (Pop-up-Abfrage).**
- **Ohne Einwilligung dürfen keine Google-Dienste aktiviert werden.**
- **Die Nutzung von Google-Diensten erfordert einen Auftragsverarbeitungsvertrag (Google bietet jeweils verschiedene AV-Verträge für unterschiedliche Dienste).**

Bilder [1]

schmid datensicherheit

Fakten:

- Im Internet werden täglich 1,8 Milliarden Bilder zu irgendwelchen Diensten hochgeladen.
- Im Jahr 2020 werden geschätzte 1,2 Billionen Fotos erstellt.
  - Allein in Indien wurden innerhalb von 5 Jahren 159 durch Selfies verursachte Todesfälle dokumentiert (Anteil der Männer: 72,5%).

Anwendbare Gesetze:

- Urheberrecht:
  - Erlaubnis des Fotografen, Rechte des Fotografen
  - Urheberpersönlichkeitsrecht: Recht auf Anerkennung der Urheberschaft (§ 13 S. 1 UrhG), Nennung des Fotografen
- Datenschutzrecht:
  - Erlaubnis und Rechte der abgebildeten Person

Bilder [2]

schmid datensicherheit

Datenschutzrecht:

- Werden die Bilder durch natürliche Personen im Rahmen ausschließlich familiärer oder persönlicher Tätigkeiten erstellt, gilt das Datenschutzrecht von vornherein nicht.
- Ist das Datenschutzrecht doch anzuwenden, können Fotos – wie bisher – in vielen Fällen auf der Grundlage einer Interessenabwägung aufgenommen und weiterverarbeitet werden.
  - Faustformel: Je geringer der Eingriff in das Persönlichkeitsrecht (bspw. bei Überblicksaufnahmen, Aufnahmen in Stadien oder bei öffentlichen Veranstaltungen usw.), umso eher fällt diese Interessenabwägung zu Gunsten des Fotografierenden aus.
  - Dies kann auch bei besonders Schutzbedürftigen wie Kindern gelten, soweit damit nicht nur eigene Interessen, sondern zum Beispiel gleichzeitig die des Kindes selbst und anderer Kinder verfolgt werden – wie im Fall von Fotoalben als Abschlussgeschenk im Kindergarten.

Bilder [3]

schmid datensicherheit

Einwilligung und andere rechtliche Aspekte:

- Eine Einwilligung ist hingegen – wie bisher – nur in wenigen Fällen notwendig, vor allem dann, wenn die Interessen des Betroffenen nicht aufgenommen zu werden, überwiegen. Eine Einwilligung kann also unter anderem notwendig sein, wenn es sich um Porträtaufnahmen handelt oder die Aufnahme eine nicht sozialadäquate Situation wiedergibt.
- Für die Veröffentlichung von Bildern im Internet gilt, wie inzwischen auch gerichtlich bestätigt wurde, weiterhin das Kunsturhebergesetz, mit dem das Recht am eigenen Bild geschützt wird.
- Dieses Gesetz erlaubt, Bilder von Versammlungen oder Aufzügen wie Volksfesten, Festumzügen usw. ohne Einwilligung zu veröffentlichen.
- Bei der Erfassung von Bildern in digitalen Archiven (z.B. Datenbanken, aber auch Webseiten) müssen die Metadaten in den Bildern bereits vor dem Abspeichern der Bilder gelöscht werden (Datenminimierung, Standort und Zeitpunkt der Aufnahme des Bildes, Seriennummer des Fotoapparates, die auf den Fotografen zurückgeführt werden kann, u.s.w.).
  Die Vorgabe zur Minimierung der Daten und die Vermeidung der Speicherung von Metadaten können z.B. Fotografen, Werbeagenturen oder andere Betreiber von Bildsammlungen betreffen.

Bilder [4]

schmid datensicherheit

Bilder von Verstorbenen:

- DS-GVO endet mit dem Tod, das Persönlichkeitsrecht gilt weiter
- Bei Vereinen kann der Umgang mit Sterbebildern (und weiteren Informationen) über die Satzung geregelt werden
- Rechtzeitig eine Einwilligung einholen
- Zustimmung der Familie abfragen

Kinder:

- Einwilligung der Eltern einholen

Medien:

- Es gelten die publizistischen Grundsätze, Pressekodex

Bilder [5], Videos, Audio

schmid datensicherheit

Persönliche und familiäre Verarbeitung:

- Familienalben und Adressbücher (mit Bild) fallen nicht unter das Datenschutzrecht
- Cloudspeicher als geschlossene familiäre Nutzergruppe ist möglich, aber Passwort-geschützt
- nicht erlaubt:
  Online-stellen anderer Personen auf Facebook, Instagram, Whatsapp & Co.

Dashcams:

- Dashcam-Videos dürfen nicht veröffentlicht werden
- Dashcam-Videos dürfen nicht der Polizei oder einer Versicherung gegeben werden
- Crashcam-Videos (nur die letzten 30 Sekunden vor einem Unfall bleiben gespeichert, alles andere wird automatisch gelöscht) dürfen zur Rekonstruktion eines Unfalls herangezogen werden

Tonaufnahmen:

- Für Tonaufnahmen muss eine Einwilligung vorliegen

Fragerunde 9

schmid datensicherheit

Sicherheit der Verarbeitung (Schutz der eigenen Informationen), Art. 32 DS-GVO:

Konten bei einem Social Media Betreiber können auf folgende Weise gehacked werden (mehrere Antworten möglich)**?**

A) Social Engineering;

B) Schwache Passwörter;

C) Phishing;

D) Denial of Service;

Fragerunde 9 (Antwort)

schmid datensicherheit

Sicherheit der Verarbeitung (Schutz der eigenen Informationen), Art. 32 DS-GVO:

Konten bei einem Social Media Betreiber können auf folgende Weise gehacked werden (mehrere Antworten möglich)**?**

A) Social Engineering;

B) Schwache Passwörter;

C) Phishing;

D) ~~Denial of Service~~;

Personalausweis

schmid datensicherheit

Kopieren von Personalausweisen:

- Der Personalausweis darf nicht ohne Zustimmung des Inhabers kopiert werden (§ 20 Abs. 2 PAuswG).
- Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist.
- Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben.
- Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun.
- Zum Zweck, die Identität einer Person zu überprüfen, genügt es, den Personalausweis einer Sichtprüfung zu unterziehen.
- Die zur Identifikation benötigten Daten (Name, Vorname, Adresse, Geburtsdatum) können auch dadurch gewonnen werden, dass die o. g. zur Identifizierung erforderlichen – aber auch ausreichenden – Daten daraus notiert werden.
- Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Internationaler Datenverkehr

schmid datensicherheit

Datenaustausch in der EU und mit Drittstaaten:

- Bei der Bearbeitung grenzüberschreitenden Datenaustausches muss zunächst die innerhalb Europas federführend zuständige Datenschutzbehörde identifiziert werden (Verfahren nach Artikel 56 DS-GVO). Diese Behörde ist bei Fragen oder Genehmigungsverfahren der relevante Ansprechpartner (One-Stop-Shop-Verfahren nach Art. 60 DS-GVO).
- Auftragsverarbeiter dürfen nicht ohne Weiteres Unterauftragsverarbeiter einsetzen, sondern müssen dabei einige Vorschriften berücksichtigen, insbesondere Artikel 28 und Artikel 44 (Datenübermittlung) DS-GVO.
- Auftragsverarbeiter dürfen Unterauftragsverarbeiter nur mit einer schriftlichen Genehmigung einschalten.
- Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation bedarf geeigneter Garantien. Die europäische Rechtslage ist noch nicht abschließend geklärt. Die Frage, ob das US-Privacy Shield tatsächlich einen wirksamen Rechtsschutz gewährleisten kann, wird in 2 Gerichtsverfahren geklärt.
- Mögliches Instrument sind die „EU-Standarddatenschutzklauseln“ gemäß Art. 46 Abs. 2 Buchstabe c bzw. d DS-GVO. Nur die verantwortliche Stelle kann diese Art von Vertrag für Auftragsverarbeiter außerhalb der EU abschließen. (Gilt auch für Unterauftragsverarbeiter.)

Beschäftigtendatenschutz [1]

schmid datensicherheit

Mitarbeiterfoto:

- Bilder von Angestellten können mit Einwilligung verwendet werden.
- Bei älteren veröffentlichten Bildern (z.B. Werbebildern) können ehemalige Mitarbeiter nur die Nutzung widerrufen, wenn ein plausibler Grund vorliegt.
- Eine Interessenabwägung kann dazu führen, den Widerruf zu verwerfen.

Versendung von Gehaltsnachweisen per E-Mail:

- Bei Versendung im firmeneigenen Netz mit ausschließlichem Zugriff der Berechtigten bestehen keine Bedenken.
- Bei Versendung an privaten E-Mail-Accounts bei Fremdprovidern sind besondere Schutzmaßnahmen zu treffen.
- Der für die Verarbeitung verantwortliche Arbeitgeber hat gemäß § 32 DS-GVO sicherzustellen, dass die Sicherheit der Verarbeitung und insbesondere die Vertraulichkeit der Informationen gewährleistet sind.
- Der Arbeitgeber kann vom Arbeitnehmer nicht verlangen, eine E-Mail-Adresse zu Zwecken der Zusendung einer Gehaltsabrechnung zur Verfügung zu stellen.

Beschäftigtendatenschutz [2]

schmid datensicherheit

- Regelungen zum Arbeitnehmerdatenschutz sind im § 26 BDSG (neu) festgelegt.
- Präzise Regelungen sind bisher nicht ausreichend verfügbar, insbesondere:
  - Datenschutz im Bewerbungsverfahren
  - Gestaltung des Arbeitsverhältnisses und Compliance-Fragen (Dienstvereinbarungen, Verpflichtungen, Dienstanweisungen)
  - Personalentwicklung und Persönlichkeitsprofile
  - Umgang mit Gesundheitsdaten
  - Überwachungssysteme am Arbeitsplatz
  - Einsatz von biometrischen Verfahren und Big Data Anwendungen
  - Private Nutzung dienstlicher Kommunikationsmittel
  - Dienstliche Nutzung privater Kommunikationsmittel
  - Transparenz der Datenverarbeitung
  - Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unt., die eine gemeinsame Wirtschaftstätigkeit ausüben
  - Whistleblowing
- **Empfehlung**: Regelungen und Prozesse gut dokumentieren!

Vereine [1]

schmid datensicherheit

Bilder in Chroniken des Vereinsleben:

- nur Vereinsmitglieder können über Satzung eingebunden werden
- Dokumentation des Vereinslebens mit Interessenabwägung
- je weniger eng die Bindung einer abgebildeten Person zum Verein ist, desto eher ist eine Einwilligung notwendig
- die Informationspflicht muss immer beachtet werden

Sportvereine:

- Bilder von Spielen mit Beteiligung einer gegnerischen Mannschaft (z.B. Fußball) sind erlaubt
- die Information der Betroffenen ist notwendig
  - über Vereinssatzung
  - über den Hauptverband der jeweiligen Sportart
  - Aushang in den Umkleiden

Vereine [2]

schmid datensicherheit

Erstellung und Veröffentlichung von Personenbildern:

- Rechtsgrundlage meist (nur) Art. 6 Abs. 1 Buchstabe f DS-GVO
- Vereine haben ein berechtigtes Interesse daran, über ihre Veranstaltungen (Mitgliederversammlung, Tag der offenen Tür, Sportereignisse einschließlich Siegerehrung, Vereinsausflug, usw.) auch durch Bilder zu berichten.
- Auch vereinsfremde Personen können abgebildet sein, wenn Interesse des Vereins überwiegt.
- Besondere Arten personenbezogener Daten im Sinne von Art. 9 DS-GVO dürfen nur mit ausdrücklicher Einwilligung nach Art. 9 Abs. 2 Buchstabe a DS-GVO angefertigt und veröffentlicht werden (z.B. Selbsthilfeverein für Menschen mit einer bestimmten Erkrankung)

Feuerwehr:

- Die Feuerwehr ist eine sogenannte Zwitter-Einrichtung: öffentlicher Auftrag versus Feuerwehrverein
- Einsatzbilder dürfen keinen Personenbezug enthalten

Datenschutzaufsicht

schmid datensicherheit

Einzelne Prüfaspekte des Bayerischen Landesamts für Datenschutzaufsicht:

Bild: Bayerisches Landesamt für Datenschutzaufsicht, Ansbach

- **Videoüberwachung in Gastronomie und Kinos**
- **Kfz-Werkstätten-Kontrolle**
- **Patch Management bei WordPress-Websites**
- **WordPress GDPR Compliance Plugin**
- **Patch Management bei Magento-Websites**
- **Informationspflichten bei Bewerbungen**
- **Ransomware bei Arztpraxen**

Videoüberwachung in Gastronomie und Kinos

schmid datensicherheit

Erwartungshaltung der Gäste ist dahin gehend, nicht Gegenstand von Überwachungsmaßnahmen zu sein. Als Zweck der Überwachung geben Unternehmen in aller Regel die Straftatprävention und erleichterte Straftatenaufklärung an. Daneben wird häufig der Kassenbereich überwacht, sodass auch Mitarbeiter von der Videoüberwachung betroffen sind.

Prüffragen (Schwerpunkt der Prüfung):

- **Wie viele Videokameras sind im Unternehmen installiert?**
- **Welche Bereiche werden von den Videokameras erfasst?**
- **Welche Zwecke werden durch die Videoüberwachung verfolgt?**
- **Haben die Kameras Zoom-, Schwenk- und/oder Neigetechnik?**
- **Werden Aufzeichnungen angefertigt und wenn ja,**
  - **wie lange werden diese gespeichert,**
  - **wer hat Zugang zu den Aufzeichnungen und**
  - **an welche Stellen werden diese ggf. weitergegeben?**
- **Wie wird auf die Videoüberwachung hingewiesen?**

Kfz-Werkstätten-Kontrolle

schmid datensicherheit

Moderne Kraftfahrzeuge generieren immer mehr Daten. Viele davon werden in der Werkstatt für die Inspektion oder die Reparatur benötigt, aber dabei zum Teil an die Kfz-Hersteller übermittelt. Auch rein technische Daten können personenbezogene Daten sein, wenn sie bspw. mit Kundendaten verknüpft werden.

Prüffragen (Auszug):

- **Welche Daten werden bei einem Werkstattbesuch (z. B. bei Wartung, Reparatur, Unfall) aus dem Fahrzeug erhoben und in den Systemen der Werkstatt gespeichert?**
- **Auf welcher Rechtsgrundlage werden die Daten verarbeitet?**
- **Für welchen Zeitraum erfolgt eine Speicherung dieser Daten?**
- **Wird der Kunde von der Speicherung in Kenntnis gesetzt und wenn ja, wie?**
- **Werden Fahrzeugdaten an den Hersteller oder sonstige Externe weitergeleitet?**
- **Falls ja: Zu welchem Zweck werden Daten weitergeleitet (Produktbeobachtung, Produktoptimierung, Bearbeitung von Garantiefällen usw.)?**

Patch Management bei WordPress-Websites

schmid datensicherheit

Regelmäßig werden Sicherheitslücken bei IT-Systemen bekannt. Besonders häufig wird über gehackte Websites berichtet, die auf Grund einer nicht aktuell gehaltenen Softwareversion angreifbar sind. Prüfungsgegenstand ist der sichere Einsatz sog. Content Management Systeme (CMS). Mit diesen Systemen lässt sich der Inhalt von Webseiten oft sehr einfach erstellen, bearbeiten und verwalten.

Prüfpunkte:

- **Version der eingesetzten WordPress-Installation**
- **Version der eingesetzten WordPress-Plugins**
- **HTTPS-Implementierung**

WordPress GDPR Compliance Plugin

schmid datensicherheit

Anfang November 2018 wurde eine sehr kritische Sicherheitslücke in einer Erweiterung für WordPress-Installationen bekannt. Das Besondere an der Sicherheitslücke war, dass diese im „WP GDPR Compliance“ vorhanden war, mit dem Websitebetreiber eigentlich Vorgaben der DS-GVO einhalten wollten. Das GDPR Compliance Plugin ergänzt Checkboxes für das explizite Einverständnis des Benutzers und die Double-Opt-in-Funktion für die Newsletter-Bestellung. Das Plugin besaß bis einschließlich Version 1.4.2 diese Lücke, durch die die Angreifer die Website ohne größeren Aufwand übernehmen konnten.

Prüffragen:

- **In welcher Version wird WordPress als CMS für den Betrieb der Website verwendet?**
- **Kommt das WP GDPR Compliance Plugin zum Einsatz?**
- **Falls ja, wurde das Plugin bereits aktualisiert (gepatcht)?**

Patch Management bei Magento-Websites

schmid datensicherheit

Die Gefährdungslage bei Online-Shops ist besonders hoch ist. Veraltete Shop-Systeme weisen oftmals Schwachstellen auf, die Cyberkriminelle gezielt ausnutzen können.

Prüffragen:

- **Kommt HTTPS in ausreichender Konfiguration zum Einsatz?**
- **Wird eine aktuelle Magento-Version eingesetzt?**
- **Wird die Magento-Installation regelmäßig hinsichtlich Updates untersucht?**
- **Sind alle relevanten Sicherheitspatches installiert?**
- **Sind sicherheitskritische Verzeichnisse des Webservers öffentlich abrufbar?**
- **Besteht ein ausreichender Schutz vor Malware und anderen Angriffsarten?**
- **Besteht ein geregelter Prozess zum Patch Management?**

Informationspflichten bei Bewerbungen

schmid datensicherheit

Zahlreiche Anfragen und Beschwerden liegen im Zusammenhang mit dem Umgang personenbezogener Daten im Bewerbungsverfahren vor.

Prüffragen:

- **Wie kommen Unternehmen als potentielle Arbeitgeber im Bewerbungsverfahren den Informationspflichten gegenüber Bewerbern nach?**
- **In welchen Fällen werden im Bewerbungsverfahren Rückfragen beim früheren Arbeitgeber gestellt?**
- **Welche Abteilungen oder Bereiche haben im Unternehmen Zugriff auf die Bewerbungsunterlagen?**
- **Wie wird sichergestellt, dass die Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens in den Abteilungen oder Bereichen wieder gelöscht werden?**
- **Wann werden die Daten der abgelehnten Bewerber gelöscht?**
- **Existiert im Verzeichnis der Verarbeitungstätigkeiten ein Eintrag für Bewerbungsverfahren?**

Ransomware bei Arztpraxen

schmid datensicherheit

Ransomware, auch Verschlüsselungstrojaner genannt, sind auch in Bayern aktiv. Durch die Schadsoftware wird der Zugriff auf Daten gesperrt und anschließend Lösegeld gefordert, um die Daten wieder zurück zu erhalten. Ziel der Datenschutzprüfung war es, Umgang und Prävention von Ransomware-Attacken zu kontrollieren und für ein geeignetes und wirksames Backupverhalten zu sorgen.

Prüffragen:

- **Werden regelmäßige, automatisierte Backups der Patientendaten durchgeführt?**
- **Mit welcher Software werden Backups durchgeführt?**
- **Auf welchen Speichermedien werden die Backups gespeichert?**
- **Wird das Zurückspielen von Backup-Daten getestet?**
- **Ist das Praxisverwaltungssystem (PVS) an das Internet angeschlossen?**
- **Befinden sich an das Internet angeschlossene (Recherche-)Rechner in anderen Netzsegmenten als das Praxisverwaltungssystem?**
- **Sind Netzlaufwerke mit relevanten Patientendaten mit Rechnern verbunden, die an das Internet angeschlossen sind?**
- **Wurden Awareness-Schulungen durchgeführt, die Internetbedrohungen (z. B. Schadcode, Phishing,...) zum Inhalt hatten?**

schmid datensicherheit

Datenschutz / EU-DS-GVO

VERORDNUNG (EU) 2016/679

... vom 27. April 2016

Bild: C.H.Beck Verlag

Datenschutz für Unternehmen

schmid datensicherheit

Wichtigste Punkte mit denen sich ein Betrieb beschäftigen muss:

- **Dokumente (Verfahrensverzeichnis, Verarbeitungstätigkeiten)**
- **Texte (Einwilligungen, Informationen für Betroffene)**
- **E-Mails** (Vertraulichkeit personenbezogener Daten)
- **Webauftritt,** Cookies, Online-Analytics
- **Datenschutzerklärung,** Impressum**, Kontaktformular**
- **Soziale Netzwerke – Like-Buttons**
- **Datenschutzbeauftragter**
- **Bilder, Veranstaltungen**
- **Kinder**
- **...**

Bilder: pixabay.com

Verantwortliche Stelle

schmid datensicherheit

Begriffsübersicht für die Pflichten der Verantwortlichen:

- **Nachweis der Einhaltung von Datenschutzgrundsätzen / Transparenz**
- **Dokumentationspflicht / Verarbeitung und Verwendung von personenbezogenen Daten muss dokumentiert werden**
- **Meldepflicht bei Datenschutzverstößen (72 Std. für Behördenkontakt)**
- **Datenschutzschulungen / Awareness-Maßnahmen – Datenschutz-Verpflichtung aller Zugriffsberechtigten**
- **Datenschutz-Beauftragter / Datenschutz-Audits**
- **Verarbeitung im Auftrag (wechselseitige Haftung/Kontrolle) / AV-Vertrag (Auftragsverarbeitung)**
- **BDSG-neu - Nationale Spielräume**
- **Sanktionsmöglichkeiten sind verschärft / Strafen sind deutlich angehoben**

Datenerhebung, Datenvermeidung und Datensparsamkeit

schmid datensicherheit

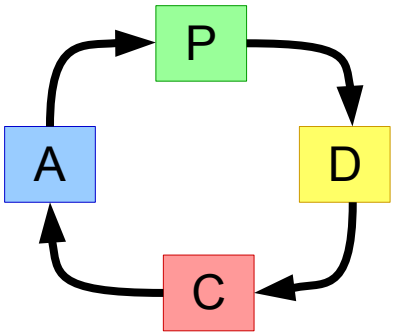
Die rechtlichen Grundlagen sind in der DS-GVO geregelt:

- **Datenerhebung ist erlaubt,**
  - wenn dieses Gesetz oder andere Vorschriften das erlauben oder anordnen, oder
  - der Betroffene eingewilligt hat.
  - Einwilligung des Betroffenen nur wirksam, wenn freie Entscheidung möglich.
  - Für Kinder (Grenze 16 Jahre) gelten besondere Voraussetzungen.
- **Der Betroffene ist über**
  - die Identität der verantwortlichen Stelle,
  - die Zweckbestimmung, sowie
  - über die Empfänger der Daten zu unterrichten
- **Erhebung, Verarbeitung und Nutzung von Daten muss mit dem Ziel erfolgen,**
  - so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen,
  - die Daten müssen für den Zweck der Datenerhebung erforderlich sein.

Auswirkungen der DS-GVO

schmid datensicherheit

Anforderungen und Reichweite:



- **Datenschutzkonzept (Datenschutz-Mgmt.system)**
- **Datenschutz als Prozess (PDCA-Zyklus)**
  {Plan → Do → Check → Act → Plan → ..., Audits}
- **spezieller Schutzbedarf für digital verarbeitete personenbezogene Daten (→ verstärkter Fokus auf IT-Sicherheit)**

- **Auch die Daten von eigenen Kontakten, die in einem anderen Unternehmen verfügbar sind, sind personenbezogene Daten !!**
- **Kein Unterschied zwischen privat und geschäftlich**
- **Personenbezug in der „Zukunft“ möglich !?!**
- **Die DS-GVO gilt für "ALLE", die personenbezogene Daten elektronisch oder nicht automatisiert in einer strukturierten Ablage verarbeiten (bzw. nutzen).** Aufwand soll im Verhältnis zur Unternehmensgröße stehen.

IT mit Personenbezug

schmid datensicherheit

Begriffsübersicht für die (digitale) Datenverarbeitung:

- **IT-Sicherheit für die Verarbeitung personenbezogener Daten**
- **Schutzziele der Informationssicherheit / Belastbarkeit der Systeme**
- **TOMs - Technisch-organisatorische Maßnahmen**
- **Datensicherung und Löschkonzept**
- **Verhinderung des Missbrauch zu anderen Zwecken**
- **Rechtmäßigkeit, z.B. einer Überwachung** (Objektschutz durch Videoüberwachung)
- **Risikoanalyse / Risikobewertung** (Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen)
- **Datenschutz-Folgenabschätzung (Privacy Impact Assessment)**
- **Privacy-by-Design / Privacy-by-Default**
- **Security-by-Design (Stand der Technik)**

Einwilligungen

schmid datensicherheit

Inhalte einer Einwilligungserklärung (Nachweis):

- Betroffene Person und Gegenstand der Einwilligung
- Verantwortlicher, Verantwortliche Stelle (hat die Rechenschaftspflicht)
- Freiwilligkeit der Einwilligung / Kopplungsverbot
- Verwendungszweck
- Empfänger der Daten / Reichweite der Nutzung
- Rechte des Betroffenen / Rechtsgrundlage
- Widerrufbarkeit / Widerspruchsrecht / Datenübertragbarkeit
- Zustimmung für die einzelnen Verwendungszwecke so differenziert wie möglich:
  - Bilder auf dem Webauftritt
  - Name bei den Bildern auf dem Webauftritt
  - Bilder auf dem Facebook-Auftritt
  - Name bei den Bildern auf dem Facebook-Auftritt
- Keine aktivierten Voreinstellungen (Privacy-by-Default)

Datenschutzverletzungen

schmid datensicherheit

Bei Datenschutzverletzungen existiert eine gesetzliche Meldepflicht bei der Aufsichtsbehörde.
Beispiele für Meldepflicht:

- **Hacking von IT-Systemen**
- **Verlust von Daten**
- **Diebstahl von papiergebundenen oder digitalen Daten**
- **Fehlversand**
- **Softwarefehler**
- **Schadcode, Trojaner (Daten sind fremdverschlüsselt)**
- **Fehlentsorgung**
- **Vernichtung (versehentliches oder absichtliches Löschen)**
- **Sonstiges ?**

Bilder: pixabay.com

Transparente Verarbeitung

schmid datensicherheit

Aus Erwägungsgrund Nr. 39 der DSGVO ergibt sich der Grundsatz der Transparenz (für das öffentliche Verfahrensverzeichnis und die Datenschutzerklärung):

- **Dieser setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind.**
- **Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden.**
- **Information plus Bildsymbole können für Transparenz (und transparente Texte) verwendet werden.**
- **Es muss eine Bewertung erfolgen, ob in Texten evtl. unwirksame datenschutzrelevante Klauseln enthalten sind.**

Arbeitnehmer

schmid datensicherheit

Neue Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO ! (§5 BDSG gibt es nicht mehr)

Fälle des Arbeitnehmerdatenschutzes:

- **Überwachung des Surfverhaltens** (Mitarbeitervereinbarungen)
- **Elektronische Zeiterfassung / Krankmeldungen**
- **Videoüberwachung am Arbeitsplatz**
- **Speicherung und Löschung von Bewerberdaten**
- **Veröffentlichung interner Daten (Unternehmenszeitung, Newsletter, Bilder, Geburtstage)**

Datenschutzerklärung

schmid datensicherheit

Jeder Online-Auftritt braucht eine Erklärung zum Datenschutz:

- **Erklärung welche Daten zu welchem Zweck verarbeitet werden**
- **Erklärung welche Daten beim Besuch der Webseite generiert oder erfasst werden**
  - Webserver-Logging, Aufzeichnungen in Schutzsystemen des Providers
  - Cookies (Einwilligungsbanner bei Personenbezug)
  - Webtracking / Web-Analytics (Einwilligungsbanner)
- **Speicherfristen beschreiben**
- **Rechtsgrundlage beschreiben**
- **Erklärung welche Rechte der Benutzer hat**
- **Kontaktmöglichkeit zum Betreiber des Webauftritts**
- **Link zur Plattform für Online-Streitbeilegung "https://ec.europa.eu/consumers/odr/" im Impressum bereitstellen**

Bilder: pixabay.com, Einladung_zum_Essen

Cookies [1]

schmid datensicherheit

Die EU-Vorgaben zu Cookies sind in der Verordnung 2009/136/EC des Europäischen Parlaments und des Rates geregelt: Cookie-Richtlinie

- **Die Cookie-Richtlinie der EU:**
  - Diese Richtlinie ist in Europa völlig uneinheitlich umgesetzt.
  - Richtlinie mit Opt-in implementiert: Dänemark, Frankreich, Großbritannien, Litauen, Niederlande, Österreich, Schweden und Spanien;
  - Richtlinie mit Opt-out implementiert: Bulgarien, Finnland, Luxemburg, Polen, Slovakei, Tschechien und Ungarn
  - Richtlinie nicht implementiert: Belgien, Deutschland, Estland, Griechenland, Italien, Lettland, Norwegen, Malta, Portugal und Zypern.
- **Cookies werden nach Anbieter unterschieden:**
  - First-Party-Cookies (Direktanbieter-Cookies): die Webseite muss den Benutzer informieren;
  - Third-Party-Cookies (Drittanbieter-Cookies): Werbeeinblendungen müssen direkt informieren (Icons).

Cookies [2]

schmid datensicherheit

Die rechtlichen Grundlagen sind im **TMG** (= Telemediengesetz) geregelt:

- **Oft ist die Information des Benutzers über Cookies durch ein pop-up-Fenster gelöst.**
  - Aktuell ist der Einsatz von pop-up-Fenstern mit Cookie-Hinweisen in Deutschland nicht notwendig, wenn die Verwendung von Cookies in der Datenschutzerklärung erläutert wird.
  - Strenge, zwingende Richtlinien für pop-ups gelten z.B. in Großbritannien.
- **Die Cookie-Policy kann generell als opt-out implementiert werden.**
  - Meistens kann man nur die Cookie-Information abnicken → Cookie-Behandlung kann durch Browser-plug-ins erfolgen.
  - Manchmal kann man Cookies "akzeptieren" oder "ablehnen". Was passiert jeweils?
- **Empfänger, Funktionsweise, Zweck und Nutzung der Cookies (auch Ausschlussaspekte), Widerspruchsrecht des Benutzers beschreiben.**

Cookies [3]

schmid datensicherheit

Neue europäische Regelwerke sind im Genehmigungsprozess:

- **VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/**
  - **e-Privacy**-Richtlinie (Verordnung über Privatsphäre und elektronische Kommunikation)
- **Die Ausgestaltung der Cookie-Richtlinie steht erst fest, wenn die e-Privacy-Richtlinie der EU (evtl. noch in 2019) verabschiedet und interpretiert ist.**
- **Die bayerische Aufsichtsbehörde ist der Meinung, dass die generelle Implementierung von pop-up-Fenstern auf allen Seiten, die Cookies verwenden, kontraproduktiv ist, weil dies jeweils zu einem grundsätzlichen Abnicken der Cookie-Hinweise durch den Nutzer führt.**

Risikobehandlung

schmid datensicherheit

Maßnahmenbeispiele (Risikobewertung, evtl. Datenschutz-Folgenabschätzung):

- **Datenminimierung**
- **Verschlüsselung**
- **Pseudonymisierung / Anonymisierung**
- **Rollen-/Rechtekonzepte**
- **Zugangs-, Zutritts- und Zugriffskontrolle**
- **Datenschutzmanagementsystem / (ISMS)**
- **Awareness / Datenschutzschulungen**
- **Trennung von Test-/Produktivsystemen**
- **Mandantentrennung**
- **Nicht-Verkettbarkeit**
- **Identifikationsprozesse**
- **Lösch-/Sperrkonzepte**

Bilder: pixabay.com, 3dman_eu

Kinder unter 16 Jahren [1]

schmid datensicherheit

Umgang mit personenbezogenen Daten von Kindern:

- **Immer schriftliche Einwilligung einholen (idealerweise von beiden Elternteilen)**
- **Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für einen kindgerechten Datenschutz im Umgang mit digitalen Medienangeboten:**
  - Empfehlung 1:
    Anbieter digitaler Medien und Dienste, die insbesondere auch Minderjährige ansprechen, sind aufgefordert, die Datenschutzbelange dieser Zielgruppe in besonderem Maße zu berücksichtigen.
  - Empfehlung 2:
    Der besonderen Schutzbedürftigkeit Minderjähriger ist durch eine entsprechende Gestaltung von Produkten und Dienstleistungen besonders Rechnung zu tragen. Informationspflichten sind kindgerecht verständlich darzustellen.

Kinder unter 16 Jahren [2]

schmid datensicherheit

Umgang mit personenbezogenen Daten von Kindern:

- **Empfehlungen der Bundesbeauftragten für den Datenschutz .....:**
  - Empfehlung 4:
    Datenschutzhinweise einschließlich Informationen zu den erforderlichen Einwilligungen sind in einfacher und für Minderjährige leicht verständlicher Sprache abzufassen und an exponierter Stelle zu platzieren.
  - Empfehlung 5:
    Erziehungsberechtigte, Lehrkräfte und alle sonstigen in die Betreuung von Kindern und Jugendlichen eingebundenen gesellschaftlichen Kräfte sind aufgerufen, gerade in Zeiten der durch die Digitalisierung ermöglichten Freiheiten sowohl für den besonderen Wert personenbezogener Informationen als auch für das Risiko der hohen Verletzbarkeit der eigenen Persönlichkeit zu sensibilisieren.

Zusammenfassung

schmid datensicherheit

Die wichtigsten Schritte in Kürze:

- **Anlegen eines Verfahrensverzeichnisses**
- **Datenschutzerklärung / Social Media**
- **Anpassung Internetseite / Webshop**
- **soweit erforderlich gesonderte Einholung von Einwilligungen (Mitarbeiter, Newsletter, Direkterhebung, Messeakquise)**
- **soweit erforderlich Verpflichtungserklärungen und Dienstvereinbarungen unterzeichnen (Mitarbeiter)**

Cookie-Hinweis

schmid datensicherheit

Bild: © kleinert.de/Kostas Koufogiorgos

ENDE

schmid datensicherheit

Vielen Dank für die Aufmerksamkeit!

Fragen?

Hinweise [1]

schmid datensicherheit

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Datenschutz in Bayern für den nicht-öffentlichen Bereich

Promenade 27 (Schloss), 91522 Ansbach

https://www.lda.bayern.de/

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD)

Zuständigkeit für bayerische öffentliche Stellen

Wagmüllerstraße 18, 80538 München

https://www.datenschutz-bayern.de/

Hinweise [2]

schmid datensicherheit

Hinweise zu gesetzlichen Informationen:

- **Gesetzliche Grundlagen:**
  Datenschutz-Grundverordnung (EU DS-GVO) ab 25. Mai 2018 anwendbar
  – https://dsgvo-gesetz.de/
- **Bundesdatenschutzgesetz:**
  – https://dsgvo-gesetz.de/bdsg-neu/
- **Bayerisches Datenschutzgesetz (BayDSG)** vom 15. Mai 2018:
  – https://www.gesetze-bayern.de/Content/Document/BayDSG
- **Weg zur DS-GVO – Selbsteinschätzung:**
  – https://www.lda.bayern.de/tool/start.html

Hinweise [3]

schmid datensicherheit

Spezifische Informationen:

- **Handreichungen für kleine Unternehmen und Vereine:**
  – https://www.lda.bayern.de/de/kleine-unternehmen.html
- **Verzeichnis von Verarbeitungstätigkeiten:**
  Bayerisches Landesamt für Datenschutzaufsicht (Vorlage)
  – https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf
- **Fragebogen zur Umsetzung der DS-GVO:**
  – https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf
- **Webauftritt der Datenschutzkonferenz (DSK):**
  Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder
  – https://www.datenschutzkonferenz-online.de/

Hinweise [4]

schmid datensicherheit

- **Datenschutzgeneratoren für Internetseiten:**
  Bund der Selbständigen - Gewerbeverband Bayern e.V
  – https://www.bds-bayern.de/datenschutzgenerator/
- **Rechtsanwaltskanzlei Dr. Thomas Schwenke:**
  – https://datenschutz-generator.de/
- **Meldung des Datenschutzbeauftragten an die Aufsichtsbehörde (Bayern) / (Wenn bestellt):**
  – https://www.lda.bayern.de/de/dsb-meldung.html
- **Meldung Datenschutzverletzung (Bayern) / Innerhalb von 72 Stunden! (Art. 33 DS-GVO):**
  – https://www.lda.bayern.de/de/datenpanne.html

Hinweise [5]

schmid datensicherheit

EU-U.S. and Swiss-U.S. Privacy Shield Frameworks

https://www.privacyshield.gov/welcome

https://www.privacyshield.gov/European-Businesses

NOYB – European Center for Digital Rights – Wien

"*Privacy is none of your business*"

https://noyb.eu/

Mag. Max Schrems, Dr. Petra Leupold, Dr. Christof Tschohl

Hinweise [6]

schmid datensicherheit

Suchmaschinen mit geringer Nutzerverfolgung

https://www.startpage.com/

https://metager.de/

https://duckduckgo.com/

Informationen über Tracking im Netz

https://crackedlabs.org/

https://whotracks.me/

Hinweise [7]

schmid datensicherheit

Studie der Universität Erlangen-Nürnberg

Wie eindeutig bin ich beim Surfen wiedererkennbar?

Nehmen Sie bitte an der Studie des Lehrstuhls Informatik 1 der Friedrich-Alexander-Universität Erlangen teil:

https://browser-fingerprint.cs.fau.de/

Panopticlick der Electronic Frontier Foundation

https://panopticlick.eff.org/

Beratungsangebot

schmid datensicherheit

Die Schmid Datensicherheit GmbH steht Ihnen für die folgenden Aufgaben zur Verfügung:

- **Datenschutz (Datenschutzberatung, DSB)**
- **Reseller für Signierzertifikate (X.509)**
- **Unterstützung bei Informationssicherheits-Managementsystemen in Unternehmen**
  - ISO/IEC 27001
- **Unterstützung bei Produktzertifizierungen**
  - Common Criteria
  - Beschleunigte Sicherheitszertifizierung
- **Unterstützung bei Auswahl von zertifizierten Produkten**
  - Security Target und was der Inhalt bedeutet

Kontakt

schmid datensicherheit

Dipl.-Ing. (Univ.) Lutz J. Schmid

Schmid Datensicherheit GmbH

Heidestraße 4

92637 Weiden / Opf.

Tel.: 0961-4712941

Mobil: 0160-98492962

Email: info@schmid-datensicherheit.de

URL: www.schmid-datensicherheit.de